Arithmetic Explorations

Jonathan M Gerhard

December 20, 2022

1 Arithmetic Rambles

Started with studying $g(n) = \gcd(n, \sigma(n))$, where

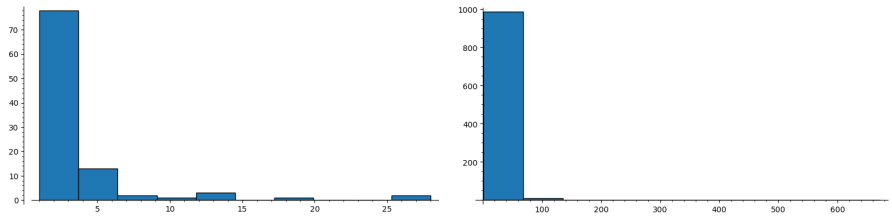
$$\sigma(n) = \sum_{d|n} d.$$

For any function $f : \mathbb{Z}^+ \to \mathbb{Z}^+$, we can look at the *average order* of f, defined as g if

$$\sum_{n=1}^{x} f(n) \approx \sum_{n=1}^{x} g(n)$$

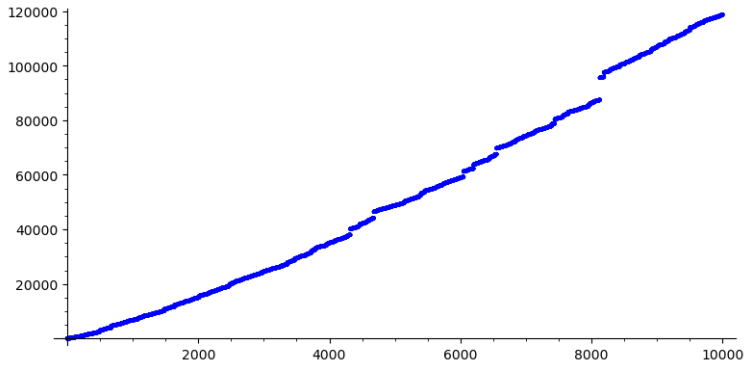
as $x \to \infty$

Looking at the distribution of $g(n)$ shows a major right-skew.



The first is with $x = 100$ and the second is $x = 1000$ and any higher pretty much just looks like a single bar at the beginning.

The following is a plot for $x = 10^5$.



A good estimate for $\sum_{n\leq x} g(n)$ is $x^{1.256}$.

Which leads to the following question.

Question 1 *Can we show for any $\theta \in (0,1)$ ($\theta > 1/3$ for example) that*

$$\sum_{n\leq x} g(n) < x^{1+\theta}$$

for large enough x.

Let's list a few known average orders.

1. $\sum_{n\leq x} d(n) \approx \sum_{n\leq x} log(n)$
2. $\sum_{n\leq x} \sigma(n) \approx \frac{\pi^2}{6} \sum_{n\leq x} n$
3. $\sum_{n\leq x} \omega(n) \approx \sum_{n\leq x} log(log(n))$
4. $\sum_{n\leq x} \Omega(n) \approx \sum_{n\leq x} log(log(n))$
5. $\sum_{n\leq x} \Lambda(n) \approx \sum_{n\leq x} 1$ (equiv. to PNT)
6. $\sum_{n\leq x} \mu(n) \approx \sum_{n\leq x} 0$ (equiv. to PNT)

To try and understand $Prob(g(n) = 1)$, we look to the proof that the probability that two integers are coprime is $\frac{1}{\zeta(2)}$.

$$\sum_{\substack{n,m\leq x \\ \gcd(n,m)=1}} 1 = \sum_{m,n\leq x} \sum_{d|\gcd n,m} \mu(d) = \sum_{d\leq x} \sum_{r,s\leq x/d} \mu(d) = \sum_{d\leq x} \mu(d)\lfloor x/d \rfloor^2.$$

The first equality comes from the fact that $\sum_{d|n} \mu(d)$ is 1 if $n = 1$ and 0 otherwise. So we can use it to extract the property $\gcd(n, m) = 1$.

The second equality comes from reversing the order of summation. For all divisors $d \leq x$, we can choose any pair $r, s \leq x/d$ and we know that $dr, ds \leq x$ and $d|\gcd(dr, ds)$.

The third equality then comes from counting the number of pairs r, s, of which there are $\lfloor x/d \rfloor^2$. To continue, we write $\lfloor x/d \rfloor^2 = (x/d)^2 + O(1)$, using big-O notation. Then

$$\sum_{d \leq x} \mu(d) \lfloor x/d \rfloor^2 = x^2 \sum_{d \leq x} \frac{\mu(d)}{d^2} + \sum_{d \leq x} \mu(d) O(1) = \frac{x^2}{\zeta(2)} + Error$$

Trying a similar trick with $g(n) = 1$ gets us to

$$\sum_{\substack{n,m \leq x \\ g(n)=1}} 1 = \sum_{m,n \leq x} \sum_{d|(n)} \mu(d) = \sum_{d \leq x} \sum_{\substack{r \leq x/d \\ d|g(rd)}} \mu(d).$$

But we get stuck because it's not true that all $r \leq x/d$ has $d|g(rd)$. But R.R Hall's ***On the probability that*** n ***and*** $f(n)$ ***are relatively prime III*** goes a bit further, writing

$$\sum_{d \leq x} \sum_{\substack{r \leq x/d \\ d|g(rd)}} \mu(d) = \sum_{d \leq \omega} \mu(d) \sum_{\substack{m \leq x/d \\ g_d(m) = -g(d) \mod d}} 1 + \theta \sum_{\omega < d < x} \sum_{\substack{m \leq x/d \\ d|g(md)}} 1 = S_1 + \theta S_2,$$

where $g_d(m) = g(md) - g(d)$ and $-1 < \theta < 1$. He proceeds to analyze S_1 and S_2. We have $g_d(m) = -g(d) \mod d$ iff $g(md) = 0 \mod d$, so it encodes the same information, but he notes that he introduces $g_d(m)$ over $g(dm)$ as it has the advantage of being additive.

For me, all of this is motivated by the following theorems.

Theorem 1 (Greening) *If $g(n) = 1$, then n is solitary.*

Theorem 2 (Loomis) *If n is odd and $g(n^2)$ is squarefree, then n^2 is solitary.*

Loomis' result came years after Greening's, but prompts a natural conjecture:

Conjecture 1 *With possible conditions on n, if $g(n^k)$ is k^{th}-power-free, then n^k is solitary.*

Note that if $g(n^k)$ is k^{th}-power-free, then $rad(n)|(n/g(n))$. This means that any friend m of n^k must be divisible by all primes that divide n. And it seems this prohibits friends somehow. A search through solitary/friendly numbers showed that

1. For friendly numbers, we often, but not always ($n = 80, 200$), have

$$rad(n) \not| (n/g(n)).$$

2. For all known solitary numbers, we have

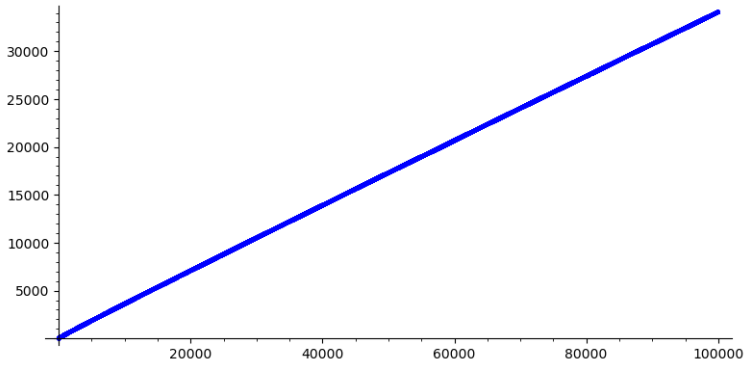
$$rad(n)|(n/g(n)).$$

To rephrase the condition, if $rad(n) \not| (n/g(n))$, then there is some $p|n$ with $\nu_p(n) = \nu_p(g(n))$. Let's define two more arithmetic functions.

$$\alpha(n) = \max_p(\nu_p(n))$$
$$\beta(n) = \min_{p|n}(\nu_p(n))$$
$$\gamma(n) = \gcd_{p|n}(\nu_p(n))$$

Conjecture 2 (Conj 1 Rephrased) *If $\alpha(g(n)) < \gamma(n)$, then n is solitary, possibly with some conditions on n.*

If this conjecture is true, then the density of $\{n \mid \alpha(g(n)) < \gamma(n)\}$ is a lower bound for the density of solitary numbers. Looking up to 10^5, this density seems to be around .34093, with the following growth.



It would be helpful if we could figure out average orders for these new arithmetic functions.

Numerically, we find

$$\frac{1}{x}\sum_{n\leq x}\alpha(n) = 1.70521\ldots$$

$$\frac{1}{x}\sum_{n\leq x}\beta(n) = 1.00918\ldots$$

$$\frac{1}{x}\sum_{n\le x}\gamma(n) = 1.003905\ldots$$

The first two were studied by Ivan Niven in ***Averages of Exponents in Factoring Integers***, Aug 1969. In that paper, he shows this constant (called *Niven's Constant*) can be written explicitly as a sum of zeta functions.

$$\lim_{x\to\infty}\frac{1}{x}\sum_{n\le x}\alpha(n) = \sum_{k=1}^{\infty}\left(1-\frac{1}{\zeta(k)}\right).$$

This would suggest that $Prob[\alpha(n)=k] = \frac{1}{k}\left(1-\frac{1}{\zeta(k)}\right)$. However, taking $k=1$ would give a probability of 1, when we know that probability of an integer being square-free is $\frac{1}{\zeta(2)}$. In fact, $1/\zeta(k)$ is the probability that an integer is k^{th}-power-free.

If $\alpha(n)=k$, then n is $(k+1)^{st}$-power-free, which has a probability of $\frac{1}{\zeta(k+1)}$. But n is not k^{th} power free, which has a probability of $1-1/\zeta(k)$. So then we should have

$$Prob[\alpha(n)=k] = \frac{1}{\zeta(k+1)}\left(1-\frac{1}{\zeta(k)}\right)$$

for $k\ge 1$. So then the average order should be

$$\sum_{k=1}^{\infty}\frac{k}{\zeta(k+1)}\left(1-\frac{1}{\zeta(k)}\right) = 2.42598.$$

Why the discrepancy? The sole difference is the $\zeta(k+1)$ in the denominator rather than k. So there is some overlap? But neither seems to capture the true probability that $\alpha(n)=k$. Strange.

Niven also shows that

$$\sum_{n\le x}\beta(n) = x + \frac{\zeta(3/2)}{\zeta(3)}\sqrt{x} + o(\sqrt{x}),$$

with little-o notation meaning the remainder grows slower than $\sqrt{x}$ asymptotically. This shows the average order of $\beta(n)$ is 1. We'd expect the average order of $\gamma(n)$ to be 1 as well.

I haven't found it in a paper, but it's not hard to show the average order of $\gamma(n)$ is indeed 1.

$$\sum_{n\le x}\gamma(n) = \sum_{k=1}^{\infty}k|\{n\le x \mid \gamma(n)=k\}| = \sum_{k=1}^{\infty}k|\{n\le x^{1/k} \mid \gamma(n)=1\}|.$$

The last equality comes from the fact that if $\gamma(n)=k$, then $\gamma(n^{1/k})=1$. This also means that we only need to study the case of $\gamma(n)=1$.

If $n \leq y$ and $\gamma(n) = 1$, then n is not a square, not a cube, not a fifth power, and so on, over all primes. The largest possible exponent is $log_2(y)$, so

$$\sum_{\substack{n \leq y \\ \gamma(n)=1}} 1 = y - \sum_{p \leq log_2(x)} y^{1/p}$$

Then

$$\sum_{n \leq x} \gamma(n) = \sum_{k=1}^{\infty} k|\{n \leq x^{1/k} \mid \alpha(n) = 1\}| = \sum_{k=1}^{\infty} \left(x^{1/k} - \sum_{p \leq log_2(x^{1/k})} x^{1/(kp)} \right).$$

For all $k \geq 2$, the summand is $O(x^{1/2})$, as is the sum over primes when $k = 1$. Therefore

$$\sum_{n \leq x} \gamma(n) = x + O(x^{1/2}).$$

This proves the average order of $\gamma(n)$ is 1. For $x = 10^5$, the estimate gives 100316 while the true number is 100586.

Attempting the same thing with the average order of $g(n)$ requires us to attempt the count $n \leq x$ with $g(n) = k$ for a fixed k. This is studied in ***On a theorem of Niven*** by Dressler (1974) and ***On the density of some subsets of integers*** by Luca (2007).

In particular, it is shown that the natural density of $\{g(n) = 1\}$ is 0. This hints that the hope of $\{n \mid \alpha(g(n)) < \gamma(n)\}$ providing a non-zero lower bound for the density of solitary numbers is probably hopeless. But we do expect the natural density of solitary numbers to be 0, so it's not unexpected.

And of course, there is a paper ***Some asymptotic formulas in number theory*** by Erdos, 1948, in which he establishes the asymptotics of our function $g(n)$! In fact, he shows that for $f(n) = \sigma(n)$ or $\phi(n)$, we have

$$\sum_{\substack{n \leq x \\ \gcd(n, f(n))=1}} 1 \approx \frac{xe^{\gamma_0}}{logloglogx},$$

where γ_0 is the Euler-Mascheroni constant. What a wonderful result! This probably comes from somewhere similar to Merten's 1874 Product Formula:

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) \approx \frac{e^{\gamma_0}}{logx}$$

He gives two other asymptotics that I'll include here:

$$\sum_{p \leq x} \frac{logp}{p} = logx + O(1)$$

$$\sum_{p \leq x} \frac{1}{p} = log_2 x + \beta + O(1/logx),$$

where $\beta = 0.26149$ is *Merten's Constant*, which can be defined via the Prime Zeta function and the Euler-Mascheroni constant γ_0,

$$\beta - \gamma_0 = \sum_{j \geq 2} \frac{P(j)}{j}$$

The Prime Zeta function is defined as

$$P(s) = \sum_{p} \frac{1}{p^s}$$

and naturally pops up when looking at the logarithm of the zeta function:

$$log\zeta(s) = \sum_{p} -log\left(1 - \frac{1}{p^s}\right) = \sum_{p} \sum_{k=1}^{\infty} \frac{1}{k} \left(\frac{1}{p^s}\right)^k$$

$$= \sum_{k=1}^{\infty} \frac{1}{k} \sum_{p} \frac{1}{p^{ks}} = \sum_{k \geq 1} \frac{P(ks)}{k}$$

Now that we're a bit more versed in arithmetic functions, we can go back to the abundancy index and see what we see.

$$\mathcal{A}(n) = \sum_{d|n} \frac{1}{d} = \prod_{p|n} \left(1 + \frac{1}{p} + \cdots + \frac{1}{p^{\nu_p(n)}}\right) \leq \prod_{p|n} \left(1 + \frac{1}{p} + \ldots\right) = \prod_{p|n} \left(1 - \frac{1}{p}\right)^{-1}$$

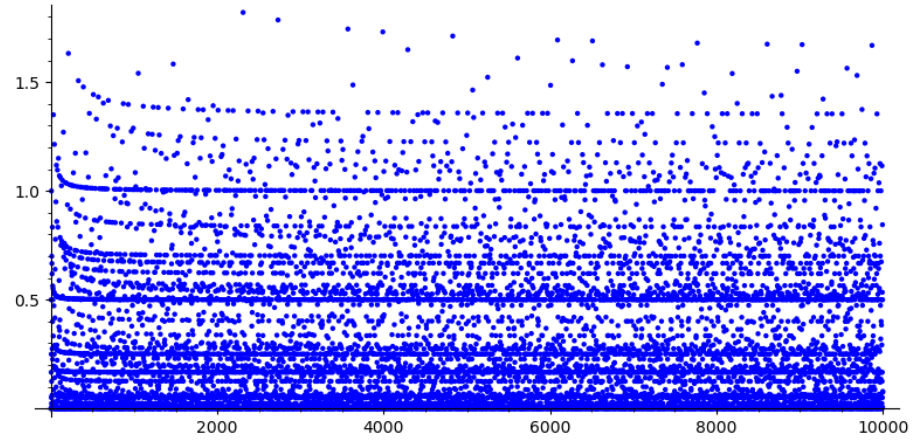
Euler's phi function $\phi(n)$ counts the number of integers less than n coprime to n. From a probability point of view, we can write

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

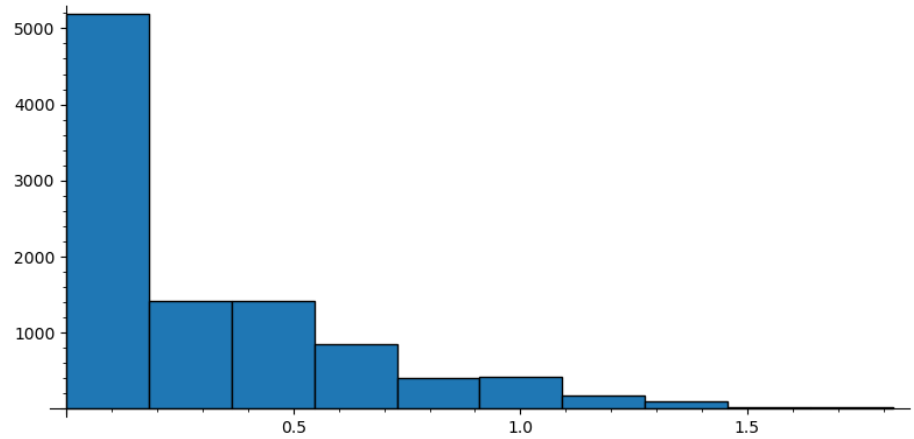
And this gives us

$$\mathcal{A}(n) \leq \frac{n}{\phi(n)}$$

Plotting $\frac{n}{\phi(n)} - \mathcal{A}(n)$ gives



And a histogram of values gives



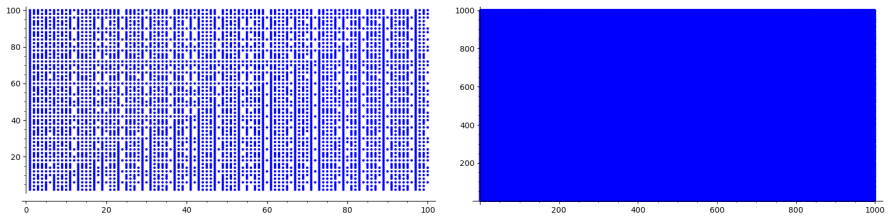
We can use this to try to sieve for friendly numbers. If n and m are friends, then $\mathcal{A}(n) = \mathcal{A}(m)$, so

$$\mathcal{A}(n) < \frac{m}{\phi(m)} \quad \text{and} \quad \mathcal{A}(m) < \frac{n}{\phi(n)}$$

So we reduce our search of friends for n from all of $\mathbb{Z}^+ \setminus \{p^k\}$ to those m with $\mathcal{A}(n) < \frac{m}{\phi(m)}$. Or more generally, we can deduce that n and m being friends implies $\mathcal{A}(n) < m/\phi(m)$ AND $\mathcal{A}(m) < n/\phi(n)$.

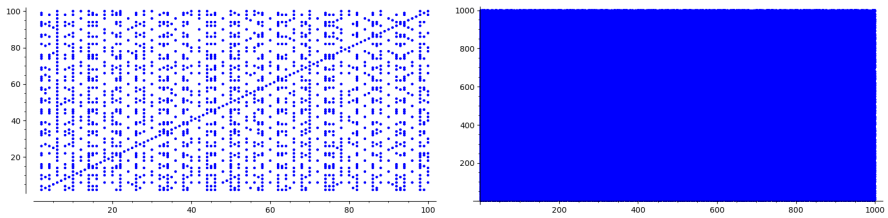
For $x = 100$ and $x = 1000$, we can plot all (n, m) with $0 < n, m \leq x$ and $\setminus < m/\phi(m)$. This is actually a descent reduction in density! The density of the larger plot is

$$7463/12500 \approx 0.59704$$



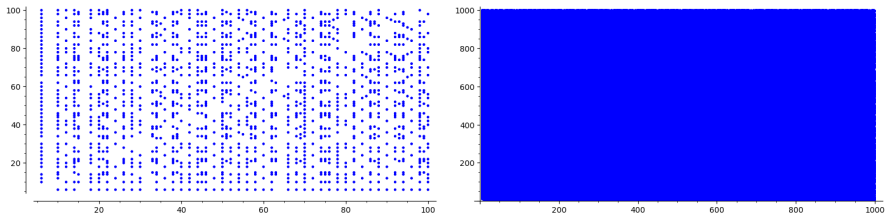
If we only look at the “symmetric core" (only those pairs (n, m) for which (m, n) also satisfied the inequality), we get these. This further reduces the density to

$$194081/500000 \approx 0.388162$$



We can go further by only plotting pairs that do not contain prime powers and are not (n, n). This brings the density for the larger plot to

$$93141/250000 \approx 0.372564$$



This wasn't much of a change, but considering that for prime powers n, we have $\mathcal{A}(n) = 1 + \epsilon$ and $n/\phi(n) = 1 + \theta$ for small ϵ, θ, it makes sense that it'd be common for $\mathcal{A}(n) < m/\phi(m)$ but rare for $\mathcal{A}(m) < n/\phi(n)$.

This suggests that n is more likely to be friendly if $n/\phi(n)$ is larger, as this allows more room for $\mathcal{A}(m)$. And $n/\phi(n)$ is maximized when $\phi(n)$ is minimized. If n has very few integers $m < n$ with $gcd(n, m) = 1$, then n is divisible by a lot of primes. Therefore, $n/\phi(n)$ is maximized when n is a primorial.

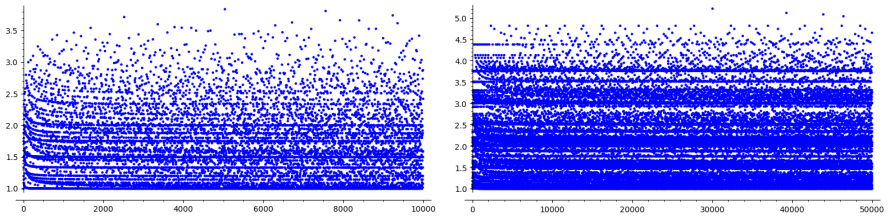
In the note ***6020*** by Andersen, Hickerson, and Greening in the American Mathematical Monthly 1977, they give an explicit lower bound on the density of friendly numbers as

$$\frac{8}{147} = \frac{2}{7}\left[\frac{1}{6} + \frac{1}{28} - \frac{1}{84}\right] \approx 0.0544217687.$$

This comes from the fact that if $\gcd(n, 42) = 1$, then $\mathcal{A}(6n) = \mathcal{A}(28n) = 2\mathcal{A}(n)$. Since the density of n coprime to 42 is $\phi(42)/42 = 2/7$, this shows there is a positive density of numbers n with $\mathcal{A}(6n) = \mathcal{A}(28n)$ and therefore the density of friendly numbers is positive.

To get the specific number, we know that $6n$ is a multiple of 6, the set of which has density $1/6$. Similarly, $28n$ is a multiple of 28 and has density $1/28$. But we overcounted and need to remove any number that is a multiple of both, i.e. any multiple of $lcm(6, 28) = 84$. This has density $1/84$ and the expression follows.

For reference, here are plots for $\mathcal{A}(n)$ and $n/\phi(n)$ respectively.



We can make the inequality $\mathcal{A}(n) < n/\phi(n)$ more exact, but we first need a definition. We say $d|n$ is a *maximal divisor* if for at least one $p|n$, we have $\nu_p(d) = \nu_p(n)$. Meaning the exponent of p in d is as large as it can be. We have

$$\frac{n}{\phi(n)} = \prod_{p|n} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p|n} \sum_{k=0}^{\infty} \frac{1}{p^k} = \sum_{\substack{a \\ rad(a)|rad(n)}} \frac{1}{a}.$$

For such an a, we say that $p|n$ maximally divides a if $\nu_p(a) > \nu_p(n)$. Let $m(a)$ be the number of primes that maximally divide a. For example, if $m(a) = 0$, then $\nu_p(a) \leq \nu_p(n)$ for all $p|n$. In other words, $m(a) = 0$ if and only if a is a divisor of n.

On the other end, if $m(a) = \omega(n)$, then all primes $p|n$ maximally divide a, so $\nu_p(a) \geq \nu_p(n)+1$ for all $p|n$. This allows us to split our sum into three parts.

$$\begin{aligned}\frac{n}{\phi(n)} &= \sum_{\substack{rad(a)=rad(n) \\ m(a)=0}} \frac{1}{a} + \sum_{\substack{rad(a)=rad(n) \\ m(a)=\omega(n)}} \frac{1}{a} + \sum_{\substack{rad(a)=rad(n) \\ 0<m(a)<\omega(n)}} \frac{1}{a} \\ &= \mathcal{A}(n) + \frac{1}{\phi(n)rad(n)} + \sum_{\substack{rad(a)=rad(n) \\ 0<m(a)<\omega(n)}} \frac{1}{a}\end{aligned}$$

The first sum is the sum of reciprocals of divisors of n, and therefore is equal to $\mathcal{A}(n)$. For the second sum,

$$\sum_{\substack{rad(a)=rad(n) \\ m(a)=\omega(n)}} \frac{1}{a} = \prod_{p|n} \sum_{k=\nu_p(n)+1}^{\infty} \frac{1}{p^k} = \prod_{p|n} \frac{1}{p^{\nu_p(n)+1}} \sum_{k=0}^{\infty} \frac{1}{p^k}$$

$$= \frac{1}{nrad(n)} \prod_{p|n} \left(1 - \frac{1}{p}\right)^{-1} = \frac{1}{\phi(n) rad(n)}$$

If $m(a) = 1$, then there is exactly one $p|n$ so that $\nu_p(a) > \nu_p(n)$. So all a can be written as $p^{\nu_p(a)+1-\nu_p(n)}d$, where d is a divisor of n.

Then

$$\sum_{\substack{rad(a)=rad(n) \\ m(a)=1}} \frac{1}{a} = \sum_{p|n} \frac{1}{p^{\nu_p(n)+1}} \sum_{k=0}^{\infty} \frac{1}{p^k} \sum_{d|(n/p^{\nu_p(n)})} \frac{1}{d}$$

$$= \sum_{p|n} \frac{1}{p^{\nu_p(n)+1}} \left(1 - \frac{1}{p}\right)^{-1} \mathcal{A}\left(\frac{n}{p^{\nu_p(n)}}\right) = \sum_{p|n} \frac{\mathcal{A}\left(\frac{n}{p^{\nu_p(n)}}\right)}{p^{\nu_p(n)}(p-1)}$$

$$= \sum_{p|n} \frac{\mathcal{A}\left(\frac{n}{p^{\nu_p(n)}}\right)}{p\phi(p^{\nu_p(n)})}$$

And in general, if $m(a) = k$, then we will sum over all k-tuples $\mathbf{P}$ of primes $p|n$, then factor a as $\mathbf{P}^{\nu_P(n)}$ multiplied by a divisor of $n/\mathbf{P}^{\nu_P(n)}$, and then multiplied by all excess powers of primes in $\mathbf{P}$. So

$$\sum_{\substack{rad(a)=rad(n) \\ m(a)=k}} \frac{1}{a} = \sum_{\mathbf{P}|n} \frac{1}{\mathbf{P}^{\nu_P(n)+1}} \sum_{k=0}^{\infty} \frac{1}{\mathbf{P}^k} \sum_{d|(n/\mathbf{P}^{\nu_P(n)})} \frac{1}{d}$$

The inner sum is $\mathcal{A}(n/\mathbf{P}^{\nu_P(n)})$ and the middle sum is

$$\prod_{p \in \mathbf{P}} \left(1 - \frac{1}{p}\right)^{-1} = \frac{\mathbf{P}^{\nu_P(n)}}{\phi(\mathbf{P}^{\nu_P(n)})}$$

So we get

$$\sum_{\substack{rad(a)=rad(n) \\ m(a)=k}} \frac{1}{a} = \sum_{\substack{\mathbf{P}|n \\ k-tuple}} \frac{\mathcal{A}(n/\mathbf{P}^{\nu_P(n)})}{\mathbf{P}\phi(\mathbf{P}^{\nu_P(n)})}$$

We can check this works by checking $k = 0$, which will be the smallest numbers, and therefore the largest contributors to the sum. Then $\mathbf{P}$ is an empty set of primes, So we get

$$\sum_{\substack{rad(a)=rad(n) \\ m(a)=0}} \frac{1}{a} = \frac{\mathcal{A}(n)}{\phi(1)} = \mathcal{A}(n)$$

And for $k = \omega(n)$, the smallest contribution, we get that $\mathbf{P}$ is all primes dividing n, so

$$\sum_{\substack{rad(a)=rad(n) \\ m(a)=\omega(n)}} \frac{1}{a} = \frac{\mathcal{A}(1)}{rad(n)\phi(n)} = \frac{1}{\phi(n) rad(n)}$$

So we get a final expression

$$\frac{n}{\phi(n)} = \sum_{k=0}^{\omega(n)} \sum_{\substack{\mathbf{P}|n \\ k-tuple}} \frac{\mathcal{A}(n/\mathbf{P}^{\nu_P(n)})}{\mathbf{P}\phi(\mathbf{P}^{\nu_P(n)})}.$$

It's fun to see an example of this. Let $n = 2^3 * 3 * 5 = 120$, so $\frac{120}{\phi(120)} = 15/4$. The righthand side is

$$= \mathcal{A}(120) + \left(\frac{\mathcal{A}(15)}{2\phi(8)} + \frac{\mathcal{A}(40)}{3\phi(3)} + \frac{\mathcal{A}(24)}{5\phi(5)}\right) + \left(\frac{\mathcal{A}(5)}{6\phi(24)} + \frac{\mathcal{A}(3)}{10\phi(40)} + \frac{\mathcal{A}(8)}{15\phi(15)}\right) + \frac{1}{30\phi(120)}$$

$$= 3 + \left(\frac{8/5}{8} + \frac{9/4}{6} + \frac{5/2}{20}\right) + \left(\frac{6/5}{48} + \frac{4/3}{160} + \frac{15/8}{120}\right) + \frac{1}{960}$$

$$= 3 + \frac{7}{10} + \frac{47}{960} + \frac{1}{960}$$

$$= \frac{15}{4}$$

In **The Error Term of the Summatory Euler Phi Function** by N.A. Carella, he covers a lot of great asymptotics. He shows

$$\sum_{n \le x} \frac{1}{\phi(n)} = c_0 + c_1 log(x) + O\left(\frac{logx}{x}\right)$$

and

$$\sum_{n \le x} \frac{\phi(n)}{n} = \frac{1}{\zeta(2)} x + O(1)$$

Most relevant to our previous work, he also gives the nice asymptotic for $n/\phi(n)$:

$$\sum_{n \le x} \frac{n}{\phi(n)} = \frac{\zeta(2)\zeta(3)}{\zeta(6)} x + O(logx)$$

Which makes me want to explore what that coefficient should be interpreted as. To establish these, he gives a few very helpful lemmas on the floor and fractional-part functions.

$$\sum_{n \le x} \left\{\frac{x}{n}\right\} = (1 - \gamma_0)x + O(\sqrt{x})$$

$$\sum_{n \le x} \frac{\mu(n)}{n} \left\{\frac{x}{n}\right\} = O(1)$$

$$\sum_{n \le x} \frac{1}{n} \left\{\frac{x}{n}\right\} = (1 - \gamma_0) logx + a_1 + O(x^{-1/2}).$$

We can use these to determine the average order of the abundancy index $\mathcal{A}(n)$! I've wondered about this for a long time.

$$\sum_{n\leq x}\mathcal{A}(n)=\sum_{n\leq x}\frac{\sigma(n)}{n}=\sum_{n\leq x}\sum_{d|n}\frac{1}{d}$$

$$=\sum_{d\leq x}\sum_{\substack{n\\ d|n}}\frac{1}{d}=\sum_{d\leq x}\frac{1}{d}\left\lfloor\frac{x}{d}\right\rfloor=\sum_{d\leq x}\frac{x}{d^2}-\sum_{d\leq x}\frac{1}{d}\left\{\frac{x}{d}\right\}$$

$$=\zeta(2)x-(1-\gamma_0)logx+a_1+O(x^{-1/2})$$

$$=\zeta(2)x+O(logx)$$

Which shows the average order of $\mathcal{A}(n)$ is $\zeta(2)\approx 1.64493$.

One awesome thing is that the average order of $n/\phi(n)$, $\frac{\zeta(2)\zeta(3)}{\zeta(6)}\approx 1.943596$, looks a lot like what I got for the average order of the product of exponents of integers:

$$\varepsilon(n)=\prod_{p|n}\nu_p(n).$$

For $x=10^6$, we get

$$\frac{1}{x}\sum_{n\leq x}\varepsilon(n)=1.93439.$$

Let's change directions and look at another decomposition of n. Generalizing $rad(n)$, the product of all primes dividing n, let $rad_k(n)$ be the product of all primes p for which $p^k|n$. Then

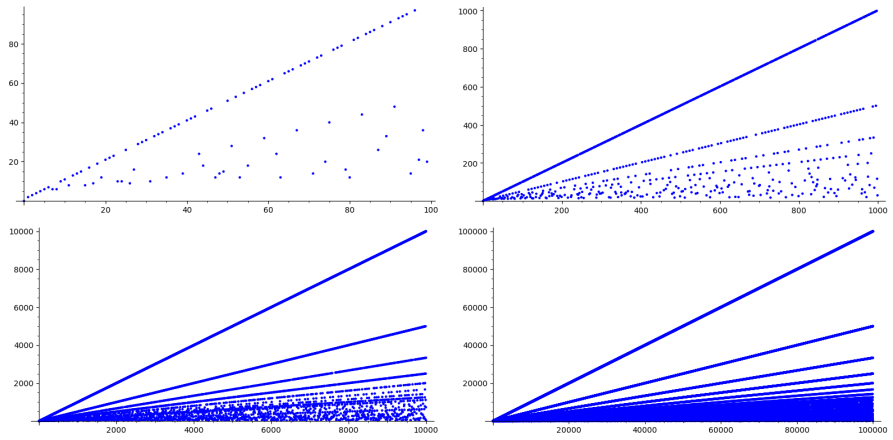
$$n=\prod_{k=1}^{\infty}rad_k(n)$$

since $p^k|n$ for $k=1,2,\ldots,v_p(n)$.

We have $rad_1(n)=rad(n)$ and $rad_{\alpha(n)+1}(n)=1$ for all n. With respect to this decomposition, we'll define a few functions. First, what if we swap addition and multiplication and see how it reacts? Let

$$\ell(n)=\sum_{k=1}^{\alpha(n)}rad_k(n)$$

We'll have more terms if $\alpha(n)$ is higher, but we'll have larger terms if $\omega(n)$ is higher. If n is square-free, $\alpha(n)=1$, then $\ell(n)=rad(n)$. Let's plot for $m=100,1000,10000,100000$.

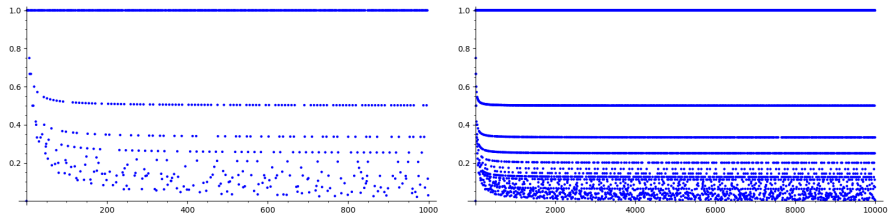


Beautiful! The top line is $\ell(n) = n$. This include square-free integers but in fact includes more. For example, $\ell(4) = 2 + 2 = 4$. More generally, $\ell(p^k) = kp$, which equals p^k only when $p(p^{k-1} - k) = 0$, which means $p^{k-1} = k$. If $k = 2$, then $p = 2$. If $k \geq 3$, then $p^{k-1} > k$ for all primes p, so 4 is actually the only prime power exception.

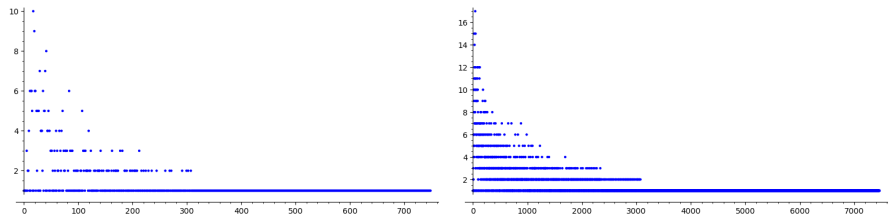
For $x, y > 2$, we have $xy > x+y$, so if $\alpha(n) = 2$, then $n > \ell(n)$. This extends to show that $n = 4$ is the only exception on the top line. So

$$\sum_{\substack{n \leq x \\ n/\ell(n)=1}} 1 \approx \frac{x}{\zeta(2)}$$

The other lines seem to line up with the slopes $1/m$ for $m = 1, 2, 3, \ldots$, but not all n fall onto these lines. In fact, most do not but are simply close to such a slope. Here is a plot of $\ell(n)/n$ for $n \leq x$ with $x = 1000, 10000$.

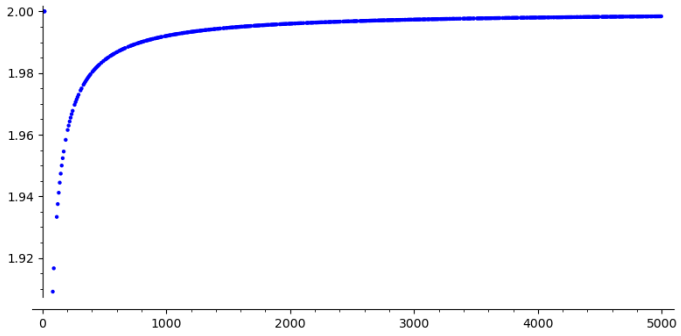


Checking up to $x = 10^5$, it seems that about 75% of $\ell(n)/n$ are distinct. Plotting out the counts of each value $\ell(n)/n$ takes for $x = 1000, 10000$ gives



So counting $n/\ell(n) = 2$ appears to have exactly 2 solutions $n = 16, 18$. But to get a true sense of the density of the line with slope $1/2$, we should count solutions to $|n/\ell(n) - 2| < \varepsilon$.

For example, taking $\varepsilon = 0.1$, we get these new solutions.



The density seems to be about 0.10 but at $x = 10^5$, already exceeds 0.1012. Taking $\varepsilon = 0.5$ makes it take slightly longer to grow, but by $x = 10^5$, is also equal to 0.1012.

A few new numbers are

$$84/\ell(84) = 2 - \frac{1}{11}$$

$$124/\ell(124) = 2 - \frac{1}{16}$$

$$1028/\ell(1028) = 2 - \frac{1}{129}$$

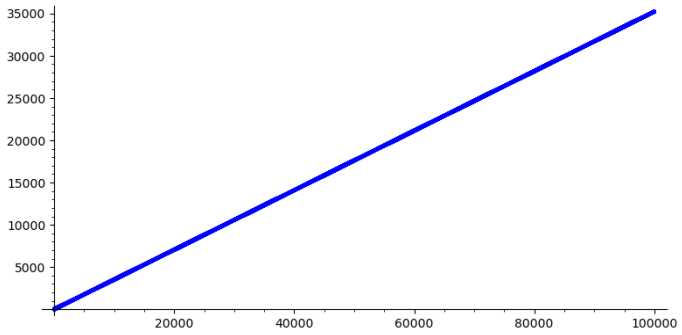
One interesting thing is that we never get a plus sign instead of the minus sign. For $m = 3$, we get numbers like

$$333/\ell(333) = 3 - \frac{3}{38}$$

$$585/\ell(585) = 3 - \frac{1}{22}$$

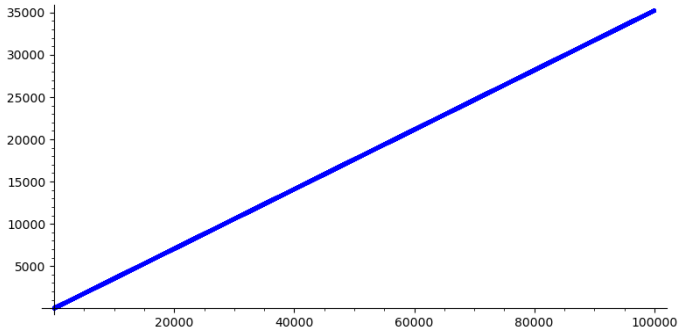
$$2826/\ell(2826) = 3 - \frac{1}{105}$$

To try to determine the average order of $\ell(n)$, we can plot the averages up to $x = 10^5$ as follows:



This suggests that the sum of $\ell(n)$ is approximately quadratic with a coefficient of around 0.35. Note that the sum of n is quadratic with a coefficient of 0.5.

Compare this to the plot of averages of $rad(n)$.



They look exactly the same! What is this coefficient? With more precision, we get 0.3522125, which looks like it might be half of the "carefree constant":

$$\prod_p \left(1 - \frac{1}{p(p+1)}\right) \approx 0.704442200$$

I will have to read some papers to prove this is the constant, but proving that $rad(n)$ and $\ell(n)$ have the same average order is actually not that difficult. Since

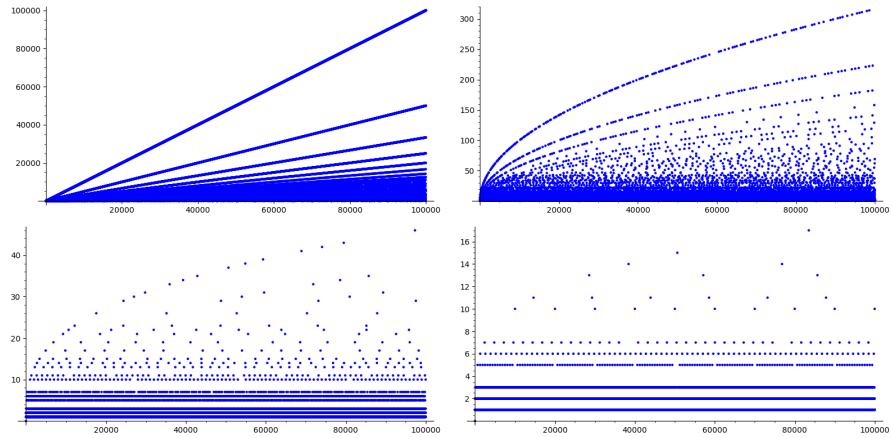
$$\ell(n) = rad(n) + \sum_{k=2}^{\alpha(n)} rad_k(n),$$

we know

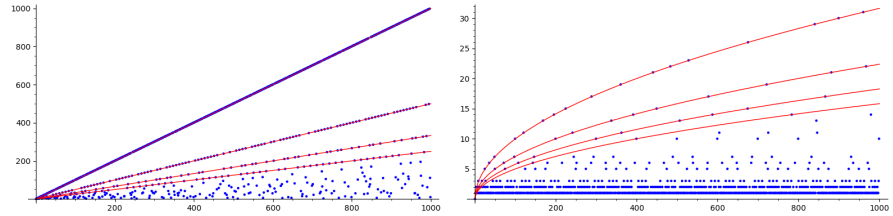
$$\sum_{n\leq x} \ell(n) = \sum_{n\leq x} rad(n) + \sum_{n\leq x} \sum_{k=2}^{\alpha(n)} rad_k(n)$$

$$= \sum_{n\leq x} rad(n) + \sum_{k=2}^{\alpha(n)} \sum_{n\leq x} rad_k(n)$$

Here are plots of $rad_k(n)$ for $k = 1, 2, 3, 4$, for $n \leq 10^5$.



Notice each tend to clump into certain curves. The first has the lines of slope 1, 1/2, 1/3, and so on. The second has curves $(x/m)^{1/2}$ for $m = 1, 2, 3, \ldots$.



So in general, we might guess that $rad_k(n)$ clusters around one of the curves $(n/m)^{1/k}$. Which one? Well if $rad_k(n) = (n/m)^{1/k}$, then

$$m = \frac{n}{rad_k(n)^k} = \prod_{\substack{p|n \\ \nu_p(n)<k}} p^{\nu_p(n)} \prod_{\substack{p|n \\ \nu_p(n)\geq k}} p^{\nu_p(n)-k}$$

So the top lines of each graph are those n with $n = rad_k(n)^k$, meaning that n is the k^{th} power of a square-free integer. So we have the asymptotic

$$\sum_{\substack{n\leq x \\ n=rad_k(n)^k}} 1 = \sum_{\substack{n\leq x^{1/k} \\ n \text{ squarefree}}} 1 = \frac{1}{\zeta(2)} x^{1/k} + O(\sqrt{x}^{1/k})$$

And the average will be $\frac{1}{\zeta(2)} x^{\frac{1}{k}-1}$, which will be $\frac{1}{\zeta(2)}$ for $k = 1$ and 0 for $k \geq 2$.

If we try to explicitly calculate how many n satisfy $\ell(n) = L$ for some fixed L, then we want to count the number of ways to write L as a sum $a_1 + \cdots + a_t$ with $a_i \neq 1$ square-free for all i, and $a_{i+1}|a_i$ for all i. Let's call these *square-free, divisible partitions*.

We can encode the square-free part easily with the generating function:

$$\prod_{n\ squarefree} \frac{1}{1-q^n} = \prod_{k\geq 1} \frac{\mu(k)^2}{1-q^k}$$

The coefficients appear in OEIS A073576. But, they include parts = 1, so we make the small adjustment $\prod_{k\geq 2} \frac{\mu(k)^2}{1-q^k}$. This appears on OEIS A280127.

Surprisingly, the divisible partitions also appear! In A003238, they describe this as the *number of roots trees with n vertices, for which vertices at the same level have the same degree.* They list other interpretations, including ours, and various facts and conjectures on asymptotics. They also link to a MathOverflow post on the sequence.

In particular, Harary and Robinson showed that the generating function $F(x)$ for the sequence (offset by 2) satisfies the functional equation

$$F(x) = x^2 \left(1 + \sum_{n=1}^{\infty} \frac{F(x^n)}{x^n}\right)$$

This looks a lot like the equation for

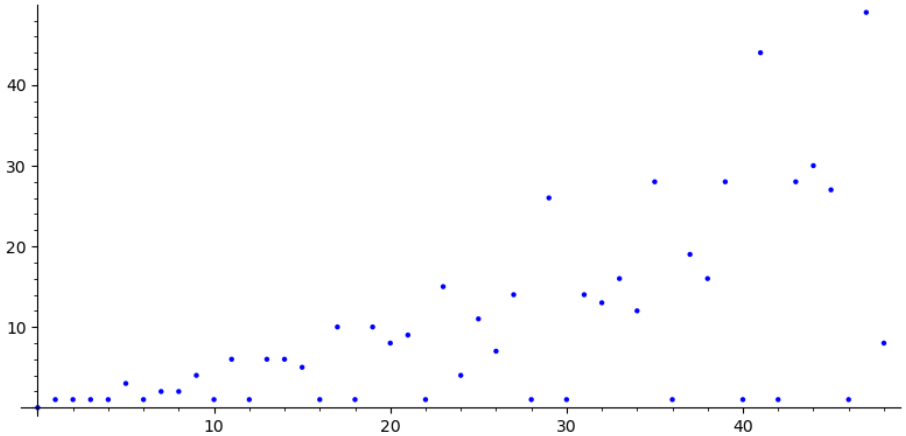
$$\log(\zeta(s)) = \sum_{n=1}^{\infty} \frac{P(ks)}{k}$$

where $P(s)$ is the prime zeta function. Of course, this includes 1 as a part as well. Looking at divisible partitions with parts > 1 gives OEIS A214579.

The number of square-free, divisible partitions does not appear on OEIS. The sequence begins as

```
[0, 1, 1, 1, 1, 3, 1, 2, 2, 4, 1, 6, 1, 6, 6, 5, 1, 10, 1, 10, 8,
9, 1, 15, 4, 11, 7, 14, 1, 26, 1, 14, 13, 16, 12, 28, 1, 19, 16,
28, 1, 44, 1, 28, 30, 27, 1, 49, 8]
```

and here are plots up to 50:



2 $q = -1$ Phenomenon and Arithmetic Functions

The classic example of the $q = -1$ Phenomenon is the q-binomial coefficients. First, we define the q-analogue of an integer

$$n_q = 1 + q + q^2 + \cdots + q^{n-1}.$$

Then we define the q-analogue of the factorial as

$$[n!]_q = n_q(n-1)_q \dots 2_q 1_q.$$

And finally, we can define the q-binomial coefficient as

$$\begin{bmatrix} n \\ m \end{bmatrix}_q = \frac{[n!]_q}{[m!]_q[(m-n)!]_q} = \prod_{i=1}^{m-1} \frac{1-q^{n-i}}{1-q^{i+1}}$$

For example,

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = \frac{[4!]_q}{[2!]_q[2!]_q} = \frac{(1+q+q^2+q^3)(1+q+q^2)(1+q)(1)}{(1+q)(1)(1+q)(1)} = \frac{(1+q)(1+q^2)(1+q+q^2)}{1+q}$$

$$= (1+q^2)(1+q+q^2) = 1+q+2q^2+q^3+q^4$$

The binomial coefficient $\binom{4}{2} = 6$ tells us there are 6 subsets of size 2 of a 4-element set. The q-binomial coefficient tells us about the structure of those subsets under some *group action*: a homomorphism from a group to a group of transformations of some object.

In our case, the objects are the six subsets $\{12, 13, 14, 23, 24, 34\}$ of the set $\{1, 2, 3, 4\}$. A group that acts on these subsets is the finite cyclic group $\mathbb{Z}/4\mathbb{Z}$ which adds 1 to each element, modulo 4. We get an orbit of size 4: $12 \to 23 \to 34 \to 14 \to 12$ and an orbit of size 2: $13 \to 24 \to 13$.

So what does the q-binomial coefficient tell us about this action? If we let $q = -1$, then we get

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_{q=-1} = 1 - 1 + 2 - 1 + 1 = 2.$$

Notice that $(-1)^2 = 1$, and therefore the group action this corresponds to should have order 2, and is therefore the $+2$ action. This splits our subsets into orbits of length 2: $12 \to 34$, $14 \to 23$ and fixed points 13 and 24.

And that is the answer. ***Setting $q = -1$ counts the number of fixed points of some involution.*** This of course leads to ideas: Encode some object you're interested in within a larger framework so that your object represents fixed points. Then use this technique to count your objects.

A more general phenomenon is called *Cyclic Sieving*. We can think about fixed points of other group actions. Indeed, if we look at the $+0$ action, we have 6 fixed points and

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_{q=1} = 1+1+2+1+1 = 6.$$

The $+1$ action leaves no fixed points. This action has order 4 in the group, so we should plug in a 4^{th} root of unity, i.e. $q = i$. This gives

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_{q=i} = 1+i-2-i+1 = 0.$$

This has been studied extensively, with Vic Reiner and Bruce Sagan a few of the leading researchers. What if we looked at a q-analogue of some of these arithmetic functions we've talked about and see if there is any kind of meaning to $q = -1$ or other roots of unity.

Let's start with $\phi(n)$, Euler's totient function. This has the following nice identity

$$\sum_{d|n} \phi(d) = n$$

which can be proven in various ways, but I like expanding the product formula.

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \sum_{d|n} \frac{\mu(d)}{d} = \sum_{d|n} \mu(d) \left(\frac{n}{d}\right)$$

Then applying Mobius Inversion, we get

$$\sum_{d|n} \phi(d) = n$$

Instead of our usual q-analogue of n, why don't we take this one? Define

$$\bar{n}_q = \sum_{d|n} \phi(d) q^d.$$

If $n = p$ a prime, for example, then

$$\bar{n}_q = q + (p-1)q^p$$

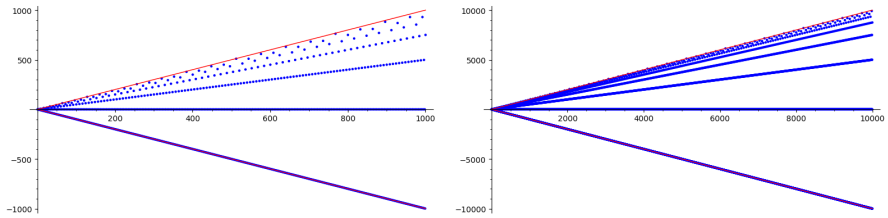
The product of two primes

$$\bar{p_1}_q \bar{p_2}_q = (q+(p_1-1)q^{p_1})(q+(p_2-1)q^{p_2}) = q^2+(p_2-1)q^{p_2+1}+(p_1-1)q^{p_1+1}+(p_1-1)(p_2-1)q^{p_1+p_2}$$

$$= q(q + (p_2-1)q^{p_2} + (p_1-1)q^{p_1} + (p_1-1)(p_2-1)q^{p_1+p_2-1})$$

Very close, but multiplied by q and the last term is off. Which means the idea of multiplication isn't quite preserved, as $\bar{p_1}_q \bar{p_2}_q \neq (\overline{p_1 p_2})_q$.

Anyway, let's plot some values for $q = -1$.



The red lines are $y = \pm x$ and it seems that the values of $\bar{n}$ are concentrated around $\bar{n} = -n$, $\bar{n} = 0$, and then some lines that cluster towards $\bar{n} = n$.

The bottom line is easily explained: $\bar{n} = -n$ if and only if n is odd. So that line has density 0.5 and every number above is even.

Numbers very close to $\bar{n} = n$ will have almost all even divisors. Since 1 is always a divisor, this means $n = 2^k$ has $\bar{n} = n - 1$ for all k, and these will be the closest integers to the line.

The line $\bar{n} = 0$ is very interesting as well. It seems that all even square-free integers n have $\bar{n} = 0$, but the converse is not true, as $\overline{18} = -1+1-2+2-6+6 = 0$. This is because the truth is that if $n = 2k$ with k any odd integer, then $\bar{n} = 0$. This is because

$$\sum_{d|n}(-1)^d\phi(d) = \sum_{d|k}(-1)^d\phi(d) + \sum_{d|k}(-1)^{2d}\phi(2d) = \sum_{d|k}(-1)^d\phi(d) + \sum_{d|k}\phi(2)\phi(d)$$

Since all divisors of k are odd, the first sum is $-k$. And since $\phi(2) = 1$, the second sum is k, so $\bar{n} = 0$. So does setting $q = -1$ count the number of factors of 2 in n?

Let $n = 2^a k$, with k odd. Then

$$\bar{n} = \sum_{d|n}(-1)^d\phi(d) = \sum_{i=0}^{a}\left(\sum_{d|k}(-1)^{2^i d}\phi(2^i d)\right)$$

$$= -k + \sum_{i=1}^{a}\sum_{d|k}\phi(2^i)\phi(d)$$

$$= -k + \sum_{i=1}^{a}2^{i-1}\sum_{d|k}\phi(d)$$

$$= -k + k\sum_{i=1}^{a}2^{i-1}$$

$$= k(-1 + (2^a - 1)) = k(2^a - 2)$$

$$= n - 2k = n\left(1 - \frac{1}{2^{a-1}}\right)$$

In other words, we can interpret $\bar{n}_{q=-1}$ as the number of integers $\leq n$ that are divisible by at most $\nu_2(n)-2$ copies of 2. To explicitly compare this to $\phi(n)$:

$$\phi(n) = \{m \leq n \mid gcd(m,n) = 1\}$$

$$\bar{n}_{q=-1} = \{m \leq n \mid \nu_2(m) < \nu_2(n) - 1\}$$

If we try to isolate an odd prime p and let $n = p^a k$, then we get to

$$\bar{n} = \sum_{i=0}^{a} \left(\sum_{d|k} (-1)^{p^i d} \phi(p^i d) \right) = \sum_{i=0}^{a} \left(\sum_{d|k} (-1)^d \phi(p^i)\phi(d) \right)$$

$$= \sum_{i=0}^{a} \phi(p^i) \sum_{d|k} (-1)^d \phi(d) = p^a \bar{k}$$

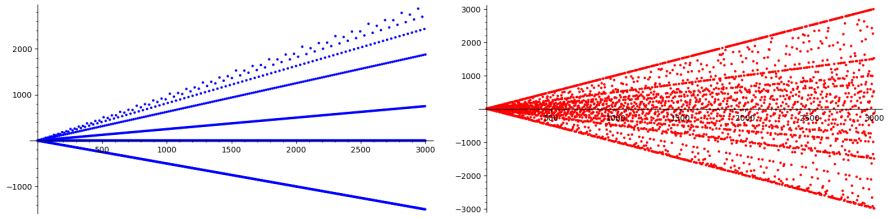
Since we've analyzed the $q=-1$ analogue for an even number, and $\nu_2(k) = \nu_2(n)$, we have

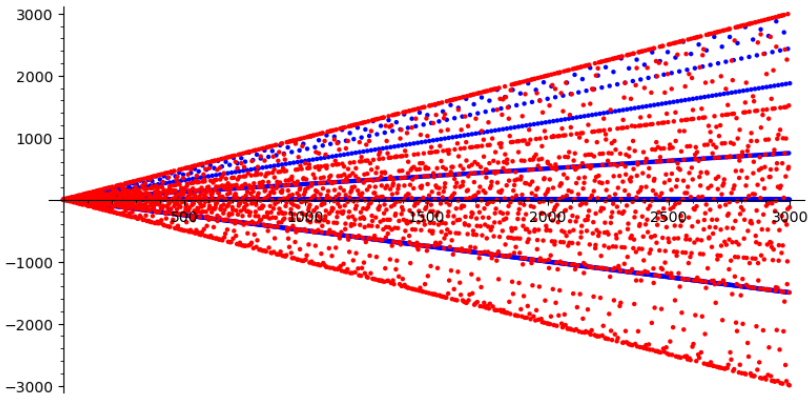
$$\bar{n} = p^a \bar{k} = p^a k \left(1 - \frac{1}{2^{\nu_2(k)-1}}\right) = n \left(1 - \frac{1}{2^{\nu_2(n)-1}}\right)$$

which shows that $q=-1$ truly does isolate the even prime.

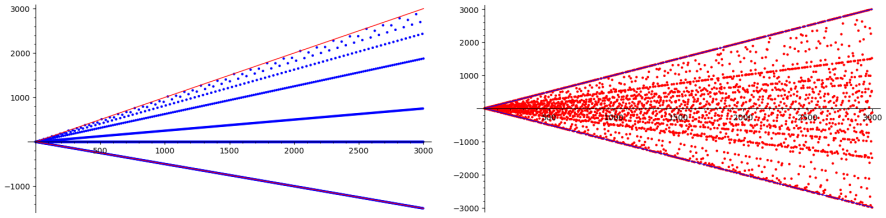
In general, there is a method called *series multisection* to isolate equally-spaced terms in a q-series, but that is a bit different than this.

The following plots are setting $q = i$ and plotting the real parts (blue) and imaginary parts (red) separately and together.

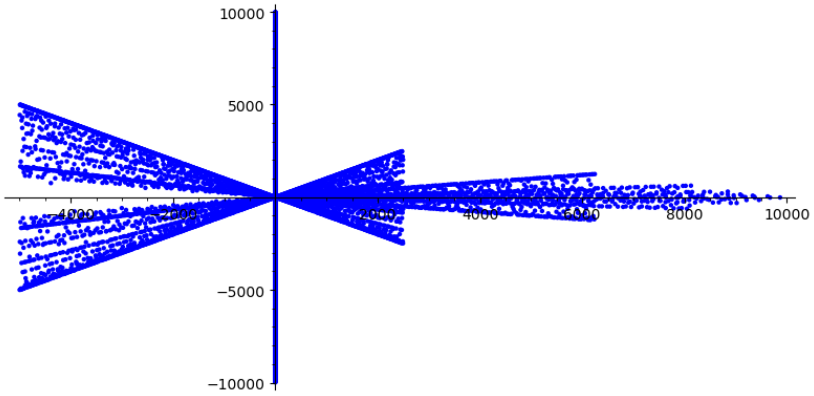




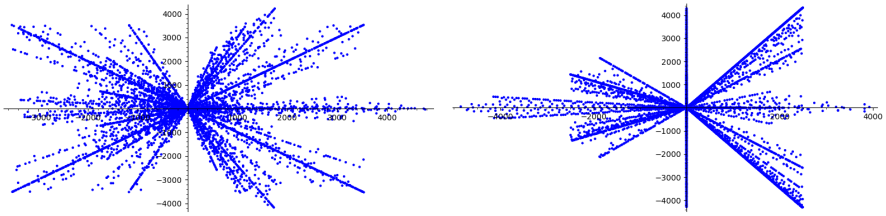
In terms of bounding lines, it seems the real part of $\bar{n}_{q=i}$ has upper bound $y = x$ and lower bound $y = -x/2$. While the imaginary part has bounding lines $y = \pm x$ like $q = -1$. Very interesting!



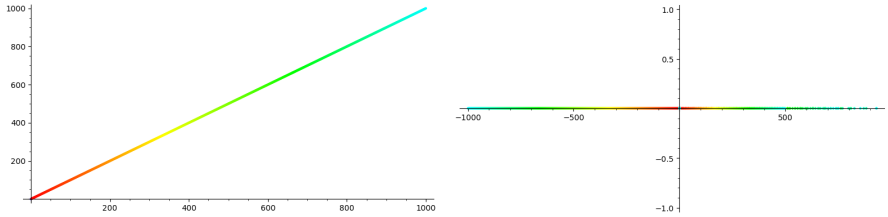
Plotting $\bar{n}_{q=i}$ on the plane gives an amazing graph!



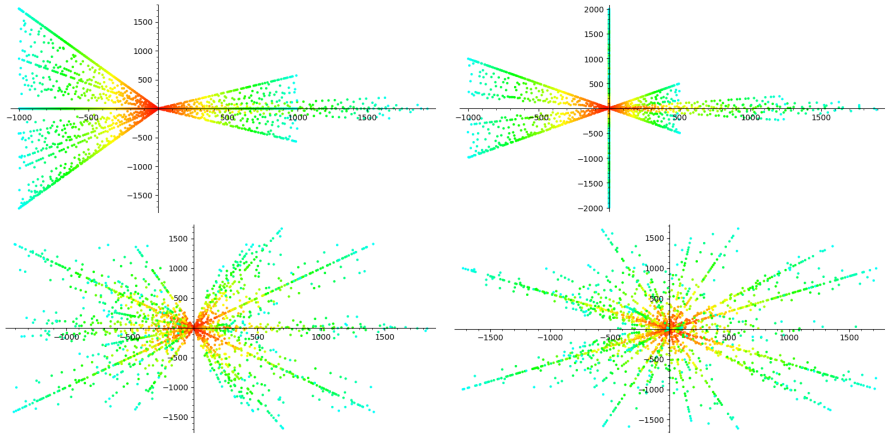
And plotting $q = i^{1/2}$ and $q = i^{1/3}$ respectively gives similarly wonderful images:



We can also plot the points colored on a gradient to show where they're mapped from, though this does take a lot longer to complete. The numbers start at red and transition to light blue. The first two plots are $q = 1, -1$, whose color will increase with n.



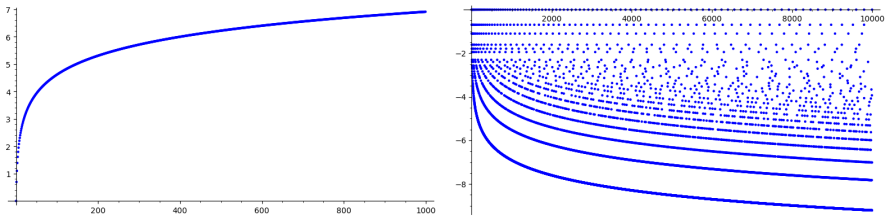
The next four are $q = i^{4/3}, i, i^{1/2}, i^{1/3}$, which are plotted by a complex number but colored linearly in n.

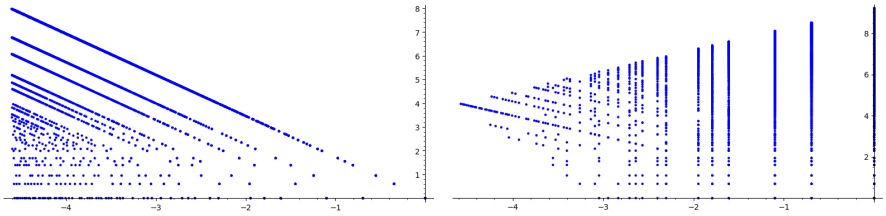


Using the radical decomposition $n = \prod_{k=1}^{\infty} rad_k(n)$, we have another expression

$$log(n) = \sum_{k=1}^{\infty} log(rad_k(n))$$

Let the q-analogue of $log(n)$ be defined by $\sum_{k=1}^{\infty} log(rad_k(n))q^k$. We plot this for $q = 1, -1, i^{4/3}, i$.





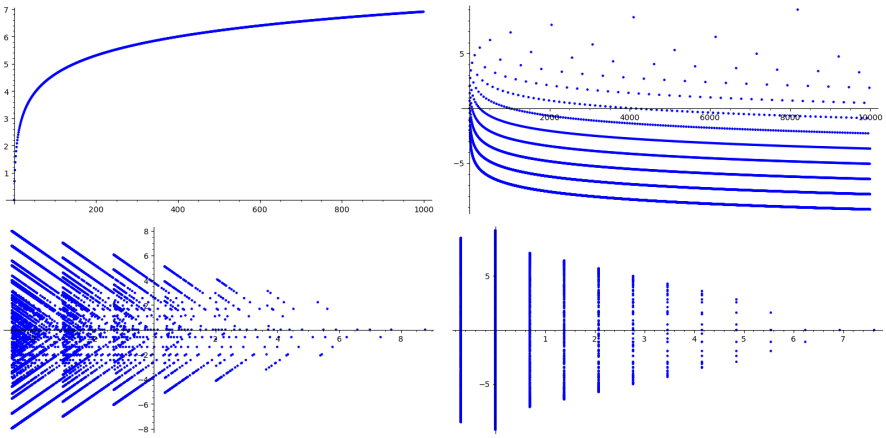
Another q-analogue of $log(n)$ can be defined by the Von Mangoldt function, for which

$$\sum_{d|n} \Lambda(d) = log(n)$$

and so our q-analogue is

$$\sum_{d|n} \Lambda(d) q^k.$$

We plot this for $q = 1, -1, i^{4/3}, i$.



Wild! Why are the real parts for $q = i$ all on certain equally-spaced points? Why the tree-looking pattern for $q = i^{4/3}$? For $q = -1$, is that really a concave down logarithmic curve up top, even with the majority being $-log(n)$ type curves? Let's work with the general q-analogue first:

$$\sum_{d|n} \Lambda(d) q^d = \sum_{p|n} \sum_{k=1}^{\nu_p(n)} log(p) q^{p^k} = \sum_{p|n} log(p)(q^p + q^{p^2} + \cdots + q^{p^{\nu_p(n)}})$$

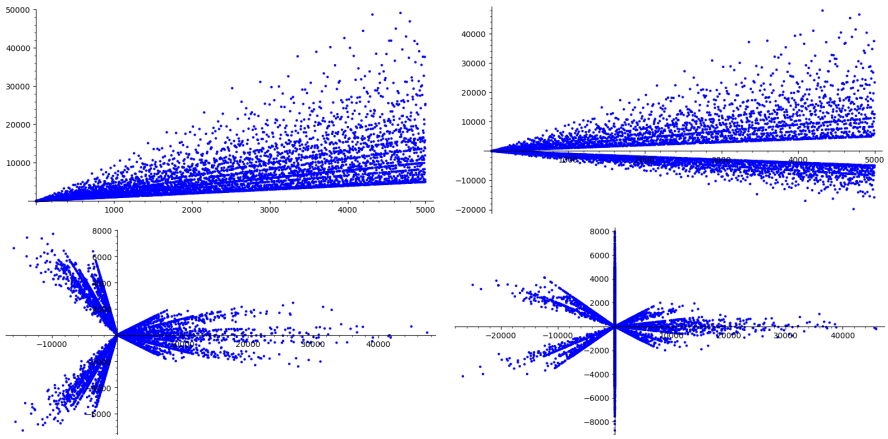
If we let $q = -1$, then we have to consider whether n is even or odd. If $n = 2^{\nu_2(n)} k$ with k odd,

$$\overline{log(n)}_{q=-1} = \sum_{p|n} log(p)(-\nu_p(n)) = \nu_2(n) log(2) - \sum_{p|k} \nu_p(n) log(p)$$

$$= log(2^{\nu_2(n)}) - \sum_{p|k} log(p^{\nu_p(n)}) = -log(k/2^{\nu_2(n)}) = log(4^{\nu_2(n)}) - log(n)$$

So the bottom curve $y = -log(n)$ can be explained by all odd numbers. And the subsequent lines are similar to what we found before, corresponding to how many powers of 2 our number has. This also explains the very sparse logarithmic curve up top. $\overline{log(n)}_{q=-1}$ will be largest when n is a power of 2.

Let's take a turn and look at another arithmetic function, $\sigma(n)$. We plot $\sum_{d|n} \sigma(d)q^d$ for $q = 1, -1, i^{4/3}$, and i.



For $q = -1$, the empty section in the middle doesn't actually seem to be bound by $y = \pm x$, but closer to $y = \pm 0.9x$.

Let's make another switch and consider a q-analogue of the point function using the Mobius function. Recall that $\sum_{d|n} \mu(d) = 0$ for all n except $n = 1$, when it equals 1. So this gives $\bar{1}_q = q$ and for $n > 1$, we get a q-analogue of 0 as

$$\bar{0}_q(n) = \sum_{d|n} \mu(d)q^d$$

This 0 is often also constant. For example, let $q = -1$ and write $n = 2^a k$ with k a non-unity odd integer. Then

$$\bar{0}_{q=-1}(n) = \sum_{d|n} (-1)^d \mu(d) = \sum_{i=0}^{a} \left(\sum_{d|k} (-1)^{2^i d} \mu(2^i d) \right)$$

$$= -\sum_{d|k} \mu(d) + \sum_{i=1}^{a} \sum_{d|k} \mu(2^i)\mu(d)$$

$$= \sum_{i=1}^{a} \mu(2^i) \sum_{d|k} \mu(d) = 0$$

If $n = 2^a$ is a power of 2, then

$$\bar{0}_{q=-1}(n) = \sum_{d|n}(-1)^d\mu(d) = -1 + \sum_{k=1}^{a}\mu(2^k)$$

$$= -1 + -1 + \sum_{d|2^a}\mu(d) = -2.$$

Therefore, this gives us an indicator function for powers of 2.

3 Back to Abundancy

Greening's Criterion says that if $\gcd(n, \sigma(n)) = 1$, then n is solitary. And the reason is because that condition means any friend m of n must be a multiple of n. But if n divides m, then

$$\mathcal{A}(n) = \sum_{d|n}\frac{1}{d} < \sum_{d|m}\frac{1}{d} = \mathcal{A}(m).$$

If $\gcd(n^k, \sigma(n^k))$ is k^{th}-power-free, then we can similarly deduce that any friend m of n^k must be a multiple of $rad(n)$. But this only implies

$$\mathcal{A}(rad(n)) < \mathcal{A}(m),$$

which is already known from the fact that m is a friend of n^k:

$$\mathcal{A}(rad(n)) \leq \mathcal{A}(n) < \mathcal{A}(n^2) < \cdots < \mathcal{A}(n^{k-1}) < \mathcal{A}(n^k) = \mathcal{A}(m)$$

Let's explore the sequence $\mathcal{A}(n^i)$. This sequence forms a strictly increasing, bounded sequence, and therefore has a limit, which we'll call $\overline{\mathcal{A}(n)}$. Since limits commute with products, we have that $\overline{\mathcal{A}(n)}$ is weakly multiplicative, so we can look at prime powers.

If $n = p^k$, then

$$\overline{\mathcal{A}(p^k)} = \lim_{i\to\infty}\mathcal{A}(p^{ki}) = \lim_{i\to\infty}\sum_{j=0}^{ki}\frac{1}{p^j} = \sum_{j=0}^{\infty}\frac{1}{p^j} = \frac{1}{\frac{1}{p}-1} = \frac{p}{p-1} = \left(1-\frac{1}{p}\right)^{-1}.$$

So the powers don't even matter. We could write this as

$$\overline{\mathcal{A}(n)} = \overline{\mathcal{A}(rad(n))}$$

If $n = p_1^{k_1}\ldots p_t^{k_t}$, we will have

$$\overline{\mathcal{A}(n)} = \overline{\mathcal{A}(p_1)}\ldots\overline{\mathcal{A}(p_t)} = \prod_{p|n}\left(1-\frac{1}{p}\right)^{-1} = \frac{n}{\phi(n)}$$

Awesome!! This means that $\mathcal{A}(n^i)$ is a monotonic increasing sequence bounded above by $n/\phi(n)$. This gives a more refined idea of m and n^k being friends implying $\mathcal{A}(m) < n/\phi(n)$. If m and n^k are friends, then

$$\mathcal{A}(n^{k-1}) < \mathcal{A}(m) < \mathcal{A}(n^{k+1})$$

Let's rephrase this in another way. Recall the definitions

$$\alpha(n) = \max_{p|n}(\nu_p(n))$$

$$\gamma(n) = \gcd_{p|n}(\nu_p(n))$$

$$g(n) = \gcd(n, \sigma(n))$$

and our conjecture was that, with possible conditions on n, if $\alpha(g(n)) < \gamma(n)$, then n is solitary. This is supported by $\gamma(n) = 1$ giving a version of Greening's criterion and $\gamma(n) = 2$ giving a version of Loomis' theorem.

So if m and n are friends, then

$$\mathcal{A}(n^{\frac{\gamma(n)-1}{\gamma(n)}}) < \mathcal{A}(m) < \mathcal{A}(n^{\frac{\gamma(n)+1}{\gamma(n)}})$$

Let's test some friendly pairs:

With $n = 6$ and $m = 28$, we have $\gamma(6) = 1$ and $\gamma(28) = 1$, and

$$\mathcal{A}(1) < \mathcal{A}(28) < \mathcal{A}(36)$$

$$1 < 2 < 2.5278$$

$$\mathcal{A}(1) < \mathcal{A}(6) < A(784)$$

$$1 < 2 < 2.254$$

What this means is that if we're looking for friends of n, we only have to search

$$\mathcal{A}^{-1}\left(\mathcal{A}(n^{1-\frac{1}{\gamma(n)}}), \mathcal{A}(n^{1+\frac{1}{\gamma(n)}})\right)$$

And if $\gamma(n)$ is particularly large, then both values are approximately $\overline{\mathcal{A}(n)} = n/\phi(n)$, which suggests higher powers are less likely to be friendly. This raises the question of whether perfect powers tend to be friendly or solitary...someone must have explored this before! Of course, these regions could all be dense, which would go the other direction. This also hints that I will soon cover *abundancy outlaws*.

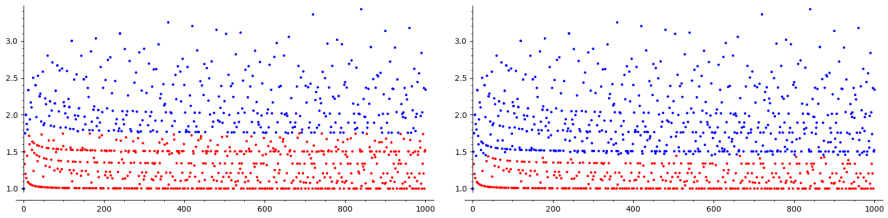
For $n = 2$, we get the interval $\mathcal{A}^{-1}(1, 7/4)$, which seems to have density about 0.60724. Fun enough, we can incorporate a very well-known result in the area. A number n is called *abundant* if $\mathcal{A}(n) > 2$. This is usually stated as $2n < \sigma(n)$. In 1998, Marc Deleglise showed that the density of *abundant* numbers is between 0.2474 and 0.2480. In terms of the abundancy index, this means the interval

$$\mathcal{A}^{-1}(1, 2)$$

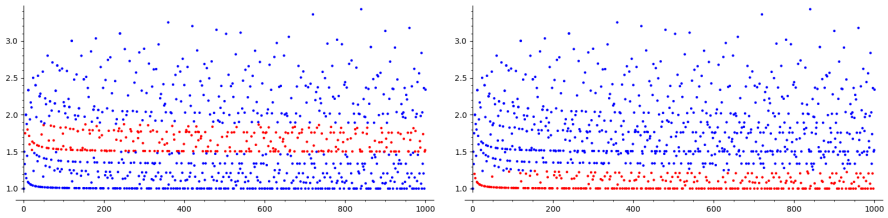
coming from any known perfect number ($n = 6$ for example) has a density of between 0.7520 and 0.7526. I wonder if his methods could be adapted to give a density to more general intervals?

His paper is ***Bounds for the Density of Abundant Integers***. This immediately gives various references to Davenport (1933), Elliott (1979), and Tenenbaum (1995). And he notes in the introduction that this does indeed give the density of $\mathcal{A}^{-1}(1, z)$ for all $z > 1$. Perhaps we can adapt it to estimate the density of $\mathcal{A}^{-1}\left(\mathcal{A}(n^{1-\frac{1}{\gamma(n)}}), \mathcal{A}(n^{1+\frac{1}{\gamma(n)}})\right)$. For brevity, let's call this the *friendly region* of n.

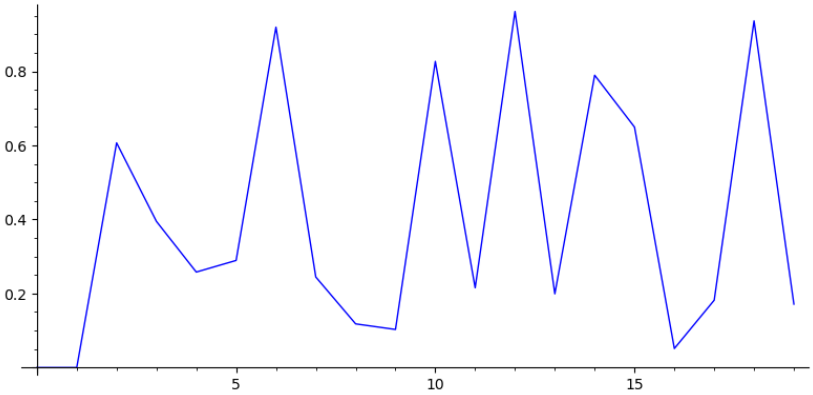
For now, let's plot the previously discussed region for a few different n. Here are $n = 2$ (density ~ 0.60724) and $n = 3$ (density ~ 0.394).



Here are $n = 4$ (density ~ 0.269) and $n = 5$ (density ~ 0.298).



If we plot the densities as a function of n and join the points, we get



4 A new day

A new day, a new realization. Finding the densities of these intervals is very easy with Deleglise's result, since

$$\delta(\mathcal{A}^{-1}(a,b)) = \delta(\mathcal{A}^{-1}(1,b)) - \delta(\mathcal{A}^{-1}(1,a))$$

But with that came the realization that while this is cool (and I still will do it), it probably won't be so helpful as it relies on computing abundancy indices to determine whether an integer is in the pre-image. So we could have just directly checked equality to $\mathcal{A}(n)$. But perhaps, if there is a way to estimate the integers in one of these intervals without explicit computation, this could be an interesting direction.

Consider the following proof that 18 is solitary. First we suppose there is a friend m so that $\mathcal{A}(m) = \mathcal{A}(18) = 13/6 = 2.167$. Then $m = 2^a 3^b \ell$ for some $a, b \geq 1$ and $\ell \geq 1$ with $gcd(6, \ell) = 1$. And since $18 = 2 * 3^2$, we actually require $b < 2$, or 18 would divide m, so $\mathcal{A}(18) < \mathcal{A}(m)$. Then $b = 1$ is a must and we have $m = 2^a 3\ell$. Then

$$\frac{13}{6} = \mathcal{A}(m) = \mathcal{A}(2^a)\mathcal{A}(3)\mathcal{A}(\ell) = \frac{(2^{a+1}-1)}{2^a}\frac{4}{3}\mathcal{A}(\ell) = \frac{2^{a+1}-1}{2^{a-2}3}\mathcal{A}(\ell)$$

and therefore

$$\mathcal{A}(\ell) = \frac{2^{a-3}13}{2^{a+1}-1}.$$

But

$$\frac{2^{a-3}13}{2^{a+1}-1} > \frac{2^{a-3}8}{2^{a+1}-1} = \frac{2^a}{2^{a+1}-1}$$

But remember that $\mathcal{A}(n) = \sigma(n)/n > 1$, but $2^a < 2^{a+1} - 1$ for all $a \geq 1$ and so this means $\mathcal{A}(\ell) < 1$, a contradiction.

This is the way a lot of proofs of solitary numbers go. In fact, even Greening's Criterion is essentially such a proof: If $gcd(n, \sigma(n)) = 1$, then $\mathcal{A}(n) = \sigma(n)/n$ and $m = m'\ell$ where we collect all powers of primes $p|n$ into m' and have $gcd(m', \ell) = 1$. Note that $gcd(n, \sigma(n)) = 1$ means that $n|m'$. Then

$$\mathcal{A}(n) = \mathcal{A}(m) = \mathcal{A}(m'\ell) = \mathcal{A}(m')\mathcal{A}(\ell)$$

so

$$\mathcal{A}(\ell) = \mathcal{A}(n)/\mathcal{A}(m').$$

But since $n|m'$, we have $\mathcal{A}(n) < \mathcal{A}(m')$, which gives a contradiction.

In the case of $n = 18$, we got that the numerator of $\mathcal{A}(\ell)$ was larger than the denominator even though $g(18) = 3$. While another case with $g(n) = 3$ is literally unknown, $n = 15$. In this case, $\mathcal{A}(15) = 8/5$, so any friend must have the form $m = 5^a\ell$ with $gcd(5, \ell) = 1$. Then

$$\frac{8}{5} = \mathcal{A}(m) = \mathcal{A}(5^a\ell) = \frac{5^{a+1}-1}{4(5^a)}\mathcal{A}(\ell)$$

which means

$$\mathcal{A}(\ell) = \frac{5^{a-1}32}{5^{a+1}-1}.$$

Trying the same trick as $n = 18$, we have that

$$\frac{5^{a-1}32}{5^{a+1}-1} > \frac{5^{a-1}25}{5^{a+1}-1} = \frac{5^{a+1}}{5^{a+1}-1}$$

But the last term is greater than 1, so it doesn't help.

So what's different? Let's consider a general case where $n/g(n) = p$. Then $m = p^a\ell$ and $\mathcal{A}(m) = \mathcal{A}(p^a)\mathcal{A}(\ell)$, so

$$\mathcal{A}(\ell) = \frac{\mathcal{A}(n)}{\mathcal{A}(p^a)}$$

So we can deduce the non-existance of ℓ if $\mathcal{A}(n) < \mathcal{A}(p^a)$. If this doesn't hold for small a, we know that taking $a \to \infty$ means $\mathcal{A}(p^a) \to p/\phi(p) = p/(p-1)$, so it might eventually hold. However, we have seen there are n for which this never works, like $n = 15$, where $\mathcal{A}(15) = 8/5 = 1.6$ but $5/\phi(5) = 5/4 = 1.2$. But for $n = 18$, we can immediately deduce it is solitary as

$$\mathcal{A}(18) = 13/6 < 3 = (2/\phi(2))(3/\phi(3)).$$

Attempting total generality, let $p_1, p_2, \ldots, p_t$ be the primes dividing $n/g(n)$. Then

$$m = \ell \prod_{i=1}^{t} p_i^{a_i},$$

where a_i are general exponents. Then

$$\mathcal{A}(\ell) = \frac{\mathcal{A}(n)}{\mathcal{A}(p^{a_1})\mathcal{A}(p^{a_2})\ldots\mathcal{A}(p^{a_1})}.$$

The denominator increases as the exponents increase and tends towards

$$\prod_{i=1}^{t} \frac{p_i}{\phi(p_i)} = \frac{rad(n/g(n))}{\phi(rad(n/g(n)))} = \frac{n/g(n)}{\phi(n/g(n))}$$

And this gives the following theorem.

Theorem 3 *If $\mathcal{A}(n) < \frac{n/g(n)}{\phi(n/g(n))}$, then the exponents of at least one prime $p|(n/g(n))$ in a friend m of n must be bounded.*

With a more refined statement, we might be able to turn this into a theorem for solitary numbers. Take $n = 20$, which is currently unknown but suspected to be solitary. We have $\mathcal{A}(20) = 21/10$ and $10/\phi(10) = 5/2$, so it satisfies the conditions of the theorem. If we try to prove $n = 20$ solitary in the normal fashion, then we'd need $m = 2^a5^b\ell$. But since $a, b \geq 1$, we need $a = 1$. So

$$\frac{21}{10} = \mathcal{A}(m) = \mathcal{A}(5^b 2\ell) = \mathcal{A}(5^b)\frac{3}{2}\mathcal{A}(\ell),$$

so

$$\mathcal{A}(\ell) = \frac{5^{b-1}28}{5^{b+1}-1}.$$

And the numerator is in fact larger than the denominator. The issue here is that while $\mathcal{A}(2^a)$ goes to 2, its exponent is bounded at $a = 1$. So the 3/2 in the denominator instead of 2 gives room for $\mathcal{A}(n) > \mathcal{A}(5^b 2\ell)$ for all b.

In fact, since $\mathcal{A}(n) = 21/10 > \left(\frac{5}{4}\right)\left(\frac{3}{2}\right) = 15/8$, we cannot actually determine that $n = 20$ is solitary from this. As mentioned before, maybe a combination with the theory of abundancy outlaws would make progress here.

But I just realized, that if m is a friend of n, then $m = \ell\frac{n}{g(n)}$ where ℓ is relatively prime to $n/g(n)$, not to n itself. So even when $rad(n) \not| (n/g(n))$, we could still have the primes dividing n appearing in m, via ℓ. So all friends of n must have the form

$$m = \ell \prod_{p|n} p^{a_p}.$$

where $gcd(\ell, n) = 1$, $a_p \neq 0$ for all $p|(n/g(n))$, and we require at least one prime have $a_p < \nu_p(n)$. Then

$$\mathcal{A}(\ell) = \prod_{p|n} \frac{\mathcal{A}(p^{\nu_p(n)})}{\mathcal{A}(p^{a_p})}$$

Term-by-term, $\frac{\mathcal{A}(p^{\nu_p(n)})}{\mathcal{A}(p^{a_p})}$ will be less than 1 if $\nu_p(n) < a_p$, greater than 1 if $\nu_p(n) > a_p$, and equal to 1 if the exponents are equal. Specifically,

$$\frac{\mathcal{A}(p^{\nu_p(n)})}{\mathcal{A}(p^{a_p})} = \frac{\mathcal{A}(p^{\nu_p(n)})}{\mathcal{A}(p^{a_p})} = \frac{p^{a_p}(1 + p + \cdots + p^{\nu_p(n)})}{p^{\nu_p(n)}(1 + p + \cdots + p^{a_p})} = \frac{p^{a_p} + \cdots + p^{\nu_p(n)+a_p}}{p^{\nu_p(n)} + \cdots + p^{\nu_p(n)+a_p}}$$

$$= 1 + \frac{(p^{a_p} + \cdots + p^{\nu_p(n)+a_p}) - (p^{\nu_p(n)} + \cdots + p^{\nu_p(n)+a_p})}{p^{\nu_p(n)} + \cdots + p^{\nu_p(n)+a_p}}$$

$$= 1 + \frac{(p^{a_p} + \cdots + p^{\nu_p(n)-1})}{p^{\nu_p(n)} + \cdots + p^{\nu_p(n)+a_p}}$$

$$= 1 + \frac{p^{\nu_p(n)} - p^{a_p}}{p^{\nu_p(n)+a_p+1} - p^{\nu_p(n)}}$$

$$= 1 + \frac{1 - p^{a_p-\nu_p(n)}}{p^{a_p+1} - 1}$$

So we have

$$\mathcal{A}(\ell) = \prod_{p|n} 1 + \frac{1 - p^{a_p-\nu_p(n)}}{p^{a_p+1} - 1} = \prod_{p|n} \frac{p^{a_p+1} - p^{a_p-\nu_p(n)}}{p^{a_p+1} - 1} = \prod_{p|n} \frac{1 - p^{-(\nu_p(n)+1)}}{1 - p^{-(a_p+1)}}$$

5 Abundancy Outlaws

The paper I originally read in 2014 about the whole friendly number/odd perfect number problem was the Master's Thesis of Jose Arnaldo B. Dris, called ***Solving the Odd Perfect Number Problem: Some Old and New Approaches***, from 2008.

In general, we consider whether a given rational a/b appears as $\mathcal{A}(n)$ for some integer n. We've used the fact that a/b is an abundancy outlaw if $a < b$, but we can go a bit further.

Theorem 4 *If $gcd(m, n) = 1$ and $n < m < \sigma(n)$, then m/n is an abundancy outlaw.*

The above theorem is due to Wiener and Ryan. Laatsch proved that the set of abundancy indices are actually dense in the interval $(1, \infty)$. Although we haven't looked at them much here, obviously a lot of Dris' thesis is about odd perfect numbers, none of which have been found. We do have a large number of properties they must satisfy if they exist.

Even perfect numbers have been well-understood since the time of Euclid, who showed that n is an even perfect number if and only if $n = 2^{p-1}(2^p - 1)$ for a prime p and for $2^p - 1$ prime. In this case,

$$\mathcal{A}(2^{p-1}(2^p - 1)) = \mathcal{A}(2^{p-1})\mathcal{A}(2^p - 1) = \frac{2^p - 1}{2^{p-1}} \frac{2^p}{2^p - 1} = 2$$

My question is about $n = 30$. Its friends seem to involve perfect numbers. Let's factor them:

$$30 = 2 * 3 * 5 = 5 * 2^1 * (2^2 - 1)$$

$$140 = 2^2 * 5 * 7 = 5 * 2^2 * (2^3 - 1)$$

$$2480 = 2^4 * 5 * 31 = 5 * 2^4(2^5 - 1)$$

$$6200 = 2^3 * 5^2 * 31 = 5^2 * 2^3 * (2^5 - 1)$$

$$40640 = 2^6 * 5 * 127 = 5 * 2^6 * (2^7 - 1)$$

If we try to find a friend of 30, we have $\mathcal{A}(m) = 12/5$, so $m = 5^a\ell$ where $6 \not| \ell$. So

$$\mathcal{A}(\ell) = \frac{12(5^a)(4)}{5(5^{a+1} - 1)} = \frac{5^{a-1}48}{5^{a+1} - 1}$$

If $a = 1$, this becomes $48/24 = 2$, and there's our answer. An integer m with $5||m$ is a friend of 30 if and only if $m/5$ is a perfect number.

If $a = 2$, then this becomes $290/124 = 60/31$. If $2^p - 1$ is prime, then

$$\mathcal{A}(2^{p-2}(2^p - 1)) = \mathcal{A}(2^{p-2})\mathcal{A}(2^p - 1) = \frac{2^{p-1} - 1}{2^{p-2}} \frac{2^p}{2^p - 1}$$

$$= \frac{4(2^{p-1} - 1)}{2^p - 1}$$

As $2^p - 1$ is prime, we must have $2^p - 1 = 31$, so $m = 5^2 * 2^3 * (2^5 - 1)$ is the only such friend.

If $a = 3$, then this becomes 15/13. Dris' thesis specifically has a section (4.1.3) on the fraction $(p + 2)/p$ as an abundancy outlaw. BUT, it's just that it's unknown whether or not such a number is an abundancy index or not. In fact, this is equivalent to the existence of an odd perfect number. Judy Holdener proved the following theorem.

Theorem 5 *There exists an odd perfect number if and only if there exists p, n, a, so that $p \equiv a \equiv 1$ mod 4, where p is a prime not dividing n and $\mathcal{A}(n) = \frac{2p^a(p-1)}{p^{a+1}-1}$*

Euler showed that any odd perfect number must be of the form $N = p^a m$, where $p \not| m$ and $p \equiv 1 \equiv a \bmod 4$. The theorem works as $\mathcal{A}(n) = 2/\mathcal{A}(p^a)$ so $\mathcal{A}(np^a) = \mathcal{A}(n)\mathcal{A}(p^a) = 2$.

Holdener and Stanton further proved a wonderful theorem about when $\frac{\sigma(N)+t}{N}$ is an abundancy outlaw. It'll be great to have here:

Theorem 6 *For a positive integer t, let $\frac{\sigma(N)+t}{N}$ be a fraction in lowest terms, and let $N = \prod_{i=1}^{n} p_i^{k_i}$ for primes $p_1, p_2, \ldots, p_n$. If there exists a positive integer $j \leq n$ such that $p_j < \frac{1}{t}\sigma(N/p_j^{k_j})$ and $\sigma(p_j^{k_j})$ has a divisor $D > 1$ such that at least one of the following is true:*

1. *$\mathcal{A}(p_j^{k_j})\mathcal{A}(D) \geq \frac{\sigma(N)+t}{N}$ and $gcd(D, t) = 1$.*
2. *$gcd(D, Nt) = 1$*

then $\frac{\sigma(N)+t}{N}$ is an abundancy outlaw.

This produces a ton of abundancy outlaws:

- For all $m \geq 0$ and $n \geq 1$ and all odd primes p with $gcd(p, \sigma(2^m)) = 1$, then
$$\frac{\sigma(2^m p^{2n+1}) + 1}{2^m p^{2n+1}}$$
is an abundancy outlaw.
- For all primes $p > 3$,
$$\frac{\sigma(2p) + 1}{2p}$$
is an abundancy outlaw.
- If N is an even perfect number, then
$$\frac{\sigma(2N) + 1}{2N}$$
is an abundancy outlaw.

- Let M be an odd integer and $p, a, t \geq 1$ be odd integers such that $p \not| M$ and $p < \frac{1}{t}\sigma(M)$. Then if
$$\frac{\sigma(p^a M) + t}{p^a M}$$
is in lowest forms, it is an abundancy outlaw.

- For primes p, q with $q > 3$ and $p < q$ and $gcd(p+2, q) = gcd(p, q+2) = 1$, then
$$\frac{\sigma(pq) + 1}{pq}$$
is an abundancy outlaw.

This gives us a different strategy in attempting to prove that a number is solitary. Take $n = 20 = 2^2 5$ for which $\mathcal{A}(20) = 21/10 = \frac{\sigma(10)+3}{10}$

Does the theorem apply? Well, $2 < \frac{1}{3}\sigma(5) = 2$ and $5 < \frac{1}{3}\sigma(2) = 1$, so the theorem doesn't apply. However, maybe it could apply after some steps of the usual solitary algorithm. If $m = 5^a 2\ell$ is a friend of $n = 20$, then

$$\mathcal{A}(\ell) = \frac{\frac{21}{10}}{\mathcal{A}(5^a)\mathcal{A}(2)} = \frac{21 * 5^a(4)(2)}{10 * (5^{a+1} - 1) * 3} = \frac{5^{a-1}28}{5^{a+1} - 1}$$

Since $5^{a+1} - 1 \equiv 0 \bmod 4$, we'll be able to cancel out a factor of 4. And $5^{a+1} - 1 \bmod 7$ cycles as $3, 5, 1, 2, 0, 4, 3, \ldots$ for $a = 1, 2, 3, 4, \ldots$.

Then we have
$$\mathcal{A}(\ell) = \frac{5^{a-1}7}{4^{-1}(5^{a+1} - 1)}$$

Our previous strategy would be to iterate until the numerator is smaller than the denominator, but this doesn't actually work here. The more general strategy would be to iterate until we hit a known abundancy outlaw. Then no such ℓ could exist and the whole thing collapses to n being solitary.

For $a = 1$, we get $\mathcal{A}(\ell) = 7/6$, which is an abundancy outlaw by Theorem 4. For $a = 2$, we get $\mathcal{A}(\ell) = 35/31$, which is of the form $\frac{\sigma(31)+3}{31}$, and unknown. But we would need $\ell = 31^b \ell_1$, so $35/31 = \mathcal{A}(\ell) = \mathcal{A}(31^b)\mathcal{A}(\ell_1)$. Then

$$\mathcal{A}(\ell_1) = \frac{35(31^{b-1})(30)}{31^{b+1} - 1} = \frac{2 * 3 * 5^2 * 7 * 31^{b-1}}{31^{b+1} - 1}$$

For $b = 1$, this gives $\mathcal{A}(\ell_1) = \frac{35}{32}$, and since $\mathcal{A}(\ell_1)$ is in reduced form, Theorem 4 tells us it is an abundancy outlaw.

And what does this tell us? That $b \neq 1$. In essence, we're doing a depth-first search. Thinking of this "***abundancy sieve***" as a depth-first search will be helpful when coding it.

For now, let's continue. Suppose $b = 2$, then $\mathcal{A}(\ell_1) = 1085/993$ and since $\sigma(993) = 1328$, Theorem 4 applies to tell us no such ℓ_1 exists. So $b \neq 2$.

For $b = 3$, we have $\mathcal{A}(\ell_1) = 33635/30784$, and $\sigma(30784) = 67564$, so Theorem 4 tells us $b \neq 3$. For $b = 4$, we have $\mathcal{A}(\ell_1) = 208537/190861$ and $\sigma(190861) = 208224$, which is surprisingly close to the numerator. We have

$$\mathcal{A}(\ell_1) = \frac{\sigma(190861) + 313}{190861}$$

Let's see whether Holdener and Stanton's result applies. We have $N = 190861 = 11 * 17351$ and $t = 313$. We must check if $11 < \frac{1}{313}\sigma(17351) \approx 55$, so we're good! We want a divisor D of $\sigma(11) = 12$ so that $gcd(D, 17351 * 313) = 1$. As both are primes, we could choose any divisor. So by Theorem 6, no such ℓ_1 can exist.

Continuing this process is what get results that look like "any friend of 20 must be divisible by at least $715728775 = 5^2 * 31^5$."

Let's increment a again and let $a = 3$. Then $\mathcal{A}(\ell) = \frac{175}{156}$ and since $\sigma(156) = 392$, Theorem 4 tells us that no such ℓ can exist. For $a = 4$, we have $\mathcal{A}(\ell) = 875/781$. This time, $\sigma(781) = 864$, so

$$\mathcal{A}(\ell) = \frac{\sigma(781) + 11}{781}$$

We have $781 = 11 * 71$ and $t = 11$, so we need $11 < \frac{1}{11}\sigma(71) \approx 6.5$, which we don't have. And this means we can't rule out $a = 4$ unless we go another step. But in this case, any such ℓ must be of the form $11^b 71^c \ell_1$. Then

$$\mathcal{A}(\ell_1) = \left(\frac{875}{781}\right) \frac{11^b(10)(71^c)(70)}{(11^{b+1} - 1)(71^{c+1} - 1)} = \frac{11^{b-1}71^{c-1}612500}{(11^{b+1} - 1)(71^c - 1)}$$

And obviously this gets tedious. In essence, we can picture this as a rooted tree with $\mathcal{A}(n)$ as the root and we connect to it the implied $\mathcal{A}(\ell)$ for various choices of exponents. Any of these that are known abundancy outlaw (by coding all the tests) are removed. Now that I think about it, this may not even be a tree. Regardless, the resulting graph corresponds to possible friends of n that pass all coded abundancy outlaw tests. If we remove at least one value in each path from $\mathcal{A}(n)$, then we'll be left with a finite graph, and only a finite amount of numbers to check to deduce n is solitary.

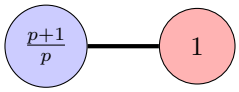
Let $AS(n)$ be this graph. We build it by starting with $\mathcal{A}(n)$ and for each $p|(n/g(n))$, we have that a possible friend looks like $m = \ell \prod_{p|n} p^{a_p}$ for some exponents a_p with $a_p \neq 0$ for all $p|(n/g(n))$. Then

$$\mathcal{A}(\ell) = \prod_{p|n} \frac{\mathcal{A}(p^{\nu_p(n)})}{\mathcal{A}(p^{a_p})}$$

The corresponding vertices are these abundancy indices for all choices of exponents a_p with $a_p \geq \nu_p(n/g(n))$. If we test it to be an abundancy outlaw, we'll color it red. The node where $a_p = \nu_p(n)$ for all $p|n$ will be colored red and hence

$AS(n)$ will not contain any choices where $a_p \geq \nu_p(n)$ for all $p|n$, with at least one strictly bigger. This boundary node will be $\mathcal{A}(\ell) = 1$.

So really our graph is a graph $AS(T, n)$ where T is a collection of abundancy outlaw tests. Let's do an example T is just the obvious test of $\mathcal{A}(\ell) \leq 1$. Let $n = p$ a prime. Then we have a single node $\mathcal{A}(p) = (p+1)/p$, and a friend of the form $p^a\ell$ gives a path $\mathcal{A}(\ell) = \frac{(p+1)p^a(p-1)}{p(p^{a+1}-1)}$ for $a \geq 1$. But for $a = 1$, we have $\mathcal{A}(\ell) = 1$, so we get that $AS(p)$ looks like

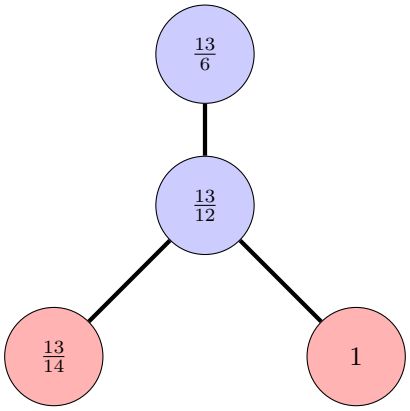


In fact, for any integer n with $\gcd(n, \sigma(n)) = 1$, we get that $m = \ell \prod_{p|n} p^{a_p}$ where $a_p \geq \nu_p(n)$. So $\mathcal{A}(\ell) \leq 1$, and $AS(n)$ consists of just two vertices.

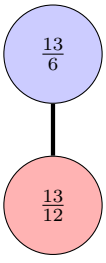
Let's consider $n = 18$, for which $\gcd(n, \sigma(n)) \neq 1$. Then $\mathcal{A}(18) = 13/6$, so $m = 2^a * 3^b * \ell$, but remember that if $b = 2$, then $n|m$, so we'd get an $\mathcal{A}(\ell) < 1$. This gives a single red vertex for $a = 1, b = 2$. So setting $b = 1$, we get

$$\mathcal{A}(\ell) = \frac{13 * 3 * 2^a}{6 * 4 * (2^{a+1} - 1)} = \frac{13 * 2^{a-3}}{2^{a+1} - 1}.$$

As $13 < 16$, this is less than 1 for $a \geq 2$. For $a = 2$, we have $\mathcal{A} = 13/14$ and for $a = 1$, we have $\mathcal{A}(\ell) = 13/12$. Therefore, $AS(18)$ is



And note that if T contains the condition "$\mathcal{A}(\ell) = a/n$ with $n < a < \sigma(n)$ and $\gcd(a, n) = 1$," then the graph would have two less vertices:



So we pose a general question:

Question 2 *For a set T of abundancy outlaw tests, describe the graph-theoretic properties of $AS(T, n)$, including the number of vertices, edges, the diameter, girth, chromatic number, clique number, genus, critical group, and of course whether or not this is actually a tree.*

Another question we can pose is how different choices of T relate to each other.

Question 3 *If we can deduce n is solitary using some set of tests T_1, can we deduce it using another set T_2?*

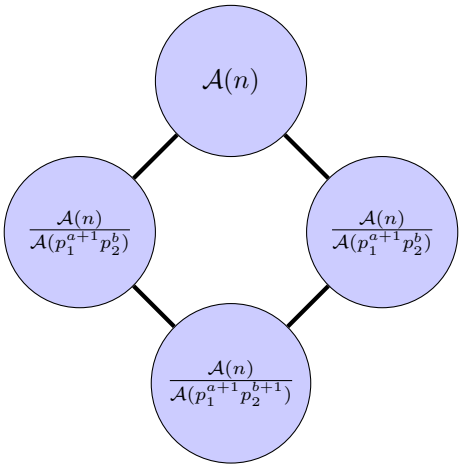
Simplified to the previous case, this comes down to asking whether $\mathcal{A}(\ell) = a/n$ with $n < a < \sigma(n)$ and $\gcd(a, n) = 1$ implies that there exists some ℓ' so that $\mathcal{A}(\ell') \leq 1$.

Well suppose we're looking at $AS(T, n)$ where T has both conditions and n has the vertex $\mathcal{A}(\ell) = a/n$ for such an a, then $\mathcal{A}(\ell) < \frac{\sigma(n)}{n} = \mathcal{A}(n)$. So

$$\mathcal{A}(\ell') = \frac{\mathcal{A}(\ell)}{\mathcal{A}(\prod_{p|n} p^{a_p})} < \frac{\mathcal{A}(n)}{\mathcal{A}(\prod_{p|n} p^{a_p})} \leq 1$$

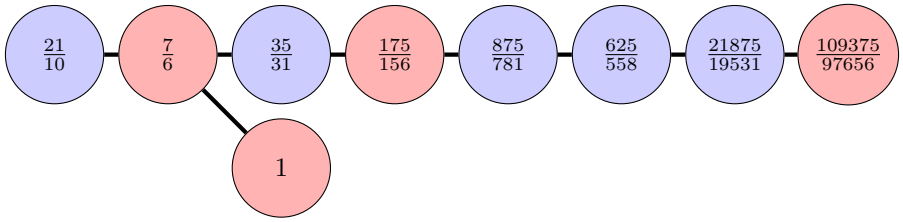
So in this case, T with both conditions and $T' = \{\mathcal{A}(\ell) \leq 1\}$ are basically equivalent. And thinking of "for each ℓ", what is the degree of a vertex in $AS(T, n)$? Each vertex from the root $\mathcal{A}(n)$ comes from $m = \ell \prod_{p|n} p^{a_p}$ and each path comes from varying a_p for a specific p. Which I believe actually shows $AS(T, n)$ is not a tree for all n. Because we can reach $p_1^{a+1} p_2^{b+1} \ell$ by incrementing $p_1^a p_2^b$ in two different ways.

In particular, if n has at least two prime factors, then we'll have



provided the middle two aren't red by T.

Let's do a fun one and see what graph we get for $n = 20$. Our previous work establishes this part of $AS(T, 20)$, where T contains Theorem 4 and Theorem 6.



But remember the idea of the "***abundancy sieve***" is that this first level may not be enough. So let's extend the definition of $AS(T,n)$ to any rational number $AS(T,a/b)$ with $b \neq 1$ by going through the same process beginning with a/b. So we interpret $AS(T,n) := AS(T,\mathcal{A}(n))$.

Then we consider $AS(T,n)$ to be the *spine* of a larger graph $\overline{AS}(T,n)$ which glues to each vertex $\mathcal{A}(\ell)$ of $AS(T,n)$ the corresponding graph $AS(T,\mathcal{A}(\ell))$. And the purpose is clear: If any non-root vertex of $\overline{AS}(T,n)$ is an abundancy index, then n has a friend, which can be explicitly determined via its path to the root.

For coding purposes, we'll compute our graph up to a depth of d from the root $\mathcal{A}(n)$. So we'll define for a rational r the function $ASr(T,r,d)$ where we extract the denominator and compute the primes that compute it. We then initialize a graph and define a set that will become its edge set.

```
def ASr(T,r,d):
  den = r.denominator()
  P = list(factor(den))
  om = len(P)
  G = Graph()
  E = []
```

Then we take r and consider some ℓ with $\mathcal{A}(\ell) = r$. This means that ℓ is a multiple of den, so $\ell = \ell' \prod_{p\in P} p^{a_p}$ where $a_p \geq \nu_p(den)$ and $\gcd(\ell', den) = 1$. So

$$\mathcal{A}(\ell') = \frac{r}{\prod_{p\in P} \mathcal{A}(p^{a_p})}.$$

So the first vertex, where $a_p = \nu_p(den)$ for all p, is $r/\mathcal{A}(den)$, which we make its own function.

```
def next_node(r):
    return r/s(-1,r.denominator())
```

We then add the edge (r,next_node(r)) to E and iterate this until we have $d+1$ vertices. If we reach an integer, then we'll repeat that forever, so we break the loop. Otherwise, we add the edge and continue.

```
E = [(r,next_node(r))]
    for i in range(d-1):
        if E[-1][1] in ZZ:
```

```
            break
        else:
            E.append((E[-1][1],next_node(E[-1][1])))
    G.add_edges(E)
    return G
```

For example, if we go to depth 10 with $n = 20$, we get vertices

$$[21/10, 7/6, 7/12, 1/4, 1/7, 1/8, 1/15, 1/24, 1/60, 1/168, 1/480]$$

which clearly goes to less than 1 very quickly. In fact, the denominators form a sequence of iterating σ starting with $\sigma(4) = 7$. This is because if $\mathcal{A}(\ell) = 1/a$ for some integer a, then the next will be $(1/a)(\mathcal{A}(a))^{-1} = (1/a)(a/(\sigma(a))) = 1/\sigma(a)$.

That's fun, but anyway, we'd end out process when we encountered a vertex that failed a test in T anyway (either 7/6 or 7/12)

6 Extremal Graph Theory

Graph Theory in particular has always been one of my favorite areas of math. In particular, there are many theorems in extremal graph theory with wonderful proofs and interesting applications to other areas of math. Before going further with forming a graph to address the abundancy problem, let's detail some nice results in this area.

Possibly the most popular such theorem is the *handshaking lemma*. This says that if $G = (V, E)$ is a graph on n vertices and m edges, then

$$\sum_{v \in V} deg(v) = 2m$$

Theorem 7 *Let G be a simple graph with no triangles. Then there exists a partition $V = X \bigcup Y$ into disjoint sets so that for all $x \in X$, we have $deg(x) < |Y|$ and for all $y \in Y$, we have $deg(y) < |X|$.*

If we fix a graph H, we can ask about the maximal number of edges a graph on n vertices can have before we're guaranteed to have a copy of H. This situation was studied by Turan in 1941 with generalizations given by Erdos-Stone a few years later.

Theorem 8 (Turan's Theorem) *If $H = K_r$ is the complete graph on r vertices, then the maximal number of edges in a K_r-free graph on n vertices is*

$$\left(1 - \frac{1}{r-1}\right)\frac{n^2}{2}$$

Theorem 9 (Erdos-Stone Theorem) *If H is a simple non-bipartite graph on n vertices, then the maximal number of edges in an H-free graph on n vertices is*

$$\left(1 - \frac{1}{\chi(H)-1}\right)\frac{n^2}{2}$$

Both are sometimes written more explicitly with a $+o(1)$ term inside the parentheses. Though simple, the following theorem is another that gives a bound on the size of edge set for certain graphs.

Theorem 10 *Let G be a simple planar graph with at least 3 vertices. Then $|E| < 3|V| - 6$.*

A more specific area with a massive amount of wonderful results is Ramsey Theory. The basic theorem in this area is that there exists a number $R(r, s)$ such that any 2-coloring of the edges of a complete graph on $R(r, s)$ vertices will contain a red clique on r vertices or a blue clique on s vertices. Proving this relies on the fact that

$$R(r, s) \leq R(r, s-1) + R(r-1, s)$$

and the handshaking lemma.

A more general (and often more useful) version is with c colors.

Theorem 11 (Ramsey's Theorem) *There exists a number $R(n_1, \ldots, n_c)$ so that any c-coloring of the complete graph on $R(n_1, \ldots, n_c)$ vertices must contain a clique of size n_i which is monochromatic of color i*

The proof for the general case procedes pretty much in the same way as the 2-color case, but uses the fact that

$$R(n_1, \ldots, n_c) \leq R(n_1, \ldots, n_{c-2}, R(n_{c-1}, n_c))$$

In fact, you can be even more general, but we'll stop here. Naturally, Erdos proved many of the important results of this area. For exact values, we have very few. And for most values, the bounds get pretty bad. It's easy to see that $R(r, s) = R(s, r)$ and $R(1, n) = 1$.

It's also pretty quick to see that $R(2, n) = n$, because $R(2, n)$ means we either have a monochromatic clique of size n or a "clique of size 2", which is an edge. So if we have $n - 1$ vertices, we just color all edges one color. If we had n vertices, this would produce a K_n. But if we try to fix this by swapping the color of a single edge, we get a K_2. The following is all other values we know exactly:

$$R(3,3) = 6 \quad R(3,4) = 9 \quad R(3,5) = 14 \quad R(3,6) = 18 \quad R(3,7) = 23$$

$$R(3,8) = 28 \quad R(3,9) = 36 \quad R(4,4) = 18 \quad R(4,5) = 25$$

A modern leading researcher in this area is Brendan McKay.

Applications of Ramsey's Theorem are far and wide. For example, here is a problem from **A Course in Combinatorics** by J.H. van Lint and R.M. Wilson.

Problem 1 *Prove that for all integers $r \geq 1$, there is a minimal number $N(r)$ with the following property. If $n \geq N(r)$ and the integers in $\{1, 2, \ldots, n\}$ are colored with r colors, then there are three elements x, y, z (not necessarily distinct) with the same color and $x + y = z$. Determine $N(2)$ and show $N(3) > 13$.*

This sounds very complicated on its own, but with the perspective of Ramsey theory, this is actually fairly simple. We claim that $R(3,3,\ldots,3) \geq N(r)$, where we have r 2s, which shows that $N(r)$ exists. Let $n = R(3,\ldots,3)$ and $c : \{1,\ldots,n\} \to \{1,\ldots,r\}$ be a fixed coloring of the vertices of K_n. Label the edge (i,j) in K_n with $c(|i-j|)$.

Then Ramsey's Theorem tells us that there exists a monochromatic triangle in K_n, so we have three vertices i,j,k for which $c(|i-j|) = c(|j-k|) = c(|i-k|)$. If we order the vertices $1 \leq i < j < k \leq n$, then $c(j-i) = c(k-j) = c(k-i)$ and

$$(j-i) + (k-j) = k-i.$$

And we're done!

To determine $N(2)$, we can first show $N(2) \geq 5$ because the sequence

$$1, 2, 3, 4$$

does not satisfy the condition. To show that $N(2) \leq 5$, suppose we have some 2-coloring c of $\{1,2,3,4,5\}$ that does not satisfy the condition. Then $c(2) \neq c(1)$, and $c(2) \neq c(4)$, so $c(1) = c(4)$ since we only have two colors. This also forces $c(5) = c(2)$. So what to color 3? Well if $c(3) = c(1)$, then we have $1+3 = 4$. If $c(3) = c(2)$, then $2+3 = 5$. So we can't color 3 anything! No such coloring exists, which shows $N(2) = 5$.

To show $N(3) > 13$, we give the following coloring of $\{1,2,\ldots,13\}$:

$$1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13$$

In fact, this reveals a larger pattern, where we form a lower bound for $N(r)$ by gluing together a copy of a lower bound for $N(r-1)$ with a long string of r-colored integers, followed by a shifted copy of the original lower bound, which shows

$$N(r) \leq 3N(r-1) - 2.$$

To show this, we can find a $(r-1)$-coloring of $\{1,2,\ldots,N(r-1)-1\}$ that contains no monochromatic $x, y, x+y$. Assign the same coloring to $\{2N(r-1), 2N(r-1)+1, \ldots, 3N(r-2)-2\}$, and then color $\{N(r-1),\ldots,2N(r-1)-1\}$ the new color. Any x, y colored with the new color have $x+y \geq 2N(r-1)$, and is therefore not colored the new color. And the other colors cannot contain any c-colored pair x, y with $x+y$ also colored c, as looking modulo $2N(r-1)-1$ would force such a pair in the original $(r-1)$-coloring of $\{1,2,\ldots,N(r-1)-1\}$.

Another problem, which we won't go into as much detail on, is

Problem 2 *Let m be given. Show that if n is large enough, then every $n \times n$ $(0,1)$-matrix has a principal submatrix of size m, in which all elements below the diagonal are the same and all the elements above the diagonal are the same.*

The trick is to take $n = R(m,m,m,m)$ and for $A = (a_{ij})$, we consider the pair (a_{ij}, a_{ji}) for $i < j$. As A is a $(0,1)$-matrix, these pairs are one of four: $(0,0), (0,1), (1,0), (1,1)$. We then consider each of these as colors and continue as expected.

There are also many theorems that apply to number theory.

Theorem 12 (Van der Waerden's Theorem) *For any positive integers r, k, there exists some N so that if the integers $\{1, 2, \ldots, N\}$ are colored with r colors, there are at least k integers in an arithmetic progression all colored the same color.*

This is a precursor to Szemeredi's theorem, 1975, which proved a conjecture by Erdos and Turan from the 30s that every subset of integers with positive density contains an arithmetic progression of length k for all k. Terrence Tao has called this theorem a "stepping stone" for connecting various fields of math.

One such example is the Green-Tao theorem, proving the existence of arbitrarily long arithmetic progressions of primes. Szemeredi's theorem doesn't apply in this case because the primes have density 0, but Tao and others introduced a "relative" Szemeredi's theorem that allowed this application.

To do: *Look at their results and see what other sets of density* 0 *are implied to contain arbitrarily long arithmetic progression.*

In 2017, I wrote a blog post on an old blog MathematicalADD concerning all these types of results. The most general is Erdos' conjecture, which states that

Conjecture 3 *If $\sum_{n \in A} \frac{1}{n}$ diverges, then A contains arbitrarily long arithmetic progressions.*

This would imply Szemeredi's theorem and the Green-Tao theorem. In my blog post, I included this chart summarizing the current-known relationships between *positive density, the divergence of the sum of reciprocals,* and *containing arbitrarily long arithmetic progressions.* We label the boxes based on whether the row implies the column.

	$\delta(A) > 0$	$\sum \frac{1}{a} = \infty.$	ALAPs
$\delta(A) > 0$	✓	X	ST
$\sum \frac{1}{a} = \infty.$	P	✓	E
ALAPs	GT	Y	✓

- X: This basically says that $\delta(A) > 0$ means we can bound partial sums of reciprocals by a constant, so the infinite sum diverges.
- ST: Szemerdi's Theorem.
- P: Primes.
- E: Erdos' Conjecture
- GT: Green-Tao Theorem

The final spot Y is proven by considering

$$A = \{1, 10, 11, 100, 101, 102, 1000, 1001, 1002, 1003, 10000, \dots\}.$$

Then this contains arbitrarily long arithmetic progressions by design but the sum of reciprocals is

$$\sum_{k=0}^{\infty} \sum_{t=0}^{k} \frac{1}{10^k + t} \leq \sum_{k=0}^{\infty} \frac{k+1}{10^k} = \frac{19}{10}.$$

A key to these results seem to be Szemeredi's regularity lemma. If we know enough about our graph, then this lemma allows us to count the number of copies of a subgraph with small error. A general mantra in using probabilistic methods is

Every random variable X takes on a value $\geq E(X)$.

Another way to phrase this is

If the probability that a set of objects has a property is > 0, then there exists at least one object with that property

or

If the probability that a set of objects has a property is < 1, then there exists at least one object without that property

The key to this is Markov's Inequality, which says that for a non-negative random variable X with pdf $f(x)$,

$$P(X \geq a) \leq \frac{E(X)}{a}.$$

This follows quickly from

$$E(x) = \int_{-\infty}^{\infty} xf(x)dx = \int_{0}^{\infty} xf(x)dx = \int_{0}^{a} xf(x)dx + \int_{a}^{\infty} xf(x)dx$$

$$\geq \int_{a}^{\infty} xf(x)dx \geq \int_{a}^{\infty} af(x)dx = aProb(X \geq a).$$

My absolute favorite example of this is the following theorem from Erdos:

Theorem 13 *For all g, k, there exists a graph G containing cycles of length at most g (i.e. girth $= g$) and chromatic number k.*

Our interpretation of this theorem is that the chromatic number is a global property of a graph. Containing a clique of size c bounds the chromatic number $\chi(G) \geq c$, but if we have high girth, then locally, our graph looks like a path, which has chromatic number 2. But this theorem shows that even with high girth, we can have as large chromatic number as we'd like. A proper coloring

of G gives a partition of the vertices of G into independent sets, so the ratio of $|V|$ and the size of the largest independent set in G gives an upper bound on $\chi(G)$. This is what we will look at instead of directly looking at $\chi(G)$.

The proof sketch is that we will compute the probability of **a random graph having few enough cycles shorter than g** and the probability of **a random graph having large enough independent sets**. We show both of these probabilities are larger than $1/2$, so their sum is greater than 1, which means there must exist a graph satisfying both properties. We then remove enough vertices to remove all cycles smaller than g and show that the largest independent set is still large enough to guarantee the chromatic number is at least k. Done!

I spent a while typing up some kind of proof, but Jacob Fox covers it very clearly and concisely.

7 The Kneser Graph

The Kneser graph $K(n, k)$ has as its vertex set all k-element subsets of an n-element set, with an edge between two vertices if their intersection is empty. One thing this immediately implies is that $K(n, k)$ is an empty graph if $2k > n$. This graph is very well-studied, and the thing that caught my eye is that its fractional chromatic number is n/k.

So if we choose an abundant number n (meaning $\sigma(n) > 2n$) and consider the graph $G(n) = K(\sigma(n), n)$, the abundancy will be its fractional chromatic number. We can ask, for example, if n and m are friends, how do $G(n)$ and $G(m)$ relate to eachother? Their regular chromatic number is

$$\chi(G(n)) = \sigma(n) - 2n + 2,$$

which was proven by various people but first by Lovasz.

For example,

$$\chi(G(30)) = 72 - 60 + 2 = 14 = 2 * 7$$

$$\chi(G(140)) = 336 - 280 + 2 = 58 = 2 * 29$$

$$\chi(G(2480)) = 5952 - 4960 + 2 = 994 = 2 * 7 * 71$$

$$\chi(G(6200)) = 14880 - 12400 + 2 = 2482 = 2 * 17 * 73$$

$$\chi(G(40640)) = 97536 - 81280 + 2 = 16258 = 2 * 11 * 739$$

When $n = 2k + 1$, we get what's called the *odd graph* O_{k+1}, which generalizes the famous Petersen graph. It is an open problem whether O_k contains a Hamiltonian cycle for all k, but it is conjectured to be true and proven to be true for $k \leq 17$.

In ***Triangle-free Hamiltonian Kneser graphs*** by Chen, 2003, it is shown that if

$$n \geq \frac{1}{2}(3k + 1 + \sqrt{5k^2 - 2k + 1}) \approx 2.62k + 1$$

then $K(n,k)$ contains a Hamiltonian path. It's also known that $K(n,k)$ contains a Hamiltonian path if there exists a non-negative integer a such that $n = 2k+2^a$. The odd graphs are the case of $a = 0$.

So the graph $G(n)$ corresponds to the odd graph O_{n+1} if $\sigma(n) = 2n+1$. It can be shown that $\sigma(n) = 2n+1$ implies n is an odd perfect square. So if $G(n)$ is an odd graph, we know n is an odd perfect square. However, no such n seems to actually exist!

But this gives some motivation to studying these graphs. If we can describe the image of $G(n)$ for all integers n, maybe we can prove an odd graph is contained within. This would imply the existence of an n with $\sigma(n) = 2n+1$. Also, if we could show the image doesn't contain any odd graphs, this would prove no such n exists.

Another interesting fact about $K(n,k)$ is that if $n > ck$, the graph does not contain any c-cliques. Therefore, if we could, without referencing $\mathcal{A}(n)$, show that $G(n)$ does not contain any c-cliques, we can use these graphs to bound the abundancy of n.

Since σ is multiplicative, we might hope for some kind of decomposition of $G(n)$ into its parts. However, remember that $G(p^k)$ is a trivial graph on $\sigma(p^k)$ vertices, so the product over all prime power divisors would just give a trivial graph on $\sigma(n)$ vertices, which if n is abundant, is not equal to $G(n)$.

So suppose that n is abundant and there exists a factorization $n = ab$ with both a, b abundant and $gcd(a,b) = 1$. Then does $G(a) \times G(b) = G(n)$? This does force the abundancy of n to be very high, i.e. $\mathcal{A}(n) > 4$, since $\mathcal{A}(n) = \mathcal{A}(a)\mathcal{A}(b)$ and both a and b are abundant.

Products of Kneser graphs have been pretty well studied. For example, **Independence number of products of Kneser graphs** by Bresar and Valencia-Pabon covers the size of the largest independent set of products of Kneser graph, for the main four different graph products. Another cool result on Kneser graphs is Friedgut establishing a removal lemma for Kneser graphs.

This type of removal lemma is related to Szemeredi's theorem that we talked about before. Roth's theorem on 3-term arithmetic progressions was proved using a triangle removal lemma and the Hardy-Littlewood circle method. A more general hypergraph removal lemma allowed Szemeredi's more general theorem on arbitrarily long arithmetic progressions in dense subsets of the integers. We'll continue to detail some facts about Kneser graphs here but the next section will go back into Szemeredi's theorem, its history, and specific cases.

Going back, we pretty much can't expect any nice decomposition. Detailing a nice bit of mathematical history, this is a StackExchange post asking about strong product decompositions of Kneser graphs. And who else answers but some leading graph theorists, Brendan McKay and Chris Godsil. Here is Godsil's answer.

```
Doerfler and Imrich and (independently) MacKenzie showed that any
connected graph has a unique factorization into graphs prime
relative to the strong product. It follows that if a connected graph
is not prime, its automorphism group is the direct product of two
```

non-identity groups, or is a wreath product. But the automorphism group of the Kneser graph K(v:k) is the symmetric group on points, and this is neither a direct nor a wreath product.

Edit: As Brendan notes below, this argument only works for Kneser graphs that are connected and not complete.

There is a polynomial time algorithm for decomposition relative to the strong product, due to Feigenbaum and Schaeffer. It's likely that if you work through this you will find other ways to show that the Kneser graphs are prime.

This shows that, at least with respect to the strong product, we can't hope for any kind of $G(n) = G(a) \times G(b)$ decomposition. Realistically, I should comb through Godsil's Algebraic Graph Theory to do a thorough refresher of this material. He has a whole chapter on the Kneser graph!

8 Szemeredi's Theorem

9 Back to Sigma

One interesting thing we came across while constructing $AS(n)$ was that iterating our function *next_node* ended up giving a sequence of $1/\sigma^k(a)$ where $a = 4$. This is OEIS sequence A007497. The few comments give a conjectured asymptotic formula

$$\frac{1}{2}log(n) < \frac{\sigma^{n+1}(2)}{\sigma^n(2)} < 2log(n)$$

They then list two conjectures about "stabilizing divisors" of a sort:

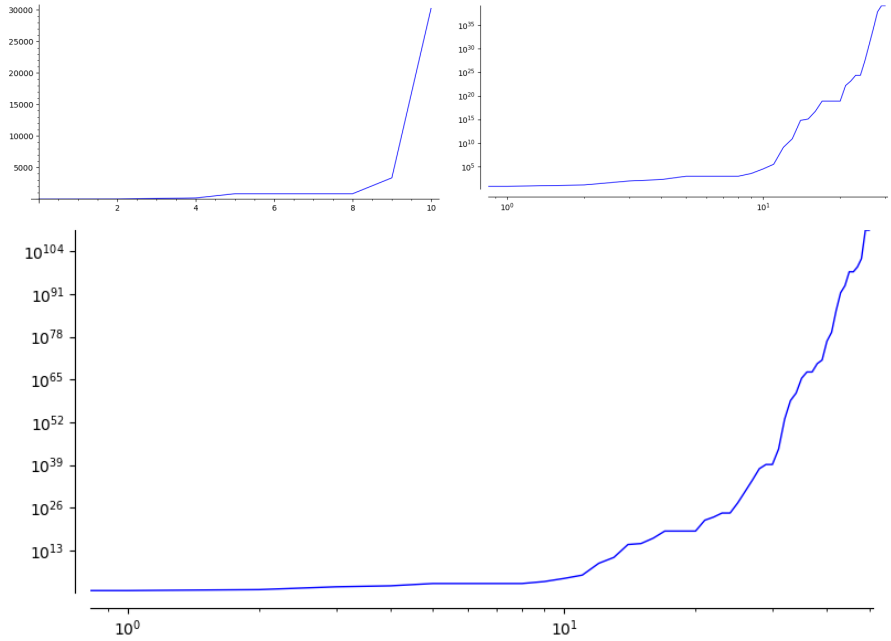
$$\sigma^n(2) \equiv 0 \mod 9, \quad n > 34$$

$$\sigma^n(2) \equiv 0 \mod 2^{22} * 3^5 * 5 * 7 = 35672555520, \quad n > 99$$

We'll look at this in a few different ways. First, for $n \leq x$, let's plot the least common divisor of $\sigma^k(2)$ for $k \leq n$. Here is the list of these values for $x = 21$:

[2, 6, 12, 84, 168, 840, 840, 840, 840, 3360, 30240, 302400, 1190548800, 76195123200, 624114254131200, 1248228508262400, 53673825855283200, 7675357097305497600, 7675357097305497600, 7675357097305497600, 7675357097305497600,157114559781843535872000]

And here are plots of its growth for $x = 10$ (log), $x = 30$, and $x = 50$ (both loglog).



This is so cool! This is such a great way to characterize the failure of σ to distribute primes evenly.

We can look at the analogous situation without σ and consider $lcm(1, 2, \ldots, x)$. We can describe this value by using Chebyshev's second function:

$$\psi(x) = \sum_{p^k \leq x} ln(p)$$

What's the connection? We take the exponential of the psi function:

$$e^{\psi(x)} = e^{\left(\sum\limits_{p^k \leq x} ln(p)\right)} = \prod_{p^k \leq x} e^{ln(p)} = \prod_{p^k \leq x} p = \prod_{p \leq x} p^{a_p},$$

where a_p is the greatest exponent k so that $p^k \leq x$. But the least common multiple of a set can be defined as

$$lcm(A) = \prod_{p} p^{\max(\nu_p(a))}$$

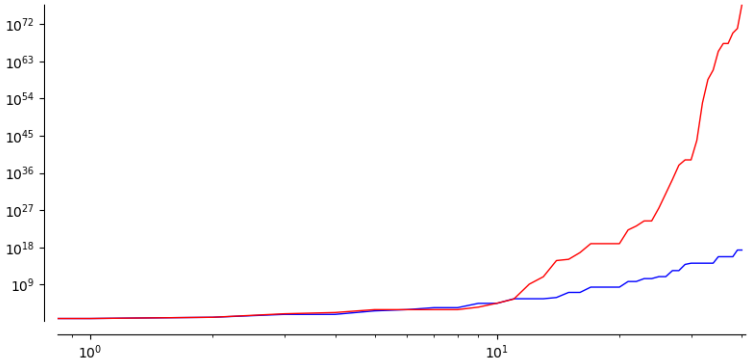
so for the set $A = \{1, 2, \ldots, x\}$, this maximum is the maximum power of p that appears below x, i.e. a_p. So

$$lcm(1, 2, \ldots, x) = e^{\psi(x)}$$

These values up to $x = 21$ are

[2, 6, 12, 60, 60, 420, 840, 2520, 2520, 27720, 27720, 360360,
360360, 360360, 720720, 12252240, 12252240, 232792560,
232792560, 232792560, 232792560, 5354228880]

And we see that $lcm(\sigma^n(2))$ grows much faster than $lcm(1, \ldots, x)$.

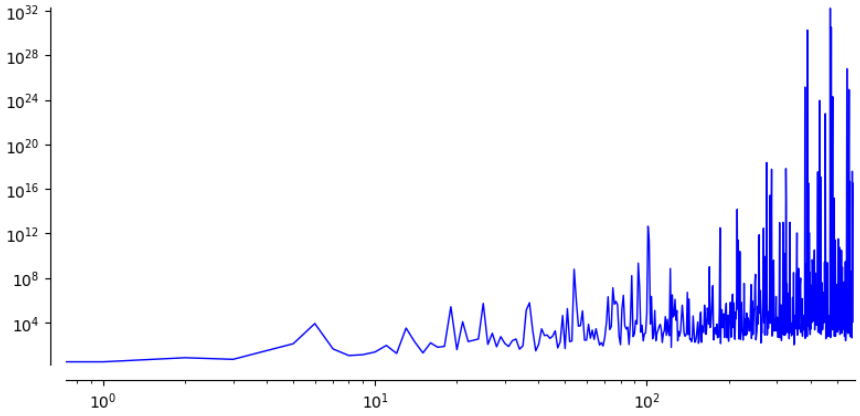


This also makes me wonder how many primes $\sigma^n(2)$ generates as n grows. If we do this for $n \leq 300$, we get these primes, in the order they appear:

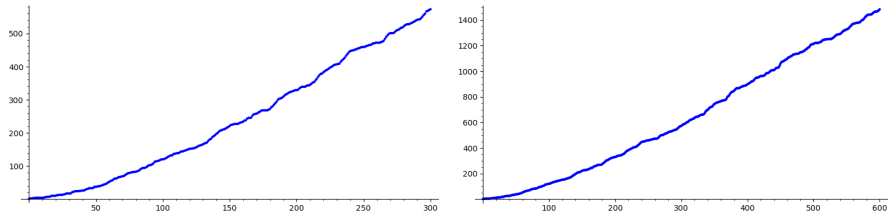
[2, 3, 7, 5, 31, 127, 8191, 43, 11, 13, 23, 89, 17, 3221, 179, 19,
151, 61, 73, 262657, 37, 11939, 199, 257, 337, 524287, 109, 1093, 67,
547, 137, 71, 241, 331, 41, 83, 131071, 599479, 2141, 29, 113, 2731,
683, 757, 379, 601, 1801, 53, 181, 43691, 47, 178481, 197, 223,
616318177, 898423, 4733, 5419, 112303, 263, 271, 7019, 397, 2113,
307, 2801, 467, 97, 157, 79, 431, 9719, 2099863, 2351, 4513, 13264529,
442151, 797161, 398581, 617, 103, 174763, 2796203, 5233, 2617, 3851,
107, 13367, 164511353, 557, 911, 15241, 7621, 2147483647, 15790321,
1361, 5801, 227, 967, 1201, 65537, 4432676798593, 201485309027, 7589,
2212471, 347, 797, 122921, 233, 1103, 2089, 4561, 6829, 2281, 163, 1063,
1871, 34511, 719, 19531, 1321, 661, 715827883, 59, 3033169, 32377, 43331,
1212847, 16189, 121369, 229, 1619, 631, 1597, 23311, 363889, 36389, 1213,
607, 673, 1181, 5229043, 829, 1307261, 313, 367, 193, 433, 38737, 2767,
173, 191, 409, 2143, 11119, 139, 281, 30941, 86171, 167, 5113, 2557, 1279,
368089, 36809, 881, 3191, 201961, 100981, 7213, 1001523179, 3607, 6361,
69431, 2384579, 20394401, 277, 1753, 3181, 3613, 877, 7321, 439, 499, 523,
179951, 3203431780337, 131, 136193, 145193, 3457, 22699, 61681, 457,
30841, 88741, 525313, 421, 2203, 44371, 211, 11093, 92737, 649657, 487,
521, 45319, 3500201, 3571, 583367, 3169, 317, 87211, 21803, 1609669,
145295143558111, 160967, 238972275589, 353, 1087, 23897227559, 311, 1861,
640333, 2521, 1613, 269, 1621, 32668561, 811, 19993, 769, 701, 70841, 953,
11807, 26317, 13159, 1723, 1777, 8951, 391151, 25781083, 373, 920753, 8209,
821, 6091, 121789, 228479, 48544121, 212885833, 283, 641, 1523, 21149,
292561, 7699, 193707721, 761838257287, 67927, 1401943, 7450297, 149, 5653,
1123, 14281, 293459, 12207031, 2932031007403, 9137, 8831418697, 761, 28537,

252283, 20381027, 2305843009213693951, 751, 1069, 99907, 3121, 14951, 24977,
4036961, 2646507710984041, 8713, 672827, 151871210317, 581283643249112959,
619, 4357, 8011, 218834597, 3892029553, 1699, 2003, 2179, 20857, 21467,
2188993, 1789, 10429, 29581, 6481, 463, 9277, 4639, 2298041, 9361973132609,
449, 3691, 127669, 389621, 251, 4051, 64937, 1013, 10052678938039, 853, 36833,
16148168401, 709, 110563, 8269, 827, 658812288653553079, 350432068432741,
8563, 29189717, 159871, 1249, 3541, 102673, 4404047, 359, 4177, 9857737155463,
1307, 9839, 2857, 6529, 653, 1429, 14449, 1772893, 1009, 1171, 305175781, 101,
293, 3499, 43609, 3833, 2687, 154543, 202029703, 466344409, 1113491139767,
743, 6662063, 21523361, 25253713, 736435939, 2593, 71119, 138793, 12626857,
36821797, 97685839, 1297, 2393, 9181, 203659, 1416223, 599, 4591, 17351,
44257, 22129, 2213, 11447, 11489, 13842607235828485645766393, 383, 1009081991,
2011630471, 727, 5821, 10613, 571, 178639387836316422785827021027 9, 70621,
18649457, 33909171296217181, 4271, 35311, 1146277171801, 2207, 302128933, 839,
16493, 180053, 2749, 70123, 22366891, 10039, 4278255361, 2139127681, 10589741,
13421, 14009, 34607, 153649, 2767631689, 33057806959, 2237, 154823, 732541,
276763169, 6451, 7793, 24571, 9225439, 6143, 8237, 7432339208719,
341117531003194129, 1373, 858293, 106551517, 745988807, 92904240109,
870035986098720987332873, 1163, 4673, 46601, 1005203, 111912126900880183,
863, 100801, 3331499, 10567201, 37159429, 2221, 3877, 48259, 5283601, 2641801,
1320901, 60041, 10007, 2664097031, 581173, 26417, 57912614113275649087721,
30707300495827, 349, 1999693963, 5483, 9161, 509, 2413941289, 2908363,
1493, 1741, 14437, 41203, 613, 7219, 10301, 733, 2083, 530713,
162259276829213363391578010288127, 443, 4057, 6740339310641,
334076228395239532950632702 3033, 2029, 29363, 292141, 5465527,
9520972806333758431, 1905907469311277390886779, 2447, 6163, 21827051,
161461131023, 165768537521, 1455309949498963, 587, 14303, 46639, 154877,
256758988973, 593, 1733, 41641, 25646167, 13999, 169553, 8101, 268501, 1471,
8971, 18837001, 332207361361, 2243, 67759, 612928711, 6965099, 5153, 17293,
54410972897, 859, 8647, 9068495483, 1999, 66739, 420778751, 30327152671,
1117, 55897, 547889, 947723521, 2609, 6491257, 5347, 6271, 3981071, 82939,
42521761, 2251, 21260881, 563, 10630441, 38239, 519499, 2931542417, 239,
1039, 3256411, 2939, 62020897, 18584774046020617, 6189700196426901374495621 11,
1433, 1637, 2459, 12611, 10451851, 1051, 5167, 7487, 86656268566282183151,
8235109336690846723986161, 3413, 57251, 2261618993, 46919171622574949, 569,
1657, 2909, 19433, 30269, 5533189, 376936499, 251291, 419, 18041,
380808546861411923, 10303, 31734045571784327]

Plotting these values (loglog plot) shows that the primes we pick up are pretty randomly small or large.

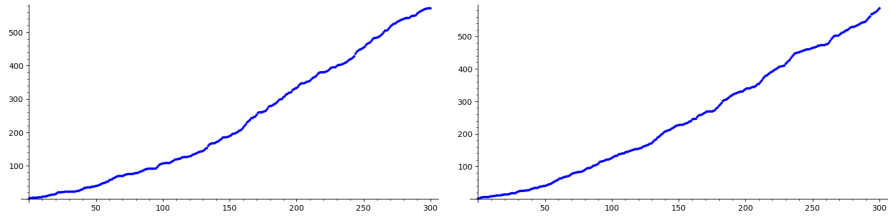


If we plot the number of distinct primes dividing any $\sigma^k(2)$ for $k \leq n$, a.k.a $|\{p|\sigma^k(2) \ : \ k \leq n\}|$, we get



for $n \leq 300$ and $n \leq 600$.

The first positive integer not in the sequence $\sigma^n(2)$ is 5, and $\sigma^n(5)$ contains 6, so the next positive integer not in either sequence is 9. So here are plots of $\sigma^n(5)$ and $\sigma^n(9)$ for $n \leq 300$.



These look pretty much the same for $2, 5$, or 9. But we've addressed this before, I think. When looking at $g(n) = \gcd(n, \sigma(n))$, we saw R.R. Hall's paper **On The Probability that n and f(n) are relatively prime**, where he discussed certain arithmetic functions $f(n)$ having probability $\frac{1}{\zeta(2)}$ of being relatively prime with n.

An interpretation of this is that $f(n)$ distributes the primes as randomly as they usually would be, since the probability that two integers are relatively prime is $1/\zeta(2)$ in general. So $f(n)$ is random with respect to n. For example, if $f(n)$ is the sum of the distinct prime factors of n, then this holds.

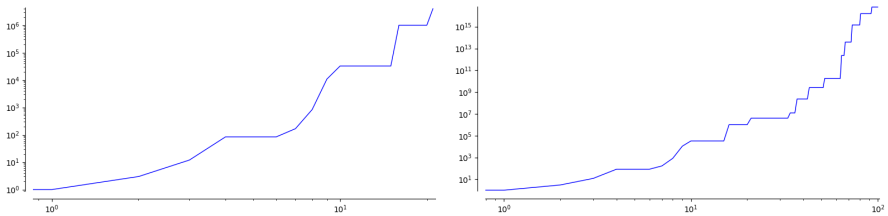
But Erdos showed that for $f(n) = \sigma(n)$ or $\phi(n)$, we have

$$\sum_{\substack{n \leq x \\ gcd(n, f(n))=1}} 1 \approx \frac{xe^{-\gamma_0}}{loglogx}$$

And this tells us that the probability that $gcd(n, f(n)) = 1$ is 0. i.e. these functions don't distribute primes randomly - the probability that they are relatively prime is 0. So the comparison would be counting

$$|\{p|n \ : \ n \leq x\}| = |\{p \leq x\}| \approx \frac{x}{logx}.$$

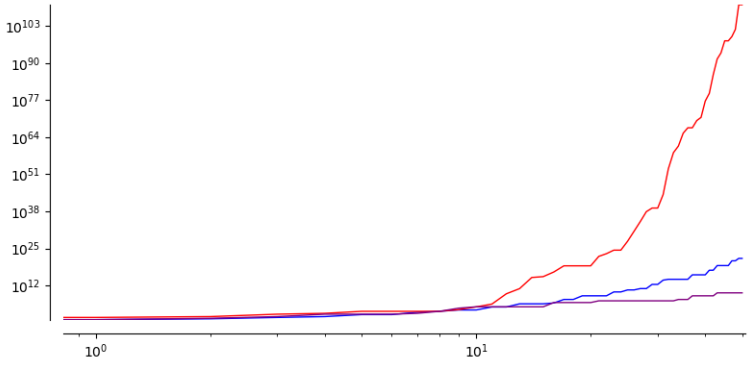
Instead of look at $lcm(\sigma^n(2))$ for $n \leq x$, we could also just iterate through $\sigma(n)$ for $n \leq x$, so let's plot that just for curiosity. Similar to last time, we'll take $x = 21$. But we can actually compute more without iterating σ, so we'll also take $x = 100$, both loglog plot.



And here are the actual values up to $x = 21$:

```
[1, 1, 3, 12, 84, 84, 84, 168, 840, 10920, 32760, 32760, 32760, 32760,
32760, 32760, 1015560, 1015560, 1015560, 1015560, 1015560, 4062240]
```

And for fun, let's plot all three, up to $x = 21$. We'll let $lcm(1, \ldots, n)$ be blue, $lcm(\sigma(2), \ldots, \sigma^n(2))$ be red, and $lcm(\sigma(1), \ldots, \sigma(n))$ be purple.



Basically for any arithmetic function $f(n)$, we can think of $lcm(f(1), \ldots, f(n))$ as telling us about the primes f generates, similar to the fact that

$$e^{\psi(x)} = lcm(1, \ldots, n).$$

Specifically, if we define

$$\psi_f(x) = \sum_{\substack{p^k \mid f(n) \\ n \leq x}} lnp,$$

then we'll have

$$e^{\psi_f(x)} = lcm(f(1), \ldots, f(n)).$$

Though there is something to be said. We take $\psi(x)$ specifically because we expect the density of primes below x to be $\frac{1}{logx}$. If we expect the number of primes $f(n)$ generates for $n \leq x$ to be a different density, it would probably make more sense to take a different weighted sum.

Regardless, we see $lcm(1, \ldots, x)$ grows faster than $lcm(\sigma(1), \ldots, \sigma(x))$, so $\psi(x)$ should grow faster than $\psi_\sigma(x)$. Finally, let's address the stabilizing divisors.

Idea: *This is going to sound incredibly vague, because it is - I remember another problem while computing generating functions related to pattern avoidance where one such pattern gave way to a function that had stabilizing exponents. But it was incredibly hard to do anything with. Then the solution came by "flipping" it in some way and working from the other end. Try to read through your old paper and see if you can remember...*

To find a stabilizing divisor, this means we want some d so that $d|\sigma^n(2)$ for all $n \geq N$ for some N. Therefore, to find these, we should consider

$$gcd(\sigma^n(2), \ldots, \sigma^x(2))$$

for decreasing $n = x-1, x-2, \ldots$. Here is the code to do so:

```
x = 200
sn = 2
A = [sn]
for n in range(1,x+1):
    sn = sigma(sn)
    A.append(sn)
GA = []
for n in range(1,x):
    GA.append(gcd(A[x-n:]))
print(GA)
list_plot(GA,plotjoined=true,scale='loglog')
```

For $x = 200$, these values are

```
[46021947589145231908607478387131678761943040000,
19452244505357153438178189849604915200000,
70804952154322984159641065226240000, 29489775990971671869904650240000,
13127571221052204358041600000, 11934155655502003961856000000,
4773662262200801584742400, 4773662262200801584742400,
4773662262200801584742400, 4773662262200801584742400,
4773662262200801584742400, 4773662262200801584742400,
```

```
477366226220080158474240, 477366226220080158474240,
159122075406693386158080, 397805188516733465395200,
4420057650185927393280, 3400044346296867225600, 3400044346296867225600,
3400044346296867225600, 3400044346296867225600, 3400044346296867225600,
3320355806930534400, 3320355806930534400, 3320355806930534400,
3320355806930534400, 3320355806930534400, 3320355806930534400,
3320355806930534400, 3320355806930534400, 3320355806930534400,
3320355806930534400, 3320355806930534400, 3320355806930534400,
3320355806930534400, 3320355806930534400, 3320355806930534400,
3320355806930534400, 174755568785817600, 174755568785817600,
174755568785817600, 239719573094400, 239719573094400, 239719573094400,
239719573094400, 239719573094400, 239719573094400, 239719573094400,
239719573094400, 239719573094400, 239719573094400, 239719573094400,
239719573094400, 239719573094400, 239719573094400, 239719573094400,
239719573094400, 239719573094400, 239719573094400, 239719573094400,
239719573094400, 239719573094400, 239719573094400, 239719573094400,
239719573094400, 239719573094400, 239719573094400, 239719573094400,
749123665920, 749123665920, 749123665920, 749123665920, 107017666560,
107017666560, 107017666560, 107017666560, 107017666560, 107017666560,
107017666560, 107017666560, 107017666560, 107017666560, 107017666560,
107017666560, 107017666560, 107017666560, 107017666560, 107017666560,
107017666560, 107017666560, 107017666560, 35672555520, 35672555520,
35672555520, 35672555520, 35672555520, 35672555520, 35672555520, 35672555520,
35672555520, 35672555520, 11890851840, 11890851840, 11890851840, 11890851840,
11890851840, 11890851840, 11890851840, 594542592, 594542592, 594542592,
594542592, 594542592, 594542592, 594542592, 594542592, 594542592, 594542592,
594542592, 594542592, 594542592, 594542592, 594542592, 9289728, 9289728,
9289728, 9289728, 9289728, 9289728, 2322432, 2322432, 2322432, 2322432,
2322432, 2322432, 2322432, 110592, 110592, 110592, 110592, 110592, 110592,
110592, 110592, 110592, 110592, 110592, 110592, 36864, 36864, 36864, 36864,
9216, 9216, 9216, 9216, 2304, 2304, 2304, 2304, 2304, 2304, 2304, 576, 576,
576, 64, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
```

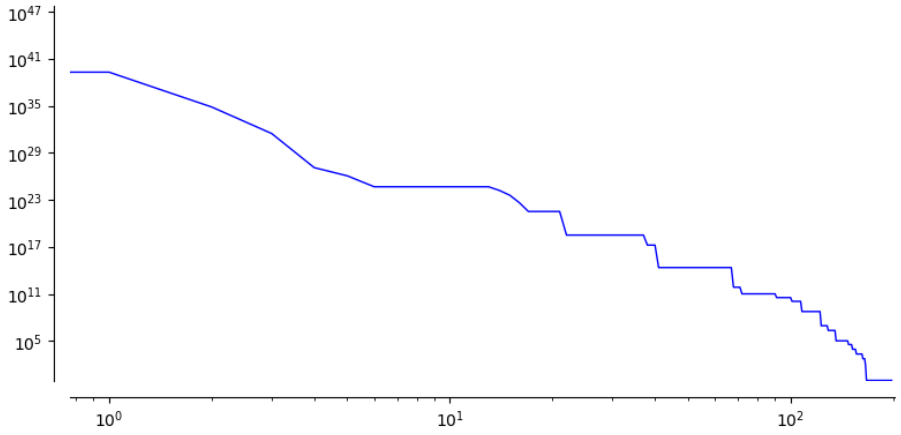
You can see the value given in the OEIS comment 35672555520 appear fairly close to the bottom of the list. The highest value we found that might be conjectured to be a stabilized divisor is

$$3400044346296867225600 = 2^{38} * 3^{12} * 5^2 * 7^2 * 19$$

And a further conjecture might be that all primes eventually appear in a stabilized divisor of $\sigma^x(2)$. For example, going from $x = 100$ to 200 picked up the prime 19. Extending to 300, we have a plausible stabilized divisor of

$$940428731128837447550277335068484567040000000 0 = 2^{71} * 3^{17} * 5^8 * 7^6 * 11 * 13^2 * 19^2$$

so you see we picked up the primes 11 and 13. Here is the loglog plot for $x = 200$:



Still no 17 though, let's see if our computer can handle $x = 500$. It can! And the highest plausible stabilized divisor is

$$368954344470806704240033498445877214030388745728582136319627841673604409364168856043520000000000$$

$$= 2^{130} * 3^{33} * 5^9 * 7^{11} * 11^5 * 13^4 * 17^2 * 19^3 * 23 * 29 * 31 * 37 * 181$$

Conjecture 4 *For all primes p, there exists N so that $p|\sigma^n(2)$ for all $n \geq N$.*

And as the powers seem to also accumulate, we could even conjecture that

Conjecture 5 *For all primes p and integers $k \geq 1$, there exists N so that $p^k|\sigma^n(2)$ for all $n \geq N$.*

And finally, replacing 2 with any other integer seems to also not affect this so much. For example, looking at $\sigma^n(5)$ instead for $x = 400$ gives a (conjectural) stabilized divisor of at least

$$13580150719726630362484005819442182164595826446512947200000000$$

$$= 2^{87} * 3^{20} * 5^8 * 7^8 * 11^2 * 13^4 * 17^2 * 19^2 * 31$$

In general, there are various theorems that analyze divisors of $\sigma(n)$. Let's go through a few of them.

Theorem 14 *The value $\sigma(n)$ is odd if and only if $n = 2^r k^2$ for some $r, k \geq 1$.*

Proof. *This boils down to two parts. First that $\sigma(2^r) = (2^{r+1} - 1)$ is odd for all $r \geq 1$, which is clear. The next is that if ℓ is odd, then $\sigma(\ell)$ is odd if and only if ℓ is a square.*

To see this, we can pair up divisors of ℓ as d and ℓ/d. If ℓ is not a square, then every divisor has a pair, and

$$\sigma(\ell) = \sum_{d<\sqrt{\ell}} d + \frac{\ell}{d}$$

Since d and ℓ/d are odd, eadch summand is even, so $\sigma(\ell)$ is even. If ℓ was an odd square, then we'd have a single unmatched divisor $\sqrt{\ell}$, so

$$\sigma(\ell) = \sqrt{\ell} + \sum_{d<\sqrt{\ell}} d + \frac{\ell}{d} = ODD + EVEN = ODD$$

Now we see that $\sigma^7(2) = 24 = 2^3 * 3$. So the conjecture that 2 is a stable divisor of $\sigma^n(2)$ is equivalent to showing that the odd part of $\sigma^n(2)$ is not a square for all $n \geq 7$.

Naturally, this raises the question: For which n does a given prime q divide $\sigma(n)$? The last theorem could be rephrased as

Theorem 15 *$\sigma(n)$ is divisible by 2 iff the odd part of n is not a square.*

Let's look at divisibility by $q = 3$. We'll phrase this theorem in the same way as the last one originally was (Theorem 14). Then we'll give a proof, which will give a guide for the general case, rephrased in a more accessible way.

Theorem 16 *$\sigma(n)$ is not divisible by 3 if and only if $n = 3^r t^2 s^3 u$, where*

- *$r \geq 0$ and $t, s, u \geq 1$.*
- *$p|t$ if and only if $p \equiv -1 \ mod \ q$*
- *$p|s$ or $p|u$ if and only if $p \equiv 1 \ mod \ q$*
- *u is square-free.*

Proof 1 *The idea here is to divide the set of primes $p|n$ into residue classes mod 3. Then since $\sigma(n)$ is multiplicative, we have*

$$\sigma(n) = \prod_{p|n} \sigma(p^{\nu_p(n)}) = \prod_{\substack{p|n \\ p \equiv 0 mod 3}} \sigma(p^{\nu_p(n)}) \prod_{\substack{p|n \\ p \equiv 1 mod 3}} \sigma(p^{\nu_p(n)}) \prod_{\substack{p|n \\ p \equiv -1 mod 3}} \sigma(p^{\nu_p(n)})$$

The first term clearly only has $p = 3$ and since $\sigma(3^{\nu_p(n)}) = 1 + 3 + \cdots + 3^{\nu_p(n)}$, we see $\sigma(3^{\nu_p(n)}) \equiv 1 \ mod \ 3$ for any choice of exponent. This gives the 3^r term in the theorem statement.

The second term has $p \equiv 1 \ mod \ 3$, so

$$\sigma(p^{\nu_p(n)}) = 1 + p + \cdots + p^{\nu_p(n)} \equiv \nu_p(n) + 1 \ mod \ 3$$

So this is only divisible by 3 if $\nu_p(n) \equiv -1 \ mod \ 3$. This means $\sigma(p^{\nu_p(n)})$ is not divisible by 3 if $\nu_p(n) \equiv 0, 1 \ mod \ 3$. Any p with exponent $0 \ mod \ 3$ contributes to the s^3 term and any p with exponent $1 \ mod \ 3$ will contribute to the s^3 term with a leftover square-free part u.

For the last part, if $p \equiv -1 \ mod \ 3$, then

$$\sigma(p^{\nu_p(n)}) = 1 + p + p^2 + \cdots + p^{\nu_p(n)} \equiv \begin{cases} 0 \ mod \ 3 & \text{if } \nu_p(n) \equiv 1 \ mod \ 2 \\ 1 \ mod \ 3 & \text{if } \nu_p(n) \equiv 0 \ mod \ 2 \end{cases}$$

Therefore, any prime $p \equiv -1 \ mod\ 3$ must have $\nu_p(n) \equiv 0 \ mod\ 2$ to not be divisible by 3. This gives the t^2 term in the theorem statement.

As we have covered all residue classes, this is a complete characterization.

The idea for a general proof is clear (and the intuitive choice!). If we care about divisibility of $\sigma(n)$ by q, then since σ is multiplicative, we really care about divisibility of $\sigma(p^a)$ by q. Then $\sigma(p^a) = 1 + p + \cdots + p^a$ is easily determined from the residue class $p \ mod\ q$. If $p \not\equiv 1 \ mod\ q$, then $p - 1$ is invertible, so we can write $\sigma(p^a) = \frac{p^{a+1}-1}{p-1}$. Then this is equal to $0 \ mod\ q$ iff $p^{a+1} - 1 \equiv 0 \ mod\ q$ iff $p^{a+1} \equiv 1 \ mod\ q$.

We usually define the *order* of an integer n mod q as the smallest k so that $n^k \equiv 1 \ mod\ q$. Notice that this is only well-defined when $gcd(n, q) = 1$. We'll make a slight change and say that $Ord_q(n)$ is defined as above in all case except if $Ord_q(n) = 1$, where we'll instead say $Ord_q(n) = q$. In other words, if $n \equiv 1 \ mod\ q$, then we'll say $Ord_q(n) = q$. Together with the last paragraph, this tell us that if $p \not\equiv 1 \ mod\ q$, then q divides $\sigma(p^a)$ if and only if $a + 1 \equiv 0 \ mod\ Ord_q(p)$.

If $p \equiv 1 \ mod\ q$, then $\sigma(p^a) = 1 + p + \cdots + p^a \equiv a + 1 \ mod\ q$. So $q|\sigma(p^a)$ if and only if $a + 1 \equiv 0 \ mod\ q$. This is the reason why we define $Ord_q(p) = q$ in this case! It allows us to state the very succinct theorem:

Theorem 17 *A prime q divides $\sigma(n)$ if and only if there exists a $p|n$ such that*

$$\nu_p(n) + 1 \equiv 0 \ mod\ Ord_q(p).$$

And since each such prime p contributes at least one factor of q, we have

Theorem 18 *For all primes q, the exponent of q in $\sigma(n)$ is at least*

$$\nu_q(\sigma(n)) \leq |\{p|n \ : \ \nu_p(n) + 1 \equiv 0 \ mod\ q\}|$$

Let's test it! Instead of starting with an n, let's build an n so that $q = 5$ will divide $\sigma(n)$. For this, we'd need some $p|n$ so that $\nu_p(n) + 1 \equiv 0 \ mod\ q$. Let's choose three! Let

$$n = 2^3 3^7 11^9$$

so

$$Ord_5(2) = 4 \quad and \quad 3 + 1 \equiv 0 \ mod\ 4$$
$$Ord_5(3) = 4 \quad and \quad 7 + 1 \equiv 0 \ mod\ 4$$
$$Ord_5(11) = 5 \quad and \quad 9 + 1 \equiv 0 \ mod\ 5$$

Then

$$\sigma(n) = 2^6 * 3^2 * 5^3 * 41 * 3221 * 13421$$

and there is that factor of 5^3. Awesome! Let's test the other primes that appear.

$$Ord_{13421}(2) = 2684 \quad and \quad 3 + 1 \not\equiv 0 \ mod\ 2684$$

$$Ord_{13421}(3) = 2684 \quad and \quad 7+1 \not\equiv 0 \ mod \ 2684$$
$$Ord_{13421}(11) = 10 \quad and \quad 9+1 \equiv 0 \ mod \ 10$$

and

$$Ord_{3221}(2) = 644 \quad and \quad 3+1 \not\equiv 0 \ mod \ 644$$
$$Ord_{3221}(3) = 644 \quad and \quad 7+1 \not\equiv 0 \ mod \ 644$$
$$Ord_{3221}(11) = 5 \quad and \quad 9+1 \equiv 0 \ mod \ 5$$

and

$$Ord_{41}(2) = 20 \quad and \quad 3+1 \not\equiv 0 \ mod \ 20$$
$$Ord_{41}(3) = 8 \quad and \quad 7+1 \equiv 0 \ mod \ 8$$
$$Ord_{41}(11) = 40 \quad and \quad 9+1 \not\equiv 0 \ mod \ 40$$

and

$$Ord_{3}(2) = 2 \quad and \quad 3+1 \equiv 0 \ mod \ 2$$
$$Ord_{3}(11) = 2 \quad and \quad 9+1 \equiv 0 \ mod \ 2$$

and

$$Ord_{2}(3) = 2 \quad and \quad 7+1 \equiv 0 \ mod \ 2$$
$$Ord_{2}(11) = 2 \quad and \quad 9+1 \equiv 0 \ mod \ 2$$

From this, we get the approximation $2^2 * 3^2 * 5^3 * 41 * 3221 * 13421$, which is only missing a factor of 2^4.

Another interesting case of partitioning a set of primes mod q is in the Leibniz formula for π:

$$\frac{\pi}{4} = \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} = \left(\prod_{p \equiv 1 \ mod \ 4} \frac{p}{p-1} \right) \left(\prod_{p \equiv 3 \ mod \ 4} \frac{p}{p+1} \right)$$

10 Back to Abundancy 2

At the beginning, we wondered when $rad(n) | \frac{n}{g(n)}$, since this condition seems to correlate to n being solitary. Now we might be in a position to better describe $g(n) = gcd(n, \sigma(n))$. If $q|n$, then $q|\sigma(n)$ if and only if there exists $p|n$ so that

$$\nu_p(n) + 1 \equiv 0 \ mod \ Ord_q(p).$$

We can visualize this as a matrix where our rows and columns correspond to the distinct prime divisors of n. In the spot (i, j), we place $\nu_{p_i}(n)+1 \ mod \ Ord_{p_j}(p_i)$, except we place 1s all along the diagonal. Define this to be $\mathcal{M}(n)$. For example,

$$\mathcal{M}(2^3 * 5 * 7^4 * 11) = \begin{bmatrix} 1 & 0 & 1 & 4 \\ 0 & 1 & 2 & 2 \\ 1 & 1 & 1 & 5 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

The number of zeros in a column j represents the minimum number of times p_j divides $\sigma(n)$. In this case, we see that $5|\sigma(n)$ and $2^2|\sigma(n)$ and $7, 11$ do not. And indeed,

$$\sigma(2^3 * 5 * 7^4 * 11) = 2^3 * 3^3 * 5 * 2801.$$

This tells us without computing $\sigma(n)$ that any friends of n must be multiples of $7^4 11$ at least.

Here's a fun question: What if $\mathcal{M}(n)$ is the $\omega(n) \times \omega(n)$ identity matrix? Then for all distinct primes $p, q|n$, we have $\nu_p(n) + 1 \equiv 0 \ mod \ Ord_q(p)$. For example, if $\omega(n) = 2$ and $p = 3$, $q = 11$, then $Ord_3(11) = 2$ and $Ord_{11}(3) = 5$, so $n = 11^3 * 3^4$ will give the identity matrix, meaning $\sigma(n)$ will be divisible by at least $11 * 3 = 33$. And

$$\sigma(11^3 * 3^4) = 2^3 * 3 * 11^2 * 61.$$

In general, if $\mathcal{M}(n)$ is the identity matrix, then every column has $\omega(n) - 1$ zeros, which means $\sigma(n)$ is divisible by at least $rad(n)^{\omega(n)-1}$. This sequence for $n \leq 5000000$ begins

$$1, 96, 864, 6144, 7776, 55296, 69984, 393216, 497664, 629856, 3538944$$

This does not appear on OEIS but a related sequence A173615 does, consisting of those n for which $\sigma(n)$ is divisible by $rad(n)^2$. There, they cite two papers: ***W. Sierpinski, Number Of Divisors And Their Sum, Elementary theory of numbers, Warszawa, 1964.*** and ***F. Luca et al, On integers for which the sum of divisors is the square of the squarefree core.***

In the second paper listed above, the authors mention the concept of a *prime-perfect* number n, for which $rad(n) = rad(\sigma(n))$, introduced and analyzed by Paul Pollack and Carl Pomerance. With Theorem 17 in mind, we can say that a number n is prime-perfect if both of the following hold.

- For all $q|n$, there exists a distinct $p|n$ so that $\nu_p(n) + 1 \equiv 0 \ mod \ Ord_q(p)$.
- For any prime q not dividing n, we have $\nu_p(n) + 1 \not\equiv 0 \ mod \ Ord_q(p)$ for all $p|n$.

Pollack and Pomerance show that the density of prime perfect numbers less than x is $x^{1/3+o(1)}$. Can we deduce that from these two statements?

And interestingly enough, all of those n above have $\omega(n) = 2$, which is why entering a partial sequence got that OEIS entry. But the entries in their list that aren't in ours are those n for which $rad(n)^2|\sigma(n)$ but $\omega(n) > 2$. For $\omega(n) \geq 3$, do there exist any n so that $rad(n)^{\omega(n)-1}$ divides $\sigma(n)$? It seems like the answer is no. Let's fix $\omega(n) = 3$ and see what we get.

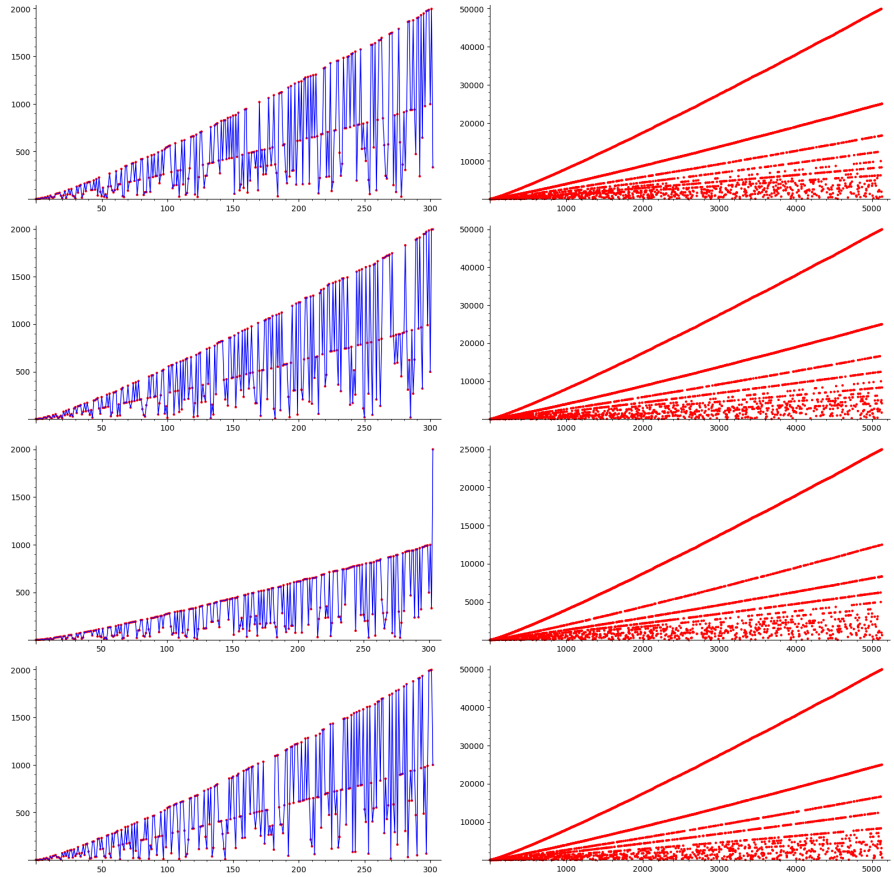
Then $n = p^a q^b r^c$ and we want to see if $\sigma(n)$ is divisible by $(pqr)^2$. For $p^2|\sigma(n)$, we'd need $p^2|\sigma(q^b)$, $p^2|\sigma(r^c)$, or ($p|\sigma(q^b)$ and $p|\sigma(r^c)$).

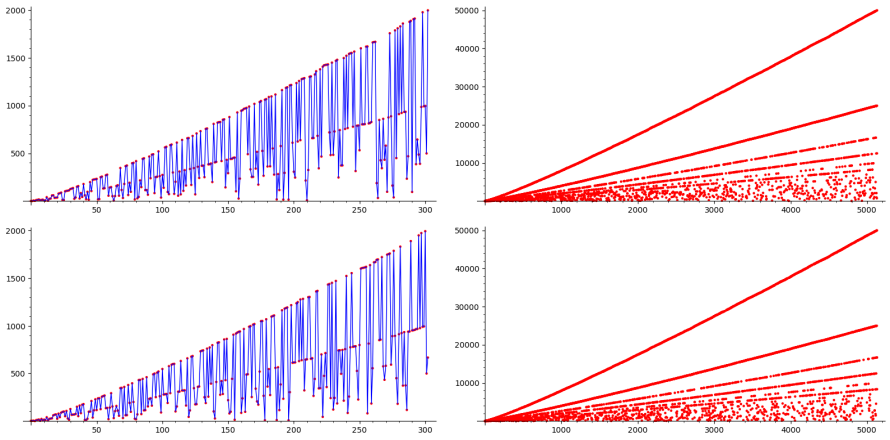
If the last case holds for all three primes, this would mean

$$\nu_q(n) + 1 \equiv 0 \ mod \ Ord_p(q) \qquad \nu_r(n) + 1 \equiv 0 \ mod \ Ord_p(r)$$

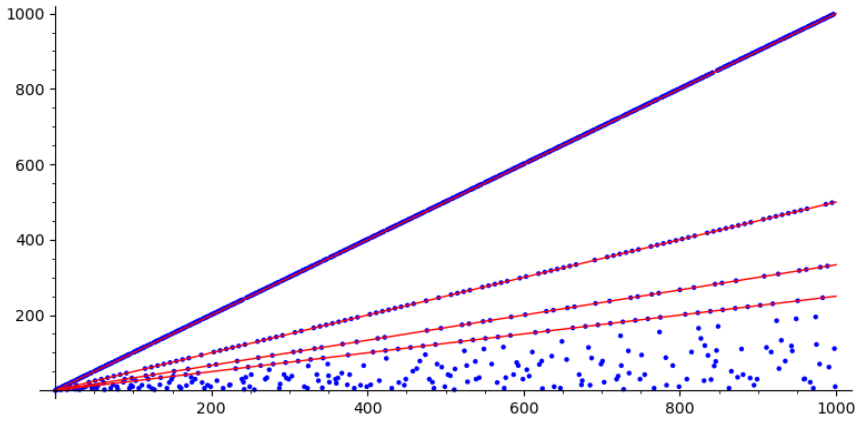
$$\nu_p(n)+1 \equiv 0 \ mod \ Ord_q(p) \qquad \nu_r(n)+1 \equiv 0 \ mod \ Ord_q(r)$$
$$\nu_p(n)+1 \equiv 0 \ mod \ Ord_r(p) \qquad \nu_q(n)+1 \equiv 0 \ mod \ Ord_r(q)$$

Paul Pollack has a talk on multiplicative orders mod p that might be helpful. Let's look through it. The first problem he introduces is looking at the distribution of $Ord_q(a)$ as q varies through the primes. He doesn't have this, but as always, I love a good visual. So here are plots for $a = 2, 3, 4, 5, 6$ with $q \leq 100$. We've connected the points to emphasize the transitions but colored the points red to distinguish the actual values. Also remember that where $Ord_q(a) = 1$ in usual texts, we're defining $Ord_q(a) = q$, which means the maximum value of the plots tell us what prime we're focusing on. Also we define $Ord_q(a) = 0$ if $gcd(q, a) \neq 1$.





This looks kind of like that plot for $rad(n)$, where the values cluster around the lines x/m for $m = \frac{n}{rad(n)}$

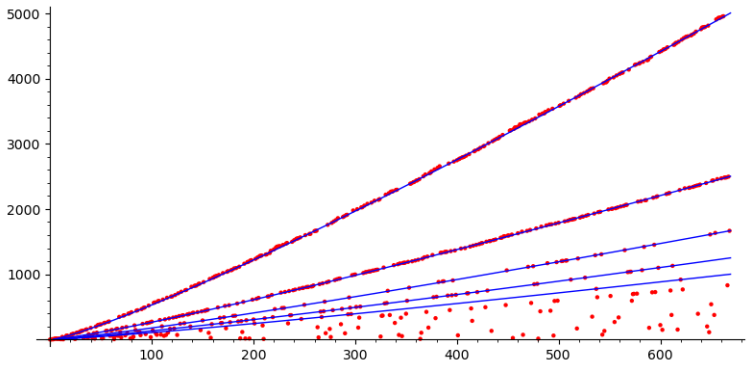


For the plots of $Ord_q(a)$, all the top lines seem to be approximately $Cxlogx$ for some $C \sim 1.15$, except for $a = 4$, in which the coefficient seems to be halved, which could have to do with $4 = 2^2$. It's easy to show that

$$Ord_q(a^s) = \frac{Ord_q(a)}{gcd(Ord_q(a), s)}$$

So the plot for $a = 8 = 2^3$ actually looks like the others, while $a = 16$ has the halved coefficient again.

And just like the $rad(n)$ plot, the $Ord_q(a)$ plot over q seems to fall into the curves $(C/m)xlogx$ for $m \geq 1$. For $a = 6$,



Of course, x here is not the prime itself but the index of the prime. The x^{th} prime is approximately $xlogx$ by the PNT, so the top line is actually just the primes q for which $Ord_q(a) = q - 1$. In other words, the top line consists of those primes for which a is a primitive root.

Artin's conjecture on primitive roots states that for all integers a that are not a perfect square or -1, we will have $Ord_q(a) = q - 1$ for infinitely many primes q. Our plots certainly seem to suggest this is true. This would also be supported by our plots of 4 and 16 being halved, meaning there is no such q for which $Ord_q(4) = q - 1$. Specifically,

Conjecture 6 (Artin's Conjecture on Primitive Roots) *Let $a = a_0 b^2$ with $a_0 \neq 1$ square-free and $S(a)$ be the set of primes for which a is a primitive root. Then*

1. *$S(a)$ has positive density inside the set of primes. In particular, $S(a)$ is infinite.*
2. *If $a_0 \neq 1 \mod 4$, this density is independent of a and equals Artin's constant*

$$C_{Artin} = \prod_p \left(1 - \frac{1}{p(p-1)}\right) \approx 0.373955$$

This focus on not being a perfect square reminds me of our previous work on $\sigma(n)$ being even if and only if the odd part of n was not a perfect square. That is, we could restate Artin's conjecture in terms of the divisibility of $\sigma(n)$. If $\sigma(n)$ is even, then the odd part of n is not a perfect square, and Artin's Conjecture would imply $n/2^{\nu_2(n)}$ is a primitive root of infinitely many primes q. Moreso, if $\nu_2(n)$ is odd, then n is a primitive root for infinitely many primes q.

A generalization of this constant by P.J. Stephens in ***"Prime Divisor of Second-Order Linear Recurrences, I."*** would give the density of the set $T(a, b)$ of primes dividing $a^k - b$ for some k, relative to the set of primes:

$$C_S = \prod_p \left(1 - \frac{p}{p^3 - 1}\right) \approx 0.5759599\ldots,$$

assuming a and b are multiplicatively independent, meaning $a^A b^B = 1$ implies $A = B = 0$.

These constants are explicitly related by

$$C_S = \prod_p \left(C_{Artin} + \left(\frac{1-p^2}{p^2(p-1)} \right) \right) \left(\frac{p}{p+1+1/p} \right)$$

So what's the lesson? The questions concerning $\mathcal{A}(n)$ are hard because they relate to multiplicative orders of integers, which are difficult to work with. But not impossible! Lots of smart people have made good progress in this area. For example, Pollack! We'll continue his talk and do some exposition.

One more thing I want to do is to read through Artin's paper to see how he derives this constant. It reminds me of the "care-free constant"

$$\prod_p \left(1 - \frac{1}{p(p+1)} \right) \approx 0.704442200$$

that is double the coefficient of x^2 in $\sum_{n \leq x} rad(n)$ and that we proved was double the coefficient of x^2 in $\sum_{n \leq x} \ell(n)$ where $\ell(n) = \sum_{k=1}^{\alpha(n)} rad_k(n)$.

Our previous characterization of divisibility of $\sigma(p^a)$ by q is that

$$q | \sigma(p^a) \iff a + 1 \equiv 0 \ mod \ Ord_q(p).$$

If we want to get exact prime powers of $\sigma(p^a)$, the same reasoning tells us that if $p - 1$ is invertible mod q^b, then

$$q | \sigma(p^a) \iff a + 1 \equiv 0 \ mod \ Ord_{q^b}(p).$$

But a more general statement is that

$$\sigma(p^a) = \prod_{q | p^{a+1}-1} q^{\nu_q(p^{a+1}-1) - \nu_q(p-1)},$$

which reduced to the previous statement because $p - 1$ being invertible means $\nu_q(p-1) = 0$. After writing this, it became obvious, as

$$\sigma(p^a) = \frac{p^{a+1} - 1}{p - 1}$$

so it consists of all primes dividing $p^{a+1} - 1$ more than $p - 1$.

Therefore, we can write $\sigma(n)$ as

$$\sigma(n) = \prod_{p | n} \prod_{q | p^{\nu_p(n)+1}} q^{\nu_q(p^{a+1}-1) - \nu_q(p-1)}$$

We can extend this to $\mathcal{A}(n)$ by dividing by n. To describe this, we'll split the abundancy index into the numerator and denominator of its reduced form.

Let $E(n,q)$ be the max of 0 and

$$\left(\sum_{\substack{p|n \\ q|p^{\nu_p(n)+1}-1}} \nu_q(p^{\nu_p(n)+1}-1) - \nu_q(p-1) \right) - \nu_q(n)$$

Notice that if q does not divide $p^{\nu_p(n)+1}-1$, then $E(n,q)=0$. Otherwise, it will be the exponent of q in the numerator of the reduced fraction of $\mathcal{A}(n)$. So define

$$N(n) = \prod_{q\ prime} q^{E(n,q)}$$

Then if we define

$$\overline{E}(n,q) = max(0, \nu_q(n) - E(n,q)),$$

we can also define

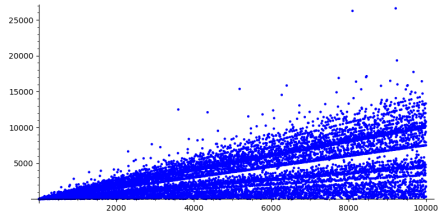
$$D(n) = \prod_{q\ prime} q^{\overline{E}(n,q)}$$

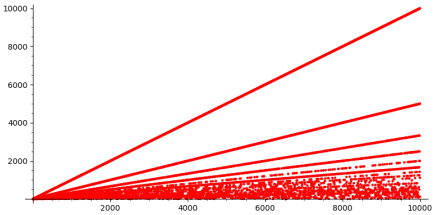
and we will have $\mathcal{A}(n) = N(n)/D(n)$ in reduced form.

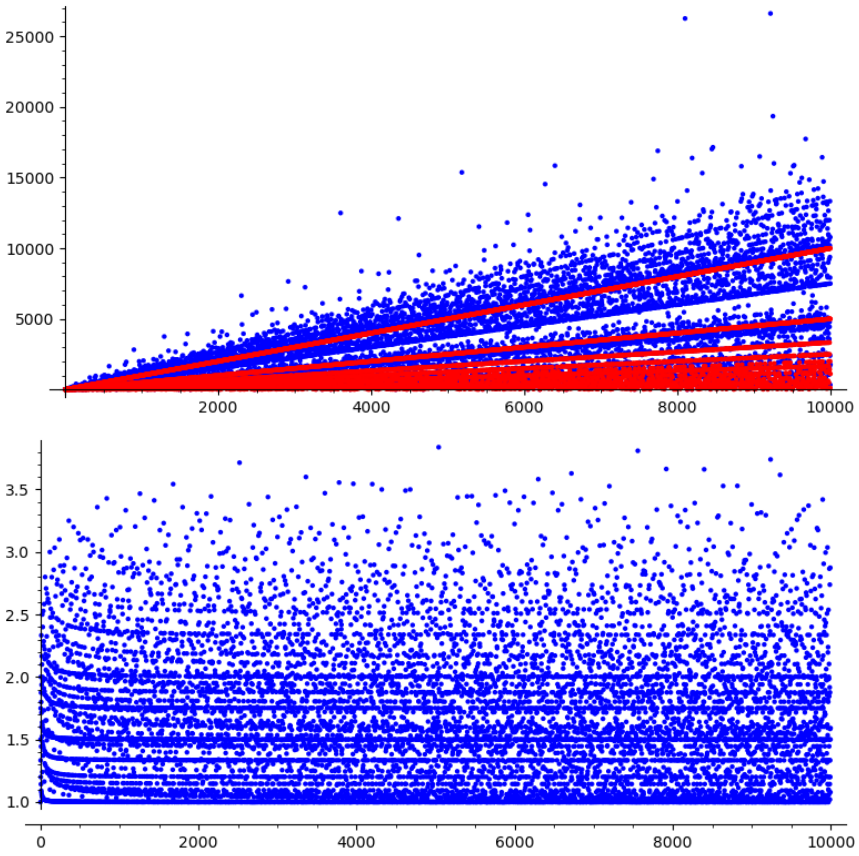
Let's introduce a few **definitions**:

- We call n and m *upper-semi-friends* if $N(n) = N(m)$.
- We call n and m *lower-semi-friends* if $D(n) = D(m)$.
- Then n and m are friends if they are both upper and lower semi-friends.
- We call n *upper/lower-solitary* if it has no upper/lower-semi-friends respectively.

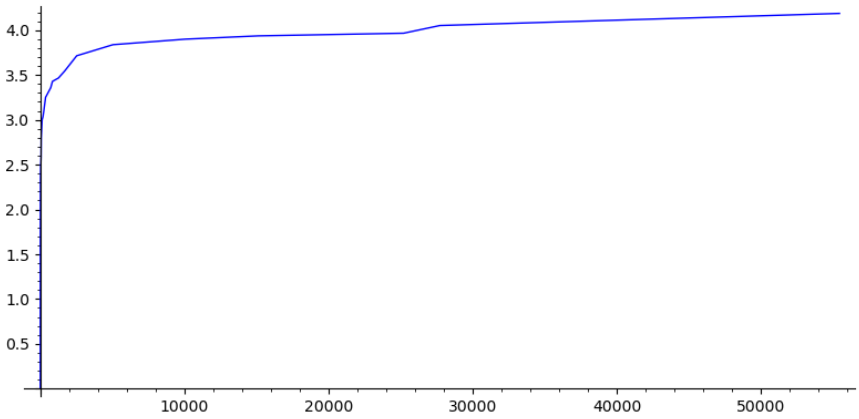
It almost seems like there are no upper-solitary or lower-solitary numbers. Let's go ahead and plot $N(n)$ and $D(n)$ for $n \leq 10000$. We'll plot them separately and then plot them on top of each other with NL blue and DL red. We'll also plot $\mathcal{A}(n)$ again, just for reference.



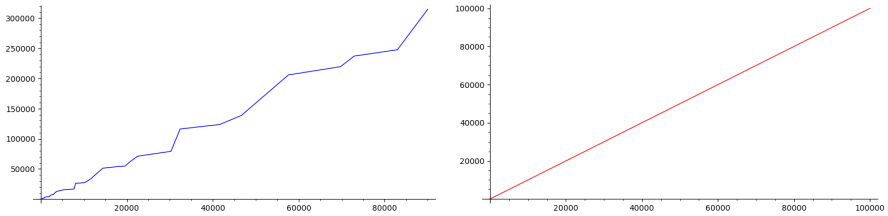




Let's plot their maxima. First, we'll do $\mathcal{A}(n)$.



Then we'll do NL and DL.



It's clear that

$$\max_{n\leq x} D(n) = \max_{\substack{n\leq x \\ g(n)=1}} n$$

but what about $N(n)$? Searching the sequence of ns on OEIS gives *A239973: Sequence, starting with 1, of increasing numbers such that both the numerator and the denominator of the abundancy index, sigma(n)/n are strictly increasing* and gives an initial list

$$1, 2, 3, 4, 7, 8, 16, 21, 27, 32, 36, 50, 63, 64, 93, 98, 100, 128, 144, 256, 324, 392, 400,$$

$$512, 576, 784, 800, 900, 1296, 1600, 1936, 2304, 2916, 3600, 5184, 6400, 7744, 8100,$$

$$9216, 10404, 11664, 14400, 17424, 19600, 20736, 22500, 30276, 32400, 41616, 46656$$

They question whether any more odd numbers than $1, 3, 7, 21, 27, 63, 93$ appear. Perhaps our characterization of when $2|\sigma(n)$ could provide some insight into this. They also question whether every number in this sequence has $g(n) = 1$.

Doing the same for $D(n)$ confirms what we thought, and gives *A014567: Numbers k such that k and sigma(k) are relatively prime.* Remember the asymptotic growth proven by Erdos,

$$\sum_{\substack{n\leq x \\ g(n)=1}} 1 \sim \frac{xe^{\gamma_0}}{loglogloglogx},$$

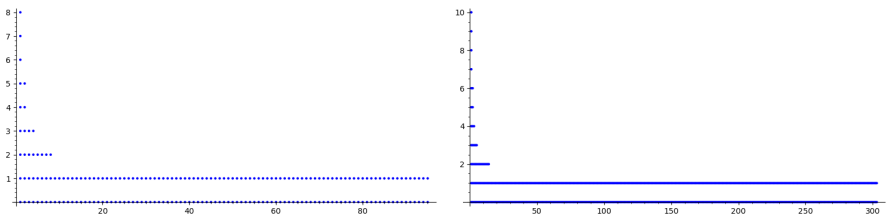
tells us the natural density of $\{n \ : \ g(n) = 1\}$ is 0. Niven proved in his paper discussed in the first section that for any k, the density of $\{n \ : \ g(n) \leq k\}$ is 0.

If we assume $g(n) = 1$ for the maximum values of $N(n)$, then this comes down to maximizing $\sigma(n)$. The characterization we had before is that

$$q^b|\sigma(n) \iff q^{b+\nu_q(p-1)}|(p^{\nu_p(n)+1} - 1)$$

So we can look through primes $p \leq x$ for which $p^{a+1} - 1$ has many large prime power divisors and construct $n = \prod_p p^a$ to maximize $\sigma(n)$.

The following plots consists of points (i, a) where $p_i^a < x$, for $x = 500, 2000$.



Let's maybe try to take a bit of a combinatorial look at this maximization (though I do know there's almost certainly optimization results that could help here, but...).

Problem 3 *How do you choose exponents* $\boldsymbol{e} = (e_1, \ldots, e_{\pi(x)})$ *so that*

$$n = \prod_p p_i^{e_i}$$

is maximized?

Problem 4 *How do you choose exponents* $(e_1, \ldots, e_{\pi(x)})$ *so that*

$$\sigma(n) = \prod_p \sigma(p_i^{e_i})$$

is maximized?

Let's introduce a swapping function and see how it effects these values. Let $sw(\mathbf{e}, i, j)$ be the tuple of exponents with e_i replaced with $e_i + 1$ and e_j replaced with $e_j - 1$. So

$$sw(\mathbf{e}, i, j) = (e_1, \ldots, e_{i-1}, e_i + 1, e_{i+1}, \ldots, e_{j-1}, e_j - 1, e_{j+1}, \ldots, e_{\pi(x)})$$

In terms of n, this means

$$sw(\mathbf{e}, i, j) = \frac{p_i}{p_j} n$$

If $n = 2^2 * 3 * 5^2 = 300$, then $\mathbf{e} = (2, 1, 2)$ and

$$sw(\mathbf{e}, 1, 2) = (3, 0, 2) = 2^3 * 5^2 = 200$$

$$sw(\mathbf{e}, 1, 3) = (3, 1, 1) = 2^3 * 3 * 5 = 120$$

$$sw(\mathbf{e}, 2, 3) = (2, 2, 1) = 2^2 * 3^2 * 5 = 180$$

$$sw^2(\mathbf{e}, 1, 3) = (4, 1) = 2^4 * 3 = 48$$

And notice then that applying $sw(\mathbf{e}, 1, 2)$ to the last term gives $(5) = 2^5$. In fact, notice that sw is invariant on $\Omega(n) = \sum_i e_i$, so for any n, we can repeatedly apply different swaps to load all exponents onto a single prime. In other words, for a fixed n, its orbit contains at its extremes the values

$$p^{\Omega(n)}$$

For example, we have swaps like

$$sw(\mathbf{e}, 2, 1) = (1, 2, 2) = 2 * 3^2 * 5^2 = 450$$

$$sw(\mathbf{e}, 3, 1) = (1, 1, 3) = 2 * 3 * 5^3 = 750$$

$$sw(\mathbf{e}, 3, 2) = (2, 0, 3) = 2^2 * 5^3 = 500$$

$$sw^2(\mathbf{e}, 3, 1) = (0, 1, 4) = 3 * 5^4 = 1875$$

This definitely leads me to wanting to form a graph...and I've got to mention the critical group!

This was my second serious research project I ever did. We studied chip-firing on graphs, an action which allowed us to form a group from the graph called the Critical Group or Smith Group. This all relates to analyzing the cokernel of certain matrices, which is a topic that appears in a lot of spots.

So what is chip-firing? Fix a graph $G = (V, E)$ and a labeling $c : V \to \{0, 1, 2, \dots\}$ of the vertices. We define the chip-firing action on the graph as follows. Firing at a vertex v sends one chip along each edge adjacent to v, so $c'(v) = c(v) - deg(v)$ and $c'(w) = c(w) + 1$ for all vertices w adjacent to v.

We consider two labelings (configurations) c and c' to be equivalent if there is a series of chip-firing that leads you from c to c'. It turns out, this equivalence relation gives a group structure on the set of all configurations on G.

With an algebraic point of view, this group is essentially the cokernel of a matrix related to G. For the Smith Group, we take the cokernel of the adjacency matrix, and for the Critical Group, we take the cokernel of the Laplacian matrix.

The name *critical group* is also replaced with *Jacobian* or *Picard Group* because of its relation to the Picard Group of a symmetric monoidal category.

A few nice examples are

1. The critical group $\mathcal{K}(C_n)$ of the cycle graph on n vertices is $\mathbb{Z}/n\mathbb{Z}$.

2. The critical group of Kneser graphs on 2-element subsets was studied by my friend Ian Hill with my old research advisor Josh Ducey.

3. Our own project with a friend Noah Watson characterized the critical group of the Rook's graph as

$$\mathcal{K}(R_n) = (\mathbb{Z}/2n\mathbb{Z})^{(n-2)^2+1} \oplus (\mathbb{Z}/2n^2\mathbb{Z})^{2(n-2)}$$

4. And probably one of the coolest things I've seen is Dr. Josh Ducey proving the form of the critical group of the missing Moore graph, which we don't even know whether or not it exists!

After writing all that, I realized that if are trying to use chip-firing to denote our swap, then we'd need exactly two vertices p_i and p_j connected by an edge. Doing the swap is firing one of these vertices. But this graph for n would then be literally the disjoint union of edges (p_i, p_j) where we don't identify two edges with coordinate p_i. It would have to just $\omega(n)^2$ vertices with $\binom{\omega(n)}{2}$ edges.

The critical group of the edge consists of two classes $(0, 0)$ and $(1, 0)$, i.e. whether the sum of the vertices is even or odd. So the critical group of this graph would be

$$(\mathbb{Z}/2\mathbb{Z})^{\binom{\omega(n)}{2}}.$$

But this REALLY does not capture what we want.

So let's go back and define a graph $S(n)$ whose vertices correspond to all possible swaps starting from n, which an edge between two vertices if there is a single swap that takes you from one to another.

For example, if $n = p^a$ is a prime power, we have no swaps, so $S(n)$ is a single vertex. If $n = p^a q^b$, then we can swap all the way down to p^{a+b} and up to q^{a+b}. So if $\omega(n) = 2$, we have that $S(n)$ is a path graph on $\Omega(n) + 1$ vertices with endpoints $p_1^{\Omega(n)}$ and $p_2^{\Omega(n)}$.

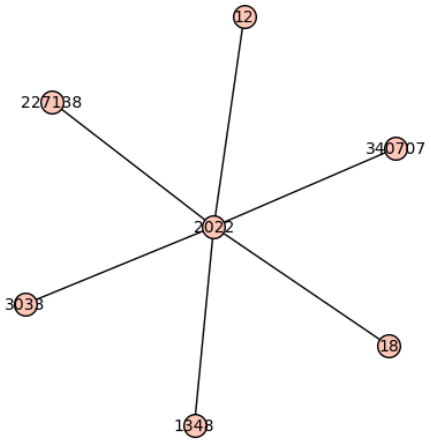
As well as the fact that $\Omega(n)$ is an invariant, we also have that all swaps have radical dividing $rad(n)$. This raises the natural question:

Question 4 *For a fixed integer n, how many integers m are there with $\Omega(m) = \Omega(n)$ and $rad(m)|rad(n)$?*

I really want to write up a program for that, but I'm trying to stay on topic! Let's begin coding up this graph $S(n)$. The following will generate the first level of this graph, applying a single swap.

```
def S(n):
    G = Graph()
    E=[]
    for i in range(1,om(n)+1):
        for j in range(1,om(n)+1):
            if i != j:
                E.append((n,sw(n,i,j)))
    G.add_edges(E)
    return G
```

For example, $S(2022) = S(2 * 3 * 337)$ is

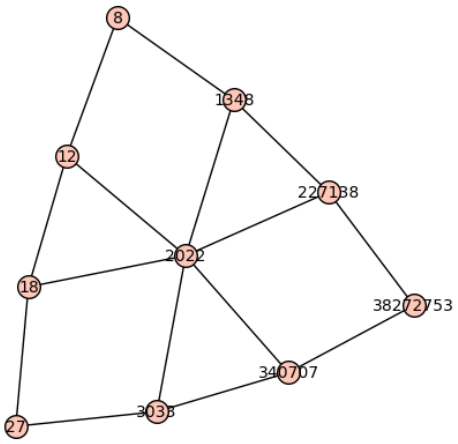


And the swapping function $sw(n, i, j)$ is defined as follows:

```
def sw(n,i,j):
    exp = [p[1] for p in list(factor(n))]
    if i > om(n) or j > om(n) or i < 1 or j < 1:
        return('Out of Bounds')
    else:
        exp[i-1] = exp[i-1]+1
        exp[j-1] = exp[j-1]-1
    return prod([list(factor(n))[i][0]^exp[i] for i in range(om(n))])
```

Now we need to implement a recursion to fill the tree out until done. Here is the final code, an example with 2022, and then an explanation of the code.

```
def S(n):
    G = Graph()
    E=[]
    TotalVerts = [n]
    NewVerts = []
    for i in range(1,om(n)+1):
        for j in range(1,om(n)+1):
            if i != j:
                E.append((n,sw(n,i,j)))
                NewVerts.append(sw(n,i,j))
    while len(NewVerts) != 0:
        for nn in NewVerts:
            NewVerts.remove(nn)
            print(NewVerts)
            for i in range(1,om(nn)+1):
                for j in range(1,om(nn)+1):
                    if i != j:
                        E.append((nn,sw(nn,i,j)))
                        if sw(nn,i,j) not in TotalVerts:
                            NewVerts.append(sw(nn,i,j))
                            TotalVerts.append(sw(nn,i,j))
    G.add_edges(E)
    return G
```



Which is honestly just awesome. It brings to mind a dozen possible conjectures (planar/genus/degrees/regularity/euler's formula/critical group,chromatic number/poly, what are the max/min values of the vertices, etc), but let's check a few more before we do that.

But first, let's go through the code.

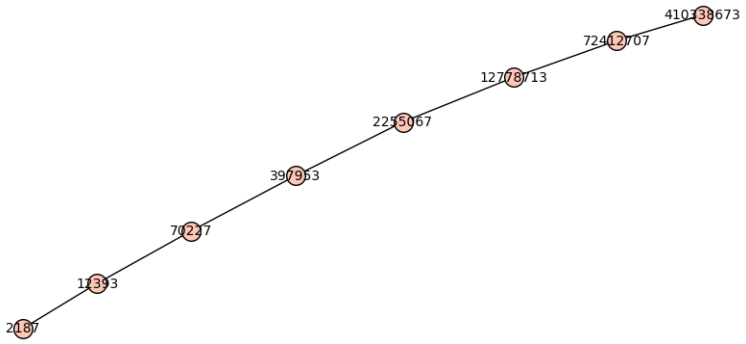
WARNING: SEEMS LIKE THIS COULD NOT BE CODED CORRECTLY, KEEPING SECTION TO REVISE.

Let's start at the first for loop. We added two lines after $E.append((n, sw(n, i, j)))$ to add that vertex to a set called $NewVerts$, which we initiate at the top with $NewVerts = []$. And we add it to a list of $TotalVerts = [n]$, which we initiate with n.

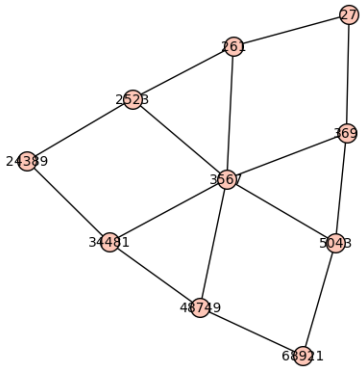
So we begin by generating this star. Then we go through the list $NewVerts$ that we made, remove it from NewVerts, and then go through the same process we just did with n. At the end, we check if $sw(nn, i, j)$ is already in TotalVerts so we know whether to add it to NewVerts or not.

Finally, to keep this going until we're done, we nest it all in a while loop as $while\ len(NewVerts)\ != 0$. Also, the print statements are for troubleshooting and can be removed.

Let's do some examples. Here is $S(397953)$, for which $\omega(397953) = 2$, so $S(397953)$ is a path graph of length $8 = \Omega(397953) + 1$, as discussed before.



What about $\omega(n) = 3$? Well, we will have these paths for each pair of prime divisors. So we get a triangle-shaped graph. The square-free n with $\omega(n)$ all look like $S(3 * 29 * 41)$ or $S(30)$ above



Testing properties for various graphs gives the following conjectures.

Conjecture 7 *For all $n \geq 1$, we have*

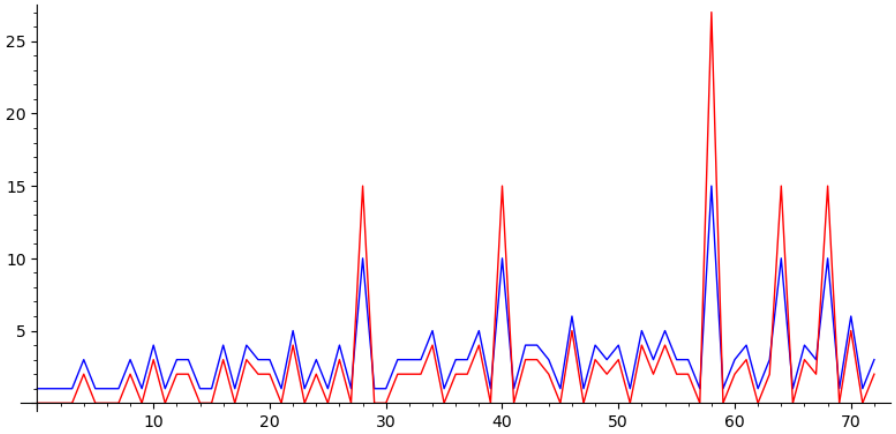
- *$S(n)$ is planar if and only if $\omega(n) \leq 3$.*
- *The chromatic number $\chi(S(n)) = \omega(n)$ is equal to the number of distinct prime divisors of n.*

This would mean that having $\omega(n) = 3$ would allow us to use Euler's Formula

$$v - e + f = 2$$

where v is the number of vertices, e is the number of edges, and f is the number of faces.

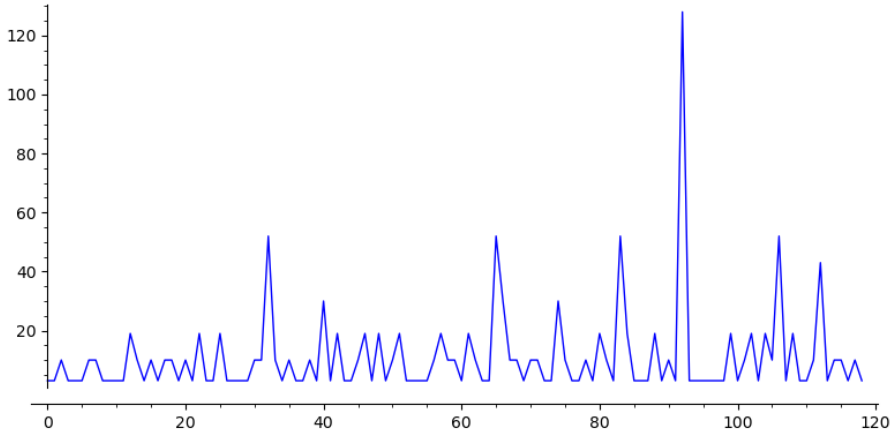
Let's go ahead and plot the numbers of vertices (blue) and the number of edges (red) for $S(n)$ for $n \leq 100$.



I did not expect it, but the number of vertices actually appears as OEIS sequence *A316314: Number of distinct nonempty-subset-averages of the integer partition with Heinz number n.*, so we have some reading to do on what that means! The sequence of numbers of edges does not appear on OEIS.

Another thing I'm very interested in is the number of triangles in $S(n)$, because they seem quite abundant. Of course, if $\omega(n) \leq 2$, then this count is zero. So here is a plot for $n < 500$ with $\omega(n) > 2$. Here is the list and the plot.

```
[3, 3, 10, 3, 3, 3, 10, 10, 3, 3, 3, 3, 19, 10, 3, 10, 3, 10, 10,
3, 10, 3, 19, 3, 3, 19, 3, 3, 3, 3, 10, 10, 52, 10, 3, 10, 3, 3,
10, 3, 30, 3, 19, 3, 3, 10, 19, 3, 19, 3, 10, 19, 3, 3, 3, 3, 10,
19, 10, 10, 3, 19, 10, 3, 3, 52, 30, 10, 10, 3, 10, 10, 3, 3, 30,
10, 3, 3, 10, 3, 19, 10, 3, 52, 19, 3, 3, 3, 19, 3, 10, 3, 128, 3,
3, 3, 3, 3, 3, 19, 3, 10, 19, 3, 19, 10, 52, 3, 19, 3, 3, 10, 43,
3, 10, 10, 3, 10, 3]
```

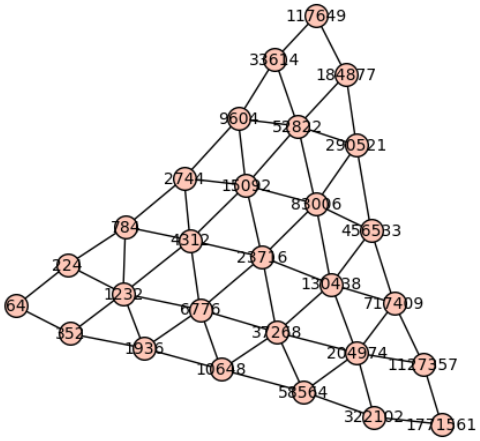


And just as a cool aside, I wanted to mention how we can count triangles. If A is the adjacency matrix of a graph G, then the (i, j) entry in A^k counts the number of paths of length k from vertex i to j. So the diagonal entries (i, i) of the matrix A^3 counts the number of paths of length 3 from i back to itself. But this is exactly a triangle!

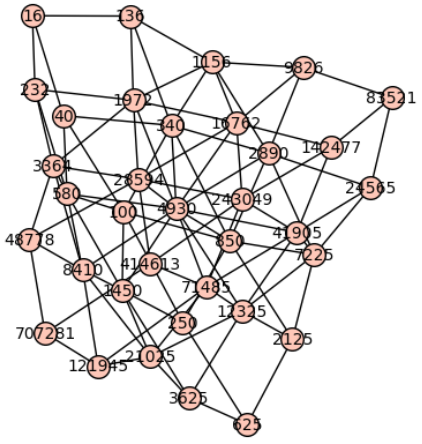
Therefore, we can take the trace of A^3 and find the number of triangles in G, except for the fact that we overcounted slightly. Each triangle has 3 vertices, so we must divide by 3!. Therefore, the number of triangles in G is

$$Tr(A^3)/6.$$

Now, let's plot a few more examples.
With $n = 2^3 * 7 * 11^2$, then $S(n)$ is



With $n = 2 * 5 * 17 * 29$, we have



You can see that this does not look planar, and indeed it is not.

But what does a triangle in $S(n)$ mean? It means there are three vertices v_1, v_2, v_3 that can be swapped in a three-cycle. For example, take

$$p^2qr, \quad sw(p^2qr, 2, 1) = pq^2r, \quad sw(pq^2r, 3, 2) = pqr^2, \quad sw(pqr^2, 1, 3) = p^2qr.$$

More generally, for any three primes p_i, p_j, p_t, we have the 3-cycle

$$sw(v_1, j, i) = v_2$$

$$sw(v_2, t, j) = v_3$$

$$sw(v_3, t, i) = v_1$$

And this will always work provided the exponent on p_i is at least 2. Recall our definition of $rad_k(n)$, the product of primes p for which $p^k|n$. Therefore, the primes we're interested in are those in $rad_2(v)$. Then we can choose any other pair of prime numbers. This gives $\omega(rad_2(v))\binom{\omega(n)-1}{2}$. But this overcounts. For example, the second part of the product could involve a prime that is also in $rad_2(v)$.

Let's go back to something mentioned long ago: The Handshaking Lemma! This tells us that

$$2|E| = \sum_{v \in V} deg(v)$$

The degree of v seems like it should be a simple $\omega(v)^2 - \omega(v)$, but this isn't totally true. We note that $sw(n, i, j)$ is only invertible if $sw(n, i, j)$ is divisible by p_i and p_j. In that case,

$$sw(sw(n, i, j), j, i) = n$$

But if $p_j||n$, then $sw(n, i, j)$ will not be divisible by p_j, so we won't be able to recover the prime p_j from here. If we have a vertex v with $rad_2(v) = rad(v)$ (or equivalently, $\beta(v) \geq 2$), then all swaps from v will be invertible, so $deg(v) = \omega(v)^2 - \omega(v)$. And for each prime dividing n that doesn't divide v, we have an incoming swap that is non-invertible as long as there is a prime dividing v with exponent at least 2. This adds $(\omega(n) - \omega(v))\omega(rad_2(v))$ to the degree. So in total,

$$deg(v) = \omega(v)^2 - \omega(v) + (\omega(n) - \omega(v))\omega(rad_2(v))$$

For example, this shows why $deg(9604)$ has degree 4 in $S(2^3 * 7 * 11^2)$. We have $\omega(n) = 3, \omega(v) = 2$, and $\omega(rad_2(v)) = 2$, so

$$deg(9604) = 2^2 - 2 + (3 - 2)(2) = 2 + 2 = 4.$$

For the endpoint vertices $p^{\Omega(n)}$, we have only incoming swaps, so

$$deg(p^{\Omega(n)}) = \omega(n) - 1,$$

assuming $\Omega(n) \geq 2$. Applying the handshaking theorem tells us

$$2|E| = \sum_{v \in V} deg(v) = \sum_{v \in V} \omega(v)^2 - \omega(v) + (\omega(n) - \omega(v))\omega(rad_2(v))$$

Consider a vertex $v \in V$ for the graph $S(n)$. Then $rad(v)|rad(n)$ and $\Omega(v) = \Omega(n)$. And if these conditions hold, then v is a vertex in $S(n)$. So the answer to Question 4, asking for the number of integers v with those two properties, is exactly the number of vertices of $S(n)$.

And analyzing this is easy if we just remember partitions and compositions. If we have a vertex, then the exponents form a weak integer composition of $\Omega(n)$ into $\omega(n)$ parts. A standard stars-and-bars argument shows that the number of such compositions is

$$\binom{\Omega(n) + \omega(n) - 1}{\omega(n) - 1}$$

and therefore, this is the size of the vertex set of $S(n)$.

Here's a theorem that could be helpful in proving $S(n)$ is not planar if $\omega(n) > 3$.

Theorem 19 *If G is a simple planar graph, then*

$$|E| \leq 3n - 6$$

When we mentioned Conjecture 7, we mentioned Euler's formula for planar graphs that says $v - e + f = 2$. To prove the theorem, we maximize this for e. The number of edges will be maximal when all faces are triangles, otherwise we could add an edge to bisect a non-triangular region. Since each triangle has three edges, we might expect $e = 3f$, but each edge will be contained in two faces, so we actually have $2e = 3f$. Plugging this into Euler's formula gives

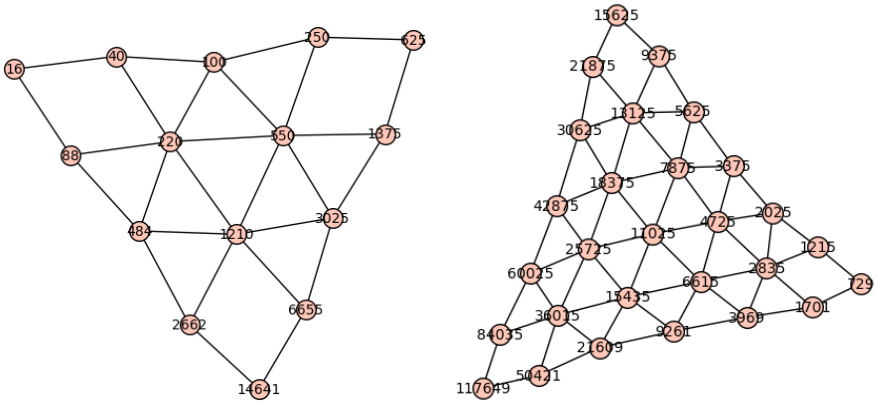
$$v - e + (2/3)e = 2$$

$$v - (1/3)e = 2$$

$$e = 3v - 6$$

So showing this bound is exceeded if $\omega(n) > 3$ would prove these graphs are not planar.

Let's try to count edges. First, if $\omega(n) = 1$, we have no edges. If $\omega(n) = 2$, then the number of edges is $\Omega(n) + 1$, since we have swaps from $p^{\Omega(n)}$ to $q^{\Omega(n)}$. The number of vertices in this case is $\Omega(n)$. If $\omega(n) = 3$, then our graphs get interesting. Take $S(2 * 5^2 * 11) = S(550)$ and $S(3^3 * 5 * 7^2) = S(6615)$.



So we can start at a corner and move along its rows adding up edges: $0 + 0 + 2 + 3 + 4 = 9$. If we do this starting at all 3 corners, we get 27 edges for $S(550)$ and $3(0 + 0 + 2 + 3 + 4 + 5 + 6) = 60$ for $S(6615)$. And this in general gives us our theorem.

Theorem 20 *For $\omega(n) = 3$, the number of edges of $S(n)$ is*

$$3(0 + 0 + 2 + \cdots + \Omega(n)) = 3\left(\binom{\Omega(n)+1}{2} - 1\right)$$

We will still have to prove this, of course. But first, let's see if we can say anything about $\omega(n) = 4$. Fun fact, if you want to be able to move the vertices and actually play with the graph, use $show(G, layout = `spring')$ for a graph G instead of $plot(G)$.

Similar to before, we seem to have lots of triangles and then an empty cube at each of the four corners. But I just remembered an old strategy - look at the degree sequence and count the appearances of each degree. There tends to be a pattern that is clearer in that way. Then we can use the Handshaking Lemma to count the edges that way!

For example, if $\omega(n) = 2$, then

$$2|E| = \sum_{v \in V} deg(v) = \sum_{v \in V} \omega(v)^2 - \omega(v) + (\omega(n) - \omega(v))\omega(rad_2(v))$$

$$= \sum_{\substack{v \in V \\ \omega(v)=2}} 2 + \sum_{\substack{v \in V \\ \omega(v)=1}} \omega(rad_2(v))$$

All vertices are of the form $v = p^a q^b$, so we'll have $\Omega(n)-1$ vertices with $\omega(n) = 2$ and the two endpoints $p^{\Omega(n)}$ and $q^{\Omega(n)}$ with $\omega(n) = 1$ have $\omega(rad_2(v)) = 1$, which means

$$|E| = \frac{1}{2}(2(\Omega(n) - 1) + 2) = \Omega(n)$$

If $\Omega(n) = 3$, we can split the sum into three parts,

$$2|E| = \sum_{\substack{v\in V\\ \omega(v)=3}} 6 + \sum_{\substack{v\in V\\ \omega(v)=2}} (2+\omega(rad_2(v))) + \sum_{\substack{v\in V\\ \omega(v)=1}} 2\omega(rad_2(v))$$

In general, since $\Omega(n) \geq 2$, any vertex with $\omega(v) = 1$ will have $\omega(rad_2(v)) = 1$. And we will have $\omega(n)$ such vertices, for a total contribution of

$$2\omega(n)$$

If $\omega(v) = \omega(n)$, then the exponents of v are a (non-weak) composition of $\Omega(n)$ into $\omega(n)$ parts, of which there are $\binom{\Omega(n)-1}{\omega(n)-1}$, for a total contribution of

$$\binom{\Omega(n)-1}{\omega(n)-1}\omega(n)(\omega(n)-1)$$

Let's go back to the $\omega(n) = 3$ case specifically. This tells us we have $\omega(v) = 1$, we get a contribution of 6. When $\omega(n) = 3$, we have $6\binom{\Omega(n)-1}{2}$. If $\omega(v) = 2$, then $v = p_i^a p_j^b$ where $a + b$ form a composition of $\Omega(n)$ and we have $\binom{3}{2} = 3$ choices for the pair of primes. This gives a total of $3\binom{\Omega(n)-1}{2-1} = 3(\Omega(n)-1)$ such vertices. But we need to know $\omega(rad_2(v))$, which will be 1 only if $a = 1$ or $b = 1$. So we have a total contribution of

$$(3\Omega(n)-5)(2+2) + 2(2+1) = 12\Omega(n) - 14$$

Therefore,

$$|E| = \frac{1}{2}\left(6 + 12\Omega(n) - 14 + 6\binom{\Omega(n)-1}{2}\right) = 3\left(\binom{\Omega(n)+1}{2} - 1\right)$$

So we recover the same count we got before! But, this will hopefully get us the edge count for all $S(n)$. The strategy is clear, split it by $\omega(v)$ and count how many v there are.

$$\begin{aligned}
2|E| = \sum_{v\in V} deg(v) &= \sum_{v\in V} \omega(v)^2 - \omega(v) + (\omega(n) - \omega(v))\omega(rad_2(v)) \\
&= \sum_{k=1}^{\omega(n)} \sum_{\substack{v\in V\\ \omega(v)=k}} k^2 - k + (\omega(n)-k)\omega(rad_2(v)) \\
&= \sum_{k=1}^{\omega(n)} k^2 - k + \sum_{\substack{v\in V\\ \omega(v)=k}} (\omega(n)-k)\omega(rad_2(v))
\end{aligned}$$

Now we'll split the inner sum based on $\omega(rad_2(v))$ given $\omega(v) = k$.

$$2|E| = \sum_{k=1}^{\omega(n)} k^2 - k + \sum_{h=1}^{k} \sum_{\substack{v\in V\\ \omega(v)=k\\ \omega(rad_2(v))=h}} (\omega(n)-k)h$$

Now if $\omega(v) = k$ and $\omega(rad_2(v)) = h$, then from the k primes dividing v, we choose $k - h$ primes for the square-free part of v. For the remaining part, we have h primes whose exponents are all at least 2 and add up to $\Omega(n) - k + h$.

So we can subtract one from each of those exponents, and we get a (non-weak) composition of $\Omega(n) - k$ into h parts. Putting all this together, we have

$$\binom{k}{k-h}\binom{\Omega(n)-k-1}{h-1}$$

vertices v.

Plugging this into our handshaking lemma sum:

$$\begin{aligned}
2|E| &= \sum_{k=1}^{\omega(n)} k^2 - k + \sum_{h=1}^{k} \binom{k}{k-h}\binom{\Omega(n)-k-1}{h-1}(\omega(n)-k)h \\
&= \sum_{k=1}^{\omega(n)} k^2 - k + (\omega(n)-k)\sum_{h=1}^{k} \binom{k}{k-h}\binom{\Omega(n)-k-1}{h-1}h \\
&= \sum_{k=1}^{\omega(n)} k^2 - k + (\omega(n)-k)\sum_{h=1}^{k} \binom{k}{k-h}\binom{\Omega(n)-k-1}{h-1}h
\end{aligned}$$

Vandermonde's Convolution Identity might be helpful: it tells us that for any m, n, we have

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}$$

Setting $m = \Omega(n) - k$ and $n = k$, we have that

$$\sum_{h=0}^{k} \binom{k}{k-h}\binom{\Omega(n)-k}{h} = \binom{\Omega(n)}{k},$$

which comes from the fact that

$$(1+x)^k(1+x)^{\Omega(n)-k} = (1+x)^{\Omega(n)}$$

But the inside isn't quite that. Let's manipulate it slightly. We have

$$(\omega(n)-k)\sum_{h=1}^{k} \binom{k}{k-h}\binom{\Omega(n)-k-1}{h-1}h = \frac{\omega(n)-k}{\Omega(n)-k}\sum_{h=1}^{k} \binom{k}{k-h}\binom{\Omega(n)-k}{h}h^2$$

The last sum with the h^2 term comes from taking a derivative of $(1+x)^{\Omega(n)}$, multiplying by x, taking another derivative, and multiplying by x again:

$$\Omega(n)x(\Omega(n)x+1)(1+x)^{\Omega(n)-2}$$

Isolating the coefficient of x^k gets $\Omega(n)\binom{\Omega(n)-2}{k-1}$ from the $\Omega(n)x$, and then gets $\Omega(n)^2\binom{\Omega(n)-2}{k-2}$ from the $\Omega(n)^2x^2$. This tells us

$$\sum_{h=1}^{k}\binom{k}{k-h}\binom{\Omega(n)-k}{h}h^2=\Omega(n)\binom{\Omega(n)-2}{k-1}+\Omega(n)^2\binom{\Omega(n)-2}{k-2}$$

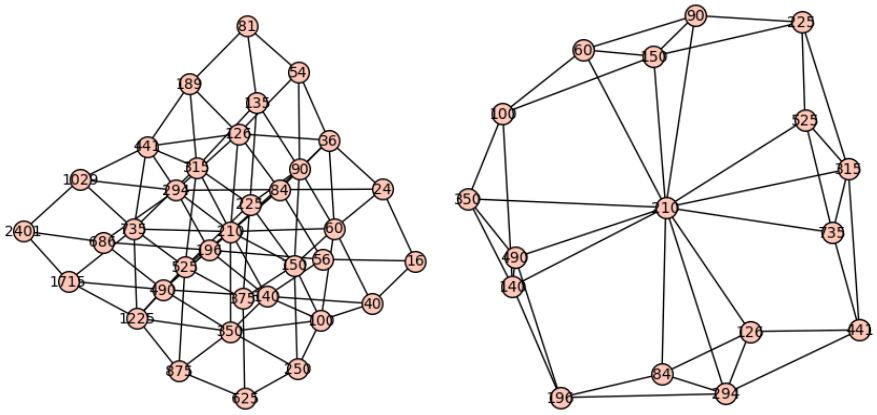
So we finally get another expression for the number of edges as

$$2|E|=\sum_{k=1}^{\omega(n)}k^2-k+\left(\frac{\omega(n)-k}{\Omega(n)-k}\right)\left(\Omega(n)\binom{\Omega(n)-2}{k-1}+\Omega(n)^2\binom{\Omega(n)-2}{k-2}\right)$$

Also, this is a good time to bring in one of the coolest characterizations ever - the graph minor theorem (or Robertson-Seymour Theorem). Here is the motivating example.

Theorem 21 (Kuratowski's Theorem) *A graph G is planar if and only if it does not contain a subdivision of K_5 or $K_{3,3}$ as a subgraph.*

This spawned dozens of very interesting questions and theorems and methods, extending to matroids and other mathematical objects. To see how we'll use it, we'll look at the graph $S(2*3*5*7)=S(210)$ and a non-planar subgraph.



The subgraph is essentially two iterations of the algorithm to build our graph. This is symmetric, so look at the top portion of the right graph and consider the copy of K_4 given by $(60, 90, 150, 210)$. Then we just need to find one vertex connected to each of these by disjoint paths. Take 225, which is already connected to 90 and 150. Then 225 is connected to 210 by $(225, 525, 210)$. Finally, we use the large outside loop to connect 225 to 60 with $(225, 315, 441, 294, 196, 140, 350, 100, 60)$. Therefore, $S(210)$ contains a subdivision of K_5 as a graph and is non-planar.

This gives a good idea for a general strategy. The idea of containing a subgraph that is a subdivision of K_5 is equivalent to showing there is a graph homomorphism from K_5 to our graph. A graph homomorphism between two

graphs G and H is defined as a map between vertices $\phi : V(G) \to V(H)$ such that edges are mapped to edges. Importantly, we don't require non-edges be mapped to non-edges, so two vertices disconnected in G could be connected in $\phi(G)$.

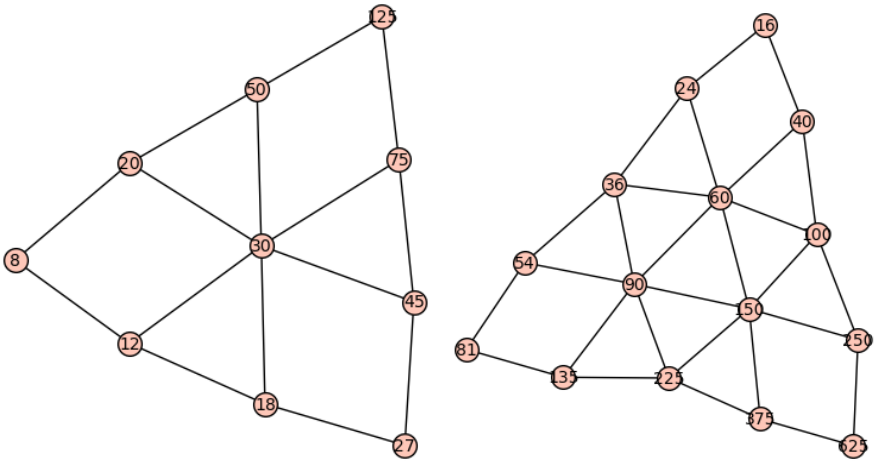
We'll go about proving these non-planar by proving it for $S(n)$ for square-free n with $\omega(n) \geq 4$, and then showing that all n that are not square-free have some square-free n' so that there exists a graph homomorphism of $S(n')$ into $S(n)$, showing $S(n)$ is non-planar.

Lemma 1 *There exists a homomorphism $\phi : S(n) \to S(m)$ if and only if $\omega(n) \leq \omega(m)$. And $S(n)$ and $S(m)$ are homomorphically equivalent iff $\omega(n) = \omega(m)$ and isomorphic iff $\Omega(n) = \Omega(m)$ as well.*

Here is an example to work with, $S(2*3*5) = S(30)$ and $S(2*3*5^2) = S(150)$. The first list is a homomorphism from $S(30) \to S(150)$ and the second is a homomorphism from $S(150) \to S(30)$.

```
{30: 150, 20: 60, 12: 60, 45: 60, 18: 100, 75: 100, 50: 100,
27: 150, 125: 150, 8: 150}
```

```
{150: 30, 100: 20, 60: 50, 225: 50, 90: 20, 375: 20, 250: 50,
40: 30, 135: 30, 625: 30, 24: 20, 36: 30, 54: 50, 81: 20, 16: 50}
```



So this would tell us that $S(n) \to S(m)$ if and only if $\omega(m) \geq \omega(n)$. So proving $S(n)$ is non-planar for $\omega(n) \geq 4$ is equivalent to showing that a single graph with $\omega(n) = 4$ is non-planar. For example, $S(2 * 3 * 5 * 7)$, which we already did! QED. That turned out simpler than we expected, though we still need to prove the lemma.

Now, thanks to some wonderfully written code from Noah Watson from around 2015, we can also compute the critical groups of these graphs and see if there are any patterns!

The critical group of a tree is trivial, so we only need to look at $\omega(n) \geq 3$. I also swear I remember reading bounding the size of the factors of the critical group by the number of triangles in the graph, but I can't find it right now. Anyway, the critical group decomposes as a product of finite cyclic groups whose order arise as elementary divisors of the Laplacian matrix of our graph. Let's define all that!

The Laplacian matrix of a graph G is $L = D - A$ where D is a diagonal matrix with $\deg(v)$ in spot (v, v) and A is the adjacency matrix of G. Then this cokernel has a single infinite term, and the finite (torsion) part of it is the critical group $\mathcal{K}(G)$ of G.

The cokernel of L is a finitely generated module over the PID $\mathbb{Z}$, so the structure theorem guarantees us a decomposition into cyclic factors, and those are our elementary divisors. We can also get them via Smith Normal Form, which Richard Stanley and others have many interesting talks on.

We've established that $S(n)$ is determined up to isomorphism by the pair $(\omega(n), \Omega(n))$, so we'll write $\mathcal{K}(a, b)$ with $a \leq b$ to stand for $\mathcal{K}(n)$ for any n with $\omega(n) = a$ and $\Omega(n) = b$. Let's compute $\mathcal{K}(a, a)$ first.

$$\mathcal{K}(3,3) = (\mathbb{Z}/11\mathbb{Z}) \times (\mathbb{Z}/88\mathbb{Z})$$

$$\mathcal{K}(4,4) = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/283960\mathbb{Z}) \times (\mathbb{Z}/22432840\mathbb{Z}) \times (\mathbb{Z}/269194080\mathbb{Z})$$

and the elementary divisors for $\mathcal{K}(5, 5)$ are

```
[4, 4, 4, 4, 8, 8, 8, 8, 8, 8, 80, 70320, 933568109040,
246520286782810093200, 246520286782810093200,
246520286782810093200, 739560860348430279600]
```

That is, they get large very quick when adding a new prime! What if we fix $\omega(n)$ and iterate $\Omega(n)$.

$$\mathcal{K}(3,4) = (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/414\mathbb{Z})^2$$

$$\mathcal{K}(3,5) = (\mathbb{Z}/4044\mathbb{Z}) \times (\mathbb{Z}/339696\mathbb{Z})$$

$$\mathcal{K}(3,6) = (\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/72462\mathbb{Z}) \times (\mathbb{Z}/43114890\mathbb{Z})$$

Going back for a moment to the edge count, I recalled Turan's theorem, which tells us

Theorem 22 (Turan's Theorem) *If $H = K_r$ is the complete graph on r vertices, then the maximal number of edges in a K_r-free graph on n vertices is*

$$\left(1 - \frac{1}{r-1}\right)\frac{n^2}{2}$$

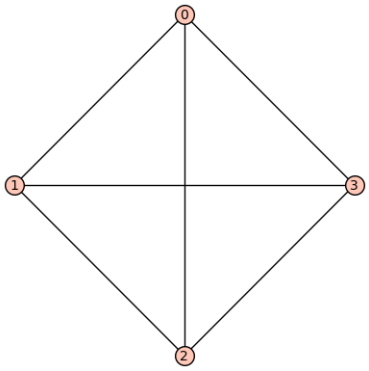
This might be helpful because it seems that $S(n)$ never contains a K_4. Let's see if we can prove this.

Proposition 1 *For all n, the graph $S(n)$ is K_4-free.*

Proof 2 *If $S(n)$ contains a copy of K_4, then we have four vertices v_0, v_1, v_2, v_3, all connected by swaps. We'll assume that we have edges between*

$$(v_0, v_2), (v_0, v_1), (v_0, v_3), (v_2, v_3), (v_1, v_2)$$

and then show that (v_1, v_3) cannot also be an edge.



STOP: I'm unsure why the four vertices

$$(p_1^2 p_2^2 p_3^2 p_4^2)$$
$$(p_1^3 p_2 p_3^2 p_4^2)$$
$$(p_1^3 p_2^2 p_3^1 p_4^2)$$
$$(p_1^3 p_2^2 p_3^2 p_4)$$

wouldn't provide a K_4 inside $S(n)$? Maybe my program generating $S(n)$ is messed up and not adding all the edges it can.

11 An Exposition of Some Papers

12 On Conjecture 1

Though the concept of upper/lower-semi friends is fun in my opinion, the actual use of $E(n, q)$ and all that seems to boil back down to $\sigma(n)$ anyway. For example, here is a proof of Greening's Theorem.

Theorem 23 *If $gcd(n, \sigma(n)) = 1$, then n is solitary.*

If $gcd(n, \sigma(n)) = 1$, then we have that $\nu_q(p^{\nu_p(n)+1} - 1) - \nu_q(p-1) > 0$ implies $\nu_q(n) = 0$. So for any $q|\sigma(n)$, we'll have $E(n, q) = \nu_q(\sigma(n))$, and otherwise $E(n, q) = 0$. So $N(n) = \sigma(n)$.

For any $p|n$, we know p does not divide $\sigma(n)$, so $E(n, p) = 0$ and $\overline{E}(n, p) = \nu_p(n)$, which means $D(n) = n$. If n had a friend m, then $D(m) = D(n)$ implies $m = n$, so we're done: n is solitary.

Can we apply any of what we've learned to try to prove Loomis' theorem?

Theorem 24 *If n is odd and $gcd(n^2, \sigma(n^2))$ is square-free, then n^2 is solitary.*

Let $gcd(n^2, \sigma(n^2)) = p_1 \dots p_t$. We discussed before that an odd square has an odd sum of divisors, so n^2 and $\sigma(n^2)$ are both odd. If m is a friend of n, then $m = \frac{n^2}{p_1 \dots p_t}\ell$ for some integer $\ell \not\equiv 0 \ mod \ p_1 \dots p_t$, and since $\nu_p(n^2) \geq 2$ for all $p|n$, we have $rad(n)|rad(m)$.

What is the relationship for abundancies of n and m when $rad(n)|rad(m)$? Remember that if $n|m$, then $\mathcal{A}(n) < \mathcal{A}(m)$. Via testing, it is not enough to say that $rad(n)|rad(m)$ and $\Omega(n) < \Omega(m)$ implies $\mathcal{A}(n) < \mathcal{A}(m)$. It seems to need a bit more nuance.

I'm not sure this is the key, but let's try. We'll define the *radical average (rad_avg)* of n to be the unique value of k so that

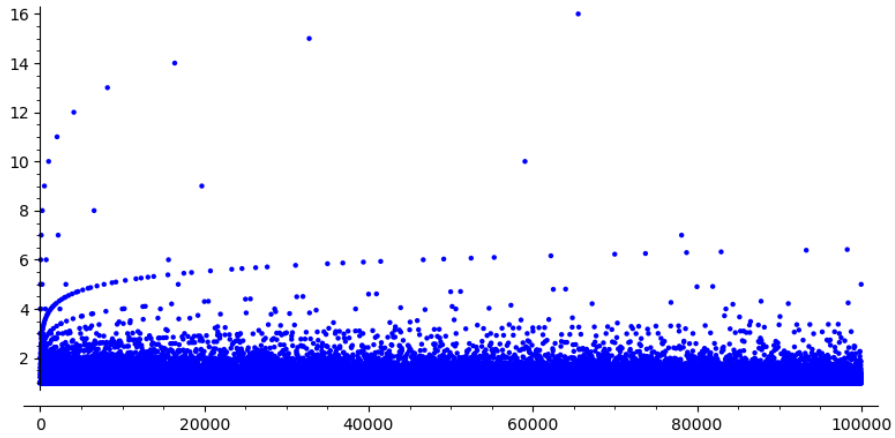
$$n = rad(n)^k.$$

Of course, we can explicitly solve for k and get

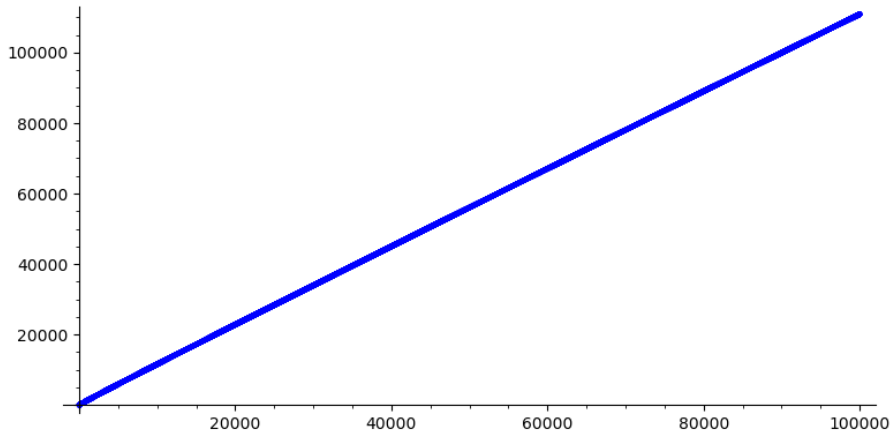
$$rad\_avg(n) = \frac{log(n)}{log(rad(n))} = \frac{\sum_{p|n} \nu_p(n) log(p)}{\sum_{p|n} log(p)}$$

We write it out in the last step to emphasize it really is an average of the exponents, but a weighted average (by $logp$) instead of the usual arithmetic average $\Omega(n)/\omega(n)$.

Here is a plot of radical averages for $n \leq 100000$. Notice the square-free integers form the line $y = 1$.



and here is a plot of $\sum_{n \leq x} rad\_avg(n)$ for $x = 100000$.



The value here is 1.1109, so it really seems like it might have average order 1. In addition to the square-free statement, we can also say that $rad\_avg(p^a) = \frac{1}{a}$ for all primes p and positive integers a. That means a portion of our sum is

$$\sum_{\substack{n \leq x \\ squarefree}} 1 + \sum_{2 \leq a \leq x} \sum_{p \leq x^{1/a}} \frac{1}{a}$$

The prime number theorem tells us the inner sum is approximately

$$\frac{x^{1/a}}{alog(x^{1/a})} = \frac{x}{alogx}$$

and the first sum is approximately $x/\zeta(2)$. So the portion we're describing becomes

$$\frac{x}{\zeta(2)} + \frac{x}{logx} \sum_{2 \leq a \leq x} \frac{1}{a}$$

$$= \frac{x}{\zeta(2)} + \frac{xlog(log(x))}{log(x)},$$

which isn't enough to deduce the average order being 1, just bounded below by $1/\zeta(2)$. But it seems the logical choice would be the to split the sum based on $\omega(n)$. For $\omega(n) = 2$, we have

$$rad\_avg(p^a q^b) = \frac{alog(p) + blog(q)}{log(p) + log(q)}$$

Basic estimate of $log(p) < log(q)$ gives

$$\left(\frac{a+b}{2}\right)\frac{log(p)}{log(q)} \leq rad\_avg(p^a q^b) \leq \left(\frac{a+b}{2}\right)\frac{log(q)}{log(p)}$$

And in general, choosing the smallest and largest primes $p_1, p_{\omega(n)}$, we have

$$\left(\frac{\Omega(n)}{\omega(n)}\right)\frac{log(p_1)}{log(p_{\omega(n)})} \leq rad\_avg(p^a q^b) \leq \left(\frac{\Omega(n)}{\omega(n)}\right)\frac{log(p_{\omega(n)})}{log(p_1)}$$

Denoting $\Omega(n)/\omega(n)$ as $arith\_avg(n)$, we get

$$\frac{log(p_1)}{log(p_{\omega(n)})} \leq \frac{rad\_avg(n)}{arith\_avg(n)} \leq \frac{log(p_{\omega(n)})}{log(p_1)}$$

Now where in this interval does it truly lie? To get a feel for this, We'll count how many n have their ratio of radical and arithmetic averages closer to the lower bound than the upper. This seems to often be the case!

$$\begin{aligned} x = 100 \quad & 0.63 \\ x = 1000 \quad & 0.80 \\ x = 10000 \quad & 0.8693 \\ x = 100000 \quad & 0.90203 \\ x = 1000000 \quad & 0.920868 \end{aligned}$$

It certainly seems like this tends to 1.

Anyway, it seems like the radical-average doesn't follow any nice patterns with $\mathcal{A}(n)$ that are immediately clear. For example, increasing lists of friends don't have increasing radical average. The radical average of $\sigma(n)$ could be higher or lower than the radical average for n. In fact, the proportion of n with $rad\_avg(n) < rad\_avg(\sigma(n))$ is

$$\begin{aligned} x = 1000 \quad & 0.7 \\ x = 10000 \quad & 0.7789 \\ x = 100000 \quad & 0.82637 \end{aligned}$$

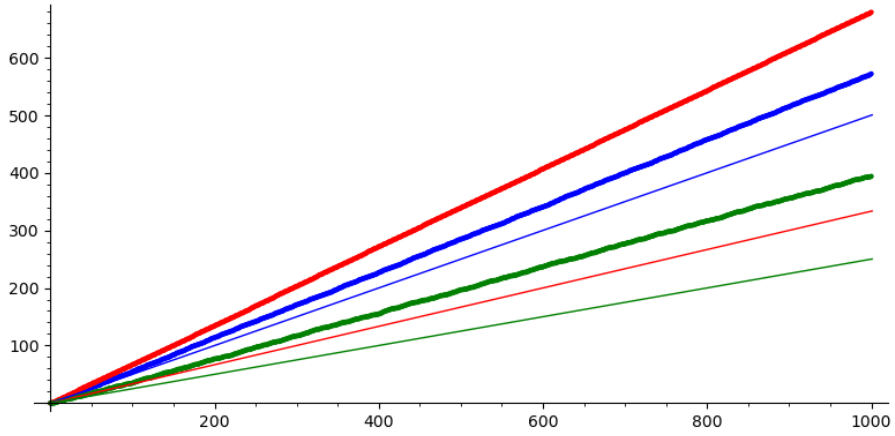
So perhaps this proportion will also go to 1?

Let's go back to the conjecture. I just realized something obvious I hadn't calculated yet. Greening's Criterion is proven from the fact that $n|m$ implies $\mathcal{A}(n) < \mathcal{A}(m)$. So let's look at the set

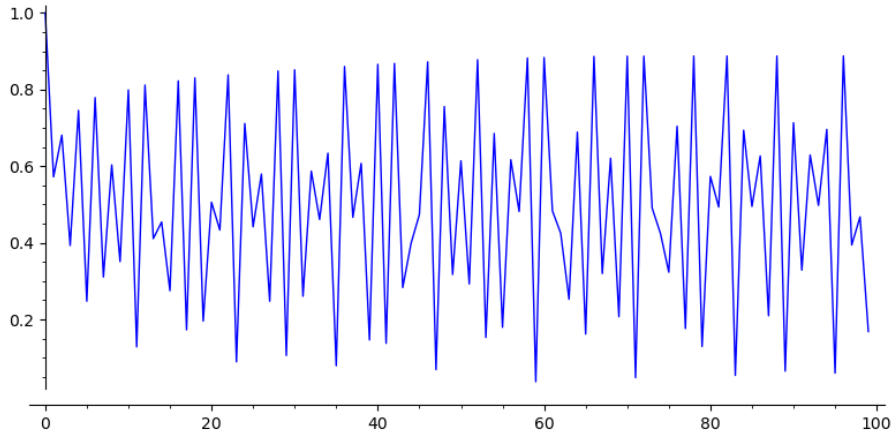
$$U(n) = \{m \mid \mathcal{A}(n) < \mathcal{A}(m)\}$$

Naturally, we write $U(n, x)$ when looking for $m \leq x$. Then the previous fact shows that $U(n)$ contains $\{2n, 3n, \dots\}$. This shows the density of $U(n)$ is at least $1/n$. Can we characterize any other subsets of $U(n)$? If the density of $U(n)$ is greater than $1/n$, we could have some non-trivial condition that n is solitary differing from Greening's Criterion.

Plotting $U(n, x)$ for $n = 2$ (blue), $n = 3$ (red), $n = 4$ (green) and $x = 10000$ shows the density most likely is higher. The bold lines are $U(n, x)$ and the lighter lines are x/n. The true density estimates at $x = 10^5$ are 0.57178 for $n = 2$, and 0.68132 for $n = 3$, and 0.39274 for $n = 4$.



Plotting these densities for $n \leq 100$ gives the following plot.



If the density of $U(n)$ was strictly greater than $1/n$, then we could remove the set $\{2n, 3n, \dots\}$ and still have a set of positive density. Szemeredi's Theorem then would tell us $U(n)$ will have arbitrarily long arithmethic progressions. However, we have no such guarantee for infinitely long arithmetic progressions. In fact, we can construct sets with density 1 with no infinite arithmetic progressions; specifically by removing one term from each arithmetic progression, so that the set of terms has density 0.

So does the existence of arbitrarily long arithmetic progressions help construct any solitary tests? That's iffy. The $\{2n, 3n, \dots\}$ progression being infinite allows us to say that $n|m \Rightarrow \mathcal{A}(n) < \mathcal{A}(m)$ even though m could be arbitrarily large.

In fact, having any infinite arithmetic sequence $\{a+kd\} \in U(n)$ would allow us to derive a condition for a number to be solitary: if $m \equiv a \ mod \ d$, then $\mathcal{A}(n) < \mathcal{A}(m)$, so m and n can't be friends. Therefore, if some condition on

friendship forces the friend to be $m \equiv a \ mod \ d$, this would show n is solitary. And it would increase our knowledge of the density of $U(n)$ by $\frac{1}{d} - \frac{1}{lcm(n,d)}$.

Though arbitrarily long, the arithmetic progressions guaranteed by Szemeredi are finite. Results of a more infinite nature concerning sets of positive density should also be looked at! In particular, again motivated by Erdos, it can be proven that any set A of positive density contains, for any k, a sumset $B_1 + B_2 + \cdots + B_k$, where $B_i \subset \mathbb{N}$ are infinite. The sumset being defined as you'd expect:

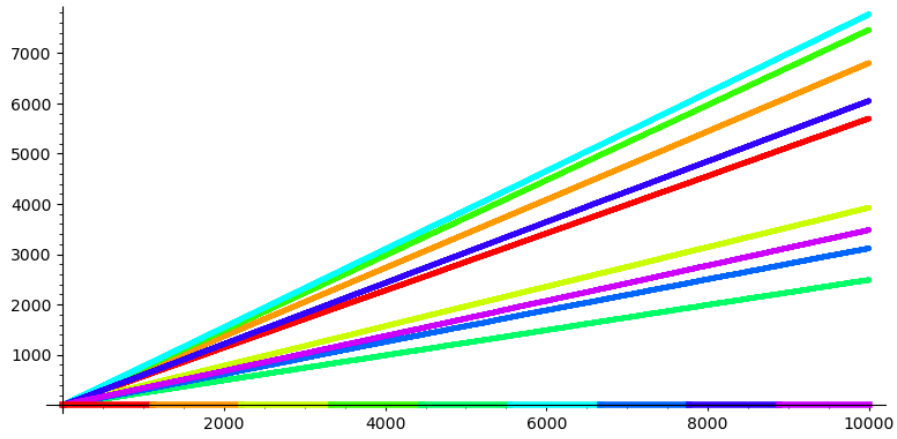
$$B_1 + \cdots + B_k = \{b_1 + \cdots + b_k \mid b_i \in B_i\}.$$

Proof methods for Szemeredi's Theorem often use Ergodic theory and this interaction has been strengthened since. We can look at Bryan Kra's Ergodic Methods in Additive Combinatorics for an overview, and also at one of his (and others') paper giving a proof of the statement in the last paragraph. However, that is a tough paper for me - I have a lot to read about to be prepared for that!

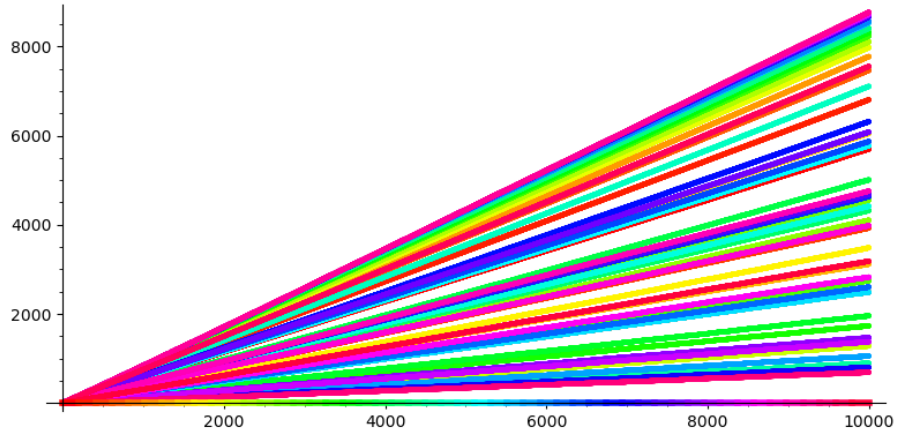
Anyway, let's go ahead and plot

$$\sum_{\substack{m \leq x \\ m \in U(n)}} 1$$

for $n = 2, \ldots, 10$. The evenly divided colored line at the bottom is the legend, i.e. 2 is red, 3 is orange, 4 is yellow, and so on.



And although it's hard to tell some colors apart, let's ramp up the number of examples to 50?



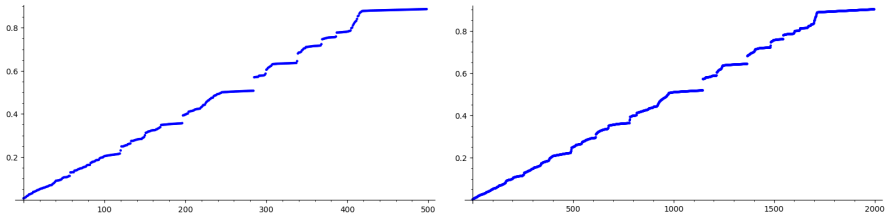
Looking at the right-most sliver, we get this wonderful swapping of colors, which is really a sequence of numbers arranged in order of increasing density of $U(n)$ (at least up to $x = 10000$ estimate).

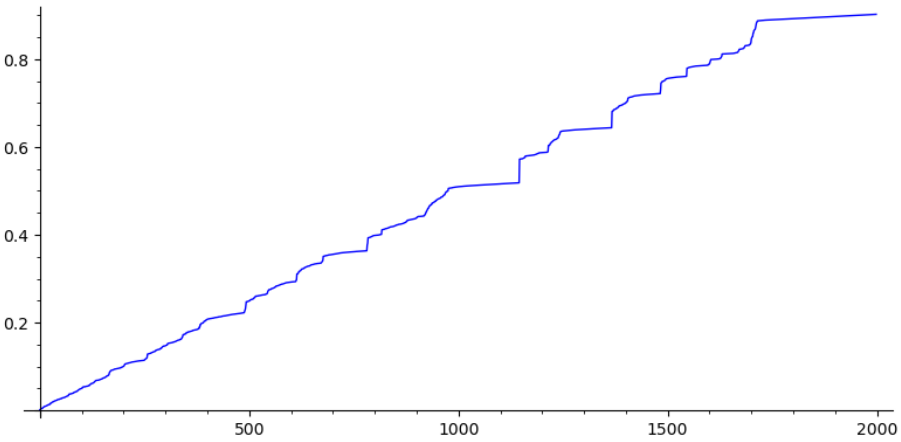
And with little gaps in between! But I'd guess that these densities would be dense in the interval $(0, 1)$ if we considered all positive integers.

And I'll include it because the code is cool (the *rainbow*(M) option is quite nice!):

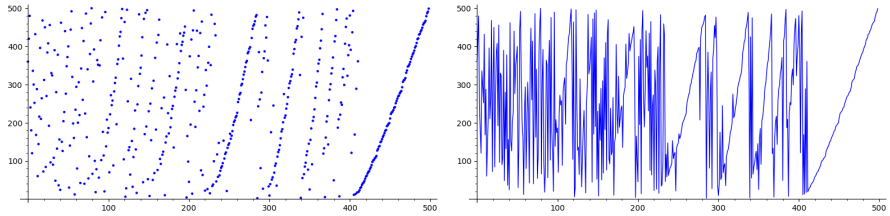
```
x=10000
M = 50
P = list_plot(U(2,x),color=rainbow(M)[0])
C = line([(0,5),(x/(M-1),5)],color=rainbow(M)[0],thickness=4)
for n in range(3,M+1):
    P += list_plot(U(n,x),color=rainbow(M)[n-2])
    C += line([((x/(M-1))*(n-2),5),((x/(M-1))*(n-1),5)],color=rainbow(M)[n-2],thickness=4)
plot(P+C)
```

Here are the plots of these densities in increasing order for the first 500 and 2000 integers, with $x = 10000$. And because I accidentally ran the second one with the points connected (which took 37m29s), I'll include that third.





And here are plots of the corresponding integers, one with points not joined and one with them joined:



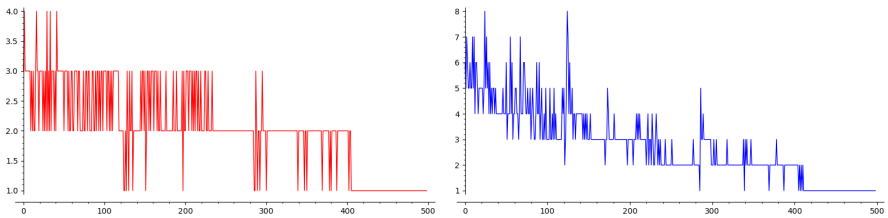
and the full list:

```
[360, 420, 480, 240, 180, 120, 336, 300, 252, 432, 168, 288, 60,
144, 216, 396, 210, 264, 468, 72, 312, 450, 84, 270, 384, 408, 192,
456, 96, 330, 324, 90, 108, 390, 48, 280, 132, 378, 36, 156, 24,
462, 150, 126, 204, 228, 440, 276, 348, 372, 400, 30, 140, 444, 492,
320, 198, 160, 12, 234, 294, 80, 200, 306, 220, 42, 342, 448, 260,
414, 40, 224, 486, 162, 340, 54, 112, 380, 460, 500, 66, 308, 392,
100, 18, 78, 364, 352, 56, 350, 416, 102, 476, 176, 114, 20, 490,
138, 208, 174, 186, 70, 222, 272, 246, 258, 88, 282, 304, 318, 196,
354, 366, 402, 426, 438, 474, 498, 368, 104, 464, 6, 28, 496, 256,
128, 136, 64, 315, 152, 32, 110, 184, 232, 130, 16, 248, 296, 484,
328, 344, 376, 424, 44, 472, 170, 488, 190, 495, 52, 230, 8, 250,
154, 290, 50, 310, 68, 370, 182, 410, 76, 430, 470, 105, 92, 238,
116, 124, 266, 10, 148, 164, 405, 225, 172, 322, 188, 212, 236, 244,
135, 268, 284, 292, 406, 316, 332, 356, 434, 388, 404, 412, 428,
436, 452, 286, 4, 165, 98, 45, 374, 195, 418, 14, 442, 494, 255, 189,
285, 441, 345, 375, 231, 435, 75, 465, 63, 242, 273, 22, 338, 297,
26, 357, 399, 15, 351, 483, 34, 38, 99, 459, 429, 46, 117, 58, 147,
62, 74, 82, 86, 94, 153, 106, 118, 122, 21, 134, 142, 146, 171, 158,
166, 178, 194, 202, 206, 214, 218, 226, 254, 262, 274, 278, 298, 302,
```

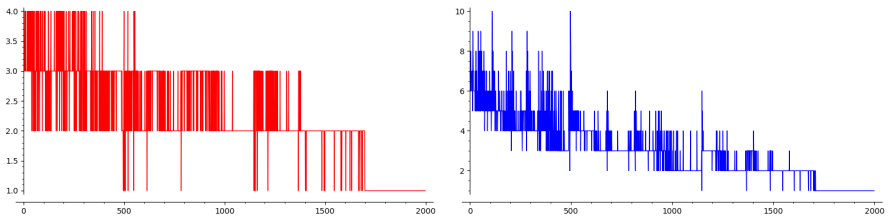
314, 326, 334, 346, 358, 362, 382, 386, 394, 398, 207, 422, 446, 454,
458, 466, 478, 482, 2, 243, 385, 261, 81, 279, 333, 27, 369, 387,
455, 423, 477, 363, 33, 9, 39, 175, 51, 57, 245, 69, 87, 93, 35, 111,
123, 129, 141, 159, 177, 183, 201, 275, 213, 219, 237, 249, 267, 291,
303, 309, 321, 327, 339, 381, 393, 411, 417, 447, 453, 471, 489, 325,
3, 425, 55, 475, 65, 85, 95, 115, 125, 77, 145, 25, 155, 185, 91,
205, 215, 235, 265, 295, 305, 335, 355, 365, 395, 415, 445, 485, 119,
133, 5, 161, 203, 217, 143, 259, 287, 301, 329, 343, 371, 49, 413, 427,
469, 497, 187, 209, 7, 221, 253, 247, 319, 341, 299, 407, 451, 473,
323, 377, 403, 481, 391, 121, 437, 493, 11, 169, 13, 289, 17, 361, 19,
23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101,
103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173,
179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251,
257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337,
347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421,
431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499]

And I realized my code for $U(n,x)$ has the condition "$if \mathcal{A}(m) > \mathcal{A}(n)$", so I was computing the abundancy (i.e. factorizing/sum of divisors/division) of n for each value of m. Storing "$ab = \mathcal{A}(n)$" at the beginning and writing "$if \mathcal{A}(m) > ab$" literally reduced the run-time down to 10m5s. Wild! Maybe we go ahead and try for 10000 integers! We'll also jump x to 100000. And after an hour and a half, I ran out of memory!

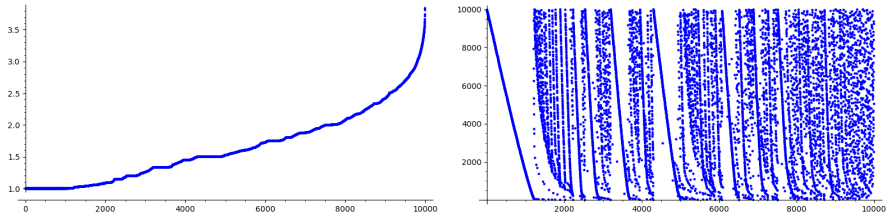
I really wonder how this looks not just as as plot more integers but as our estimate goes to the real value as $x \to \infty$. For example, does that gap around $0.5, 0.6$ persist? Well, how can we even describe this? Primes should be at the bottom of the list, which means maybe the order of this list is correlated to either $\omega(n)$ (red) or $\Omega(n)$ (blue).



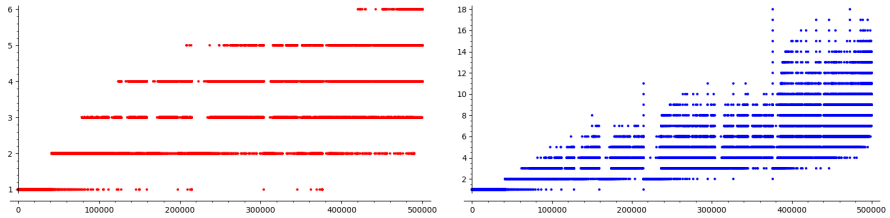
Ok, we have to try to push this computer! We'll plot the first 2000 integers with $x = 20000$. Took about 30 minutes for each graph!



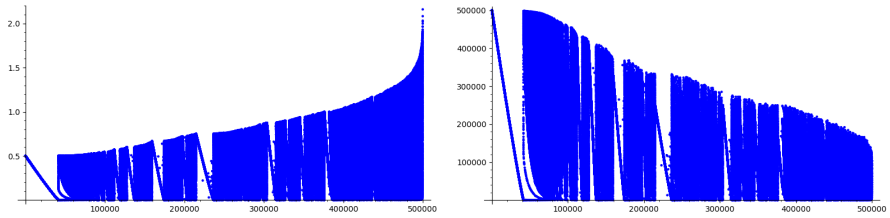
This makes me realize I've never done the same for the abundancy index itself. So here are two plots; the first is $\{\mathcal{A}(n) \mid n \leq 10000\}$ in increasing order and the second is the corresponding plot of integers n.



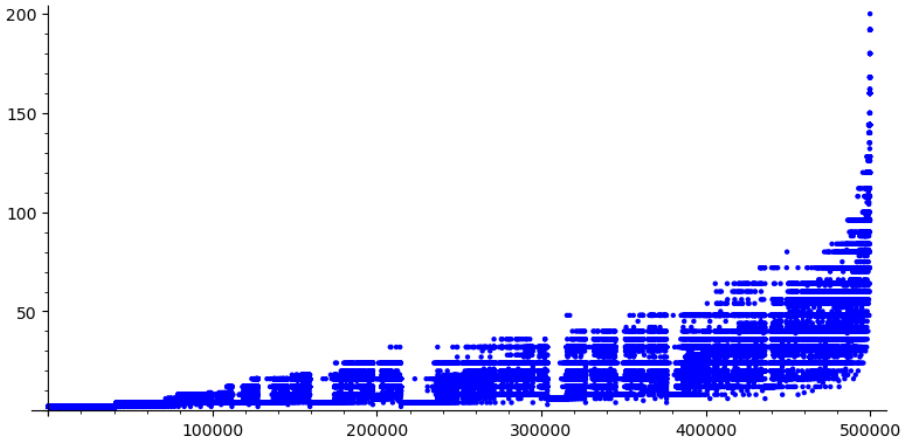
Notice, for example, the first bar representing the prime numbers below 10000. There seems to be other spots where we get these lines, but with more randomness, like between $(2800, 3200)$ and $(4300, 5000)$. Taking this list of integers ≤ 300000 with ordered by abundancy index and calculating $\omega(n)$ (red) and $\Omega(n)$ (blue) gives



And just for fun, let's also plot $\sigma(n)$ and $\phi(n)$ for this list.



And here are plots of the number of divisors function.



Ok, so let's try to summarize some trends.

- It seems that $\mathcal{A}(n)$ may be correlated to $\omega(n)$ vaguely, meaning that if you fix $\omega(n)$, there is some *minimum* index that n must achieve.
- A similar thing seems to hold for $\Omega(n)$, perhaps slightly stronger. We see that it may be true as well that if you fix a value of $\Omega(n)$ or $\omega(n)$, there may be some *maximum* index n can achieve in this list.
- While the plots for $\sigma(n)$ and $\phi(n)$ bounce all around, we see that general $\mathcal{A}(n)$ is positively correlated with $\sigma(n)$, which makes sense, and negatively correlated with $\phi(n)$, which also makes sense, considering our previous work showing that $\mathcal{A}(n) < n/\phi(n)$. So the larger $\phi(n)$ is, the smaller $\mathcal{A}(n)$ must be.
- The number of divisors seems to be positively correlated to $\mathcal{A}(n)$, though moreso on the minimum index side. It seems like maybe if you're far enough along in the list, you have at least a certain amount of divisors, which would seem to make sense. But even with a small number of divisors, it seems you can have very large abundancy.

13 Return from Hiatus

So I ended up taking a bit of a break! It's November 12, 2022. To start, let's recall the goal of studying conditions to ensure a number is solitary. The most basic condition is Greening's Criterion, which says that

$$gcd(n, \sigma(n)) = 1 \implies n \ solitary.$$

A result from Loomis (2015) says that

$$n \ odd \ and \ gcd(n^2, \sigma(n^2)) \ squarefree \implies n \ solitary.$$

I can't access the paper without paying, so I'm just going to try to dedicate this section to proving this result.

One fact that we can recognize is that n^2 being an odd square implies that $\sigma(n^2)$ is odd. If n^2 has a friend m, then $\mathcal{A}(m) = \mathcal{A}(n^2)$, which means

$$\frac{n^2}{g(n^2)} = \frac{m}{g(m)} \quad and \quad \frac{\sigma(n^2)}{g(n^2)} = \frac{\sigma(m)}{g(m)}$$

Since $g(n^2) = gcd(n^2, \sigma(n^2))$ is square-free, we have that $g(n^2) = p_1 \dots p_t$. As $p_i^2 | n^2$ for each i, the only way for $g(n^2)$ to be square-free is if each prime p_i exactly divides $\sigma(n^2)$. This means $\sigma(m)/g(m)$ is relatively prime to $g(n^2)$. It also means that n^2 almost divides m, but could fail by at most $rad(n)$. Specifically,

$$m = m' \prod_{i=1}^{t} p_i^{\nu_{p_i}(n^2)+a_{p_i}} \prod_{\substack{p|n \\ p \neq p_i}} p^{\nu_p(n^2)+a_p}$$

where $a_{p_i} \geq -1$ for $i = 1, \dots, t$, $a_p \geq 0$ for $p \neq p_i$ and $gcd(m', n) = 1$.

If $a_{p_i} \geq 0$ for all i, then $n^2 | m$, which contradicts friendship. So for at least one i, we have $a_{p_i} = -1$. Let I be a non-empty subset of $\{1, \dots, t\}$ corresponding to the indices for which $a_{p_i} = -1$. Then

$$m = m' \prod_{i \in I} p_i^{\nu_{p_i}(n^2)-1} \prod_{i \notin I} p_i^{\nu_{p_i}(n^2)+a_{p_i}} \prod_{\substack{p|n \\ p \neq p_i}} p^{\nu_p(n^2)+a_p}$$

Writing n^2 in the same decomposition and taking $\mathcal{A}$ on both sides gives the following:

$$\prod_{i \in I} \mathcal{A}(p_i^{\nu_{p_i}(n^2)}) \prod_{i \notin I} \mathcal{A}(p_i^{\nu_{p_i}(n^2)}) \prod_{\substack{p|n \\ p \neq p_i}} \mathcal{A}(p^{\nu_p(n^2)}) =$$

$$= \mathcal{A}(m') \prod_{i \in I} \mathcal{A}(p_i^{\nu_{p_i}(n^2)-1}) \prod_{i \notin I} \mathcal{A}(p_i^{\nu_{p_i}(n^2)+a_{p_i}}) \prod_{\substack{p|n \\ p \neq p_i}} \mathcal{A}(p^{\nu_p(n^2)+a_p})$$

Isolating $\mathcal{A}(m')$ gives

$$\mathcal{A}(m') = \prod_{i \in I} \frac{\mathcal{A}(p_i^{\nu_{p_i}(n^2)})}{\mathcal{A}(p_i^{\nu_{p_i}(n^2)-1})} \prod_{i \notin I} \frac{\mathcal{A}(p_i^{\nu_{p_i}(n^2)})}{\mathcal{A}(p_i^{\nu_{p_i}(n^2)+a_{p_i}})} \prod_{\substack{p|n \\ p \neq p_i}} \frac{\mathcal{A}(p^{\nu_p(n^2)})}{\mathcal{A}(p^{\nu_p(n^2)+a_p})}$$

In general,

$$\frac{\mathcal{A}(p^a)}{\mathcal{A}(p^b)} = \frac{p^{a+1}-1}{p^{b+1}-1} p^{b-a} = \frac{p^{b+1}-p^{b-a}}{p^{b+1}-1} \approx 1 - \frac{1}{p^{a+1}} + \frac{1}{p^{b+1}}$$

When $a > b$, this is an under-estimate, and when $a < b$, it is an over-estimate.

I can never decide whether I want to dig into the notation-heavy stuff somehow or try to look at more data to look for patterns. Let's do the second for a second. If m is a potential friend of n, then $n/g(n)$ divides m,

so $\mathcal{A}(n/g(n)) < \mathcal{A}(m)$. But this doesn't immediately help. The question of whether n has a friend is a question of whether there exists some positive integer k so that $\mathcal{A}(k(n/g(n))) = \mathcal{A}(g(n)(n/g(n)))$.

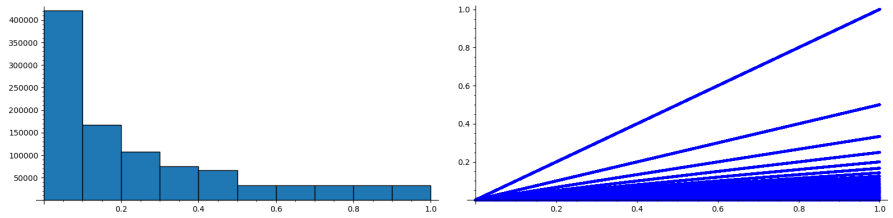
Let's define the pair (a, b) to be *n-friendly* if $\mathcal{A}(a(n/g(n))) = \mathcal{A}(b(n/g(n)))$ and let $F(n) \subset \mathbb{Z}^+ \times \mathbb{Z}^+$ be the set of n-friendly pairs. Looking at some basic properties, $F(n)$ is an equivalence relation, inherited from equality, and we have the diagonal embedding $\mathbb{Z}^+ \to F(n)$.

Let's do an example: $(3, 14) \in F(2)$ since $\mathcal{A}(6) = \mathcal{A}(28)$. More generally, if a and b are friends, then any divisor d of $gcd(a, b)$ gives rise to a point $(a/d, b/d) \in F(n)$ for any n with $n/g(n) = d$. Take $a = 80$ and $b = 200$, and let $d = 10$. We could choose $n = 20$, so $(8, 20) \in F(20)$.

How many $n \leq x$ have $n/g(n)$ for some fixed d? Looking at the distribution for $x = 10^6$, we have

$$mean = 243801 \quad median = 140717 \quad mode = [419, 659] \quad stdv = 263172$$

And we can see this major right-skew in the histogram and plot:



And we'd expect this because the points in the plot of $n/g(n)$ group into lines $y = X/m$ for $m = 1, 2, \ldots$, with $X = n$ lying on this line if $g(n) = m$. Then fixing $n/g(n) = d$ is like drawing a horizontal line and picking up a point from each line we cross. We'd cross X/m at $X = md$, so we'd cross x/d lines if we're looking at $n \leq x$.

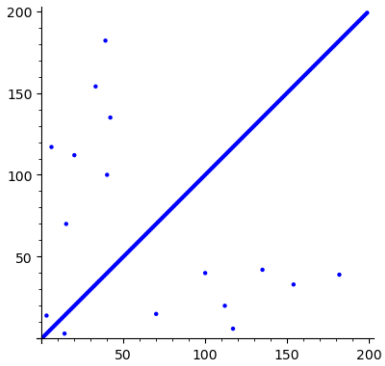
But we only *actually* pick up a point if $g(md) = d$. Counting the set of m that satisfy is exactly what Hall did in the paper we looked at in the very beginning, ***On the probability that*** n ***and*** $f(n)$ ***are relatively prime III***. So we've essentially gotten back to there.

Going back to the sets $F(n)$, notice that fixing the line $a = n/g(n)$ means $(a, b) \in F(n)$ if and only if b is a friend of n. So if n is solitary, this line will return a single point $(a, g(n))$. Are there other lines that we can say have few points?

Let's do a few plots! For $n = 2$ and $x = 200$, we get 7 distinct points

$$[(3, 14), (6, 117), (15, 70), (20, 112), (33, 154), (39, 182), (40, 100), (42, 135)]$$

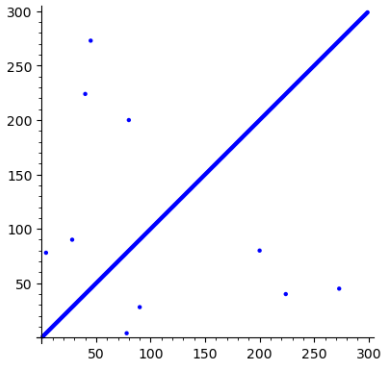
with plot



For $n = 3$ and $x = 300$, we get 5 distinct points

$$[(4, 78), (28, 90), (40, 224), (45, 273), (80, 200)]$$

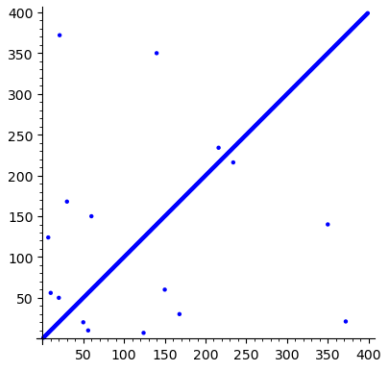
with plot



For $n = 4$ and $x = 400$, we get 8 distinct points

$$[(7, 124), (10, 56), (20, 50), (21, 372), (30, 168), (60, 150), (140, 350), (216, 234)]$$

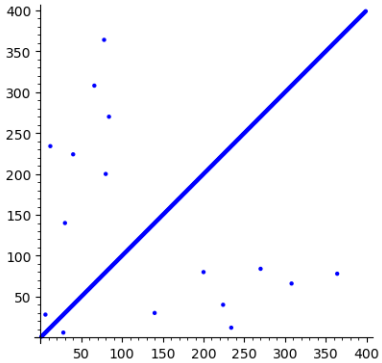
with plot



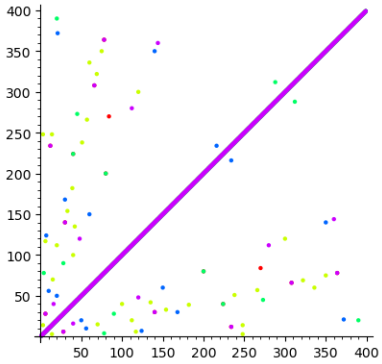
Another thing to notice is that while $a = g(n)$ in $F(n)$ gives a line of friends for n, we can also encompass all friendly numbers by looking at $F(1)$, since (a, b) is 1-friendly if and only if a and b are a friendly pair. Plotting this for $x = 400$ gives 8 distinct points

$$[(6, 28), (12, 234), (30, 140), (40, 224), (66, 308), (78, 364), (80, 200), (84, 270)]$$

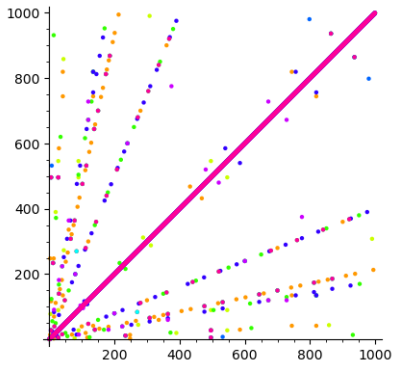
with plot



Let's do something fun and plot these on top of each other for $n = 1, 2, 3, 4, 5$ with $x = 400$, with colors (from red to purple) indicating the value of n.



And for n up to 10 and $x = 1000$, we get 138 total distinct pairs, with plot



Adding a third coordinate to indicate the value of n that they came from, we get a total of 214, meaning we have a decent amount of repeats in pairs. This list is

```
{(138, 644, 5), (15, 70, 2), (112, 280, 10), (28, 496, 3),
(165, 924, 8), (6, 28, 1), (114, 532, 5), (6, 28, 10), (272, 680, 10),
(20, 112, 2), (360, 900, 2), (864, 936, 1), (135, 744, 2), (10, 56, 4),
(141, 658, 2), (260, 650, 4), (6, 496, 5), (115, 644, 8), (864, 936, 10),
(80, 200, 1), (30, 140, 5), (170, 425, 8), (496, 546, 3), (78, 364, 5),
(432, 468, 2), (798, 980, 7), (96, 104, 9), (84, 270, 1), (28, 496, 5),
(93, 434, 2), (21, 372, 4), (42, 744, 2), (123, 574, 2), (288, 312, 3),
(20, 390, 3), (80, 200, 3), (112, 280, 5), (480, 520, 9), (240, 600, 3),
(210, 525, 8), (40, 224, 3), (20, 50, 4), (102, 476, 1), (6, 28, 5),
(272, 680, 5), (102, 476, 10), (75, 350, 2), (864, 936, 5), (213, 994, 2),
(375, 775, 9), (12, 234, 7), (340, 850, 4), (66, 308, 1), (280, 700, 2),
(180, 450, 4), (30, 585, 2), (135, 819, 2), (30, 75, 8), (16, 40, 10),
(3, 248, 2), (48, 120, 10), (310, 775, 8), (66, 308, 10), (165, 770, 2),
(28, 496, 9), (90, 496, 3), (39, 182, 2), (108, 117, 8), (6, 117, 2),
(186, 868, 6), (864, 936, 7), (28, 546, 3), (80, 200, 7), (40, 100, 2),
(3, 14, 2), (240, 600, 7), (7, 124, 4), (135, 819, 4), (150, 700, 6),
(368, 920, 10), (14, 248, 2), (60, 150, 4), (42, 819, 2), (57, 266, 2),
(102, 476, 5), (110, 616, 4), (6, 496, 7), (48, 120, 5), (80, 200, 9),
(380, 950, 4), (16, 40, 5), (66, 308, 5), (540, 585, 8), (195, 910, 2),
(240, 600, 9), (336, 840, 10), (55, 308, 8), (40, 224, 9), (129, 602, 2),
(120, 672, 9), (744, 819, 2), (114, 532, 6), (186, 868, 1), (390, 975, 8),
(111, 518, 2), (230, 575, 8), (186, 868, 10), (159, 742, 2), (4, 78, 3),
(30, 168, 4), (10, 25, 8), (30, 140, 6), (78, 364, 6), (150, 700, 1),
(140, 350, 4), (35, 620, 4), (290, 725, 8), (150, 700, 10), (368, 920, 5),
(28, 496, 6), (90, 504, 4), (5, 28, 8), (120, 300, 2), (170, 952, 4),
(85, 476, 8), (330, 825, 8), (208, 520, 10), (65, 364, 8), (110, 275, 8),
(12, 234, 6), (145, 812, 8), (216, 234, 4), (120, 728, 9), (14, 931, 4),
(336, 840, 5), (304, 760, 10), (114, 532, 1), (6, 28, 6), (756, 819, 8),
(186, 868, 5), (174, 812, 6), (864, 936, 6), (30, 140, 1), (78, 364, 1),
(80, 200, 6), (95, 532, 8), (240, 600, 6), (150, 700, 5), (28, 496, 1),
```

(138, 644, 6), (40, 224, 6), (220, 550, 4), (120, 672, 6), (135, 819, 6), (45, 252, 8), (370, 925, 8), (155, 868, 8), (208, 520, 5), (45, 273, 3), (176, 440, 10), (12, 234, 1), (6, 496, 6), (130, 728, 4), (12, 234, 10), (304, 760, 5), (15, 91, 9), (183, 854, 2), (69, 322, 2), (135, 819, 8), (102, 476, 6), (174, 812, 1), (144, 360, 10), (174, 812, 10), (42, 135, 2), (33, 154, 2), (240, 600, 1), (201, 938, 2), (66, 308, 6), (138, 644, 1), (87, 406, 2), (40, 224, 1), (138, 644, 10), (135, 819, 1), (120, 672, 1), (90, 546, 3), (15, 84, 8), (176, 440, 5), (44, 858, 3), (60, 364, 9), (28, 90, 3), (6, 496, 1), (90, 225, 8), (60, 336, 2), (177, 826, 2), (672, 728, 9), (12, 234, 5), (270, 675, 8), (6, 496, 10), (30, 140, 10), (130, 325, 8), (78, 364, 10), (120, 672, 3), (84, 270, 6), (135, 756, 8), (28, 496, 10), (114, 532, 10), (8, 532, 7), (144, 360, 5), (174, 812, 5), (51, 238, 2), (308, 990, 3), (190, 475, 8), (30, 182, 9), (70, 175, 8)}

Similar to the trick of showing that friendly numbers have a positive density, we can say that any friendly pair (a, b) will appear in $F(n)$ for all n with $gcd(n/g(n), lcm(a, b)) = 1$. But now with ordered pairs, this doesn't really give us anything except that the friendly pair (a, b) is contained in $\bigcup_n F(n)$, which we know since $(a, b) \in F(1)$.

The more interesting question is what the density of $\bigcup_n F(n) \subseteq \mathbb{Z}^+ \times \mathbb{Z}^+$ is. The points seem to almost form lines, with the colors swapping randomly, and some points scattered off any apparent line.

14 A return to Graph Theory

I've spent a few days trying to look through algebraic methods that might be helpful in encoding $\sigma(n)$ and as usual, my interests turned to Graph Theory. Two graphs we've already defined were

- The ***abundancy sieve graph*** $AS(n, T)$ whose vertices are abundancy indices that would guarantee n has a friend, colored based on whether a test in T determines that vertex to be an abundancy outlaw. We could consider it a doubly weighted graph by assigning the edge (u, v) the value $|u - v|$.
- The ***swapping graph*** $S(n)$, where we begin with a vertex n and iteratively add vertices for each swap $sw(v, i, j) = \frac{p_i}{p_j} n$ for a vertex v. This graph doesn't *really* depend on n, but the vector of exponents $(\nu_p(n))$ for each $p|n$. The goal was to look at the change in abundancy along an edge. Also, this should really be a directed graph.

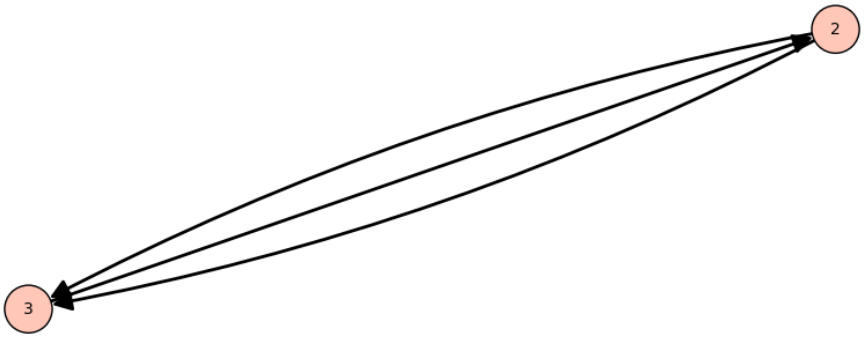
The following graph will try to isolate $gcd(n, \sigma(n))$. The graph $\mathcal{F}(n)$ will have $\omega(n)$ vertices corresponding to each $p|n$, with an edge from p to q if $p|\sigma(q^{\nu_q(n)})$, with a weight of k if $p^k||\sigma(q^{\nu_q(n)})$. So this is a directed edge-weighted graph. By ordering the primes dividing n as $p_1 < p_2 < \cdots < p_{\omega(n)}$, we could also describe this via its adjacency matrix $A(\mathcal{F}(n))$ whose $(i, j)^{th}$ entry is

$$\nu_{p_i}(\sigma(p_j^{\nu_{p_j}(n)}))$$

Since $\sigma(p) \equiv 1 \ mod \ p$, this graph will be simple (have no loops). It will often not be symmetric. Let's see an example.

Let $n = 6$. Then $2^2|\sigma(3)$ and $3|\sigma(2)$, so

$$A(\mathcal{F}(n)) = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}$$



The sum of a row i is the exponent of p_i in $\sigma(n)$, so writing $\sigma(n) = \overline{\sigma}(n)s(n)$ where $rad(\overline{\sigma}(n))|rad(n)$ and $gcd(s(n), n) = 1$, we can recover $\overline{\sigma}(n)$ by matrix multiplication:

$$\begin{bmatrix} log(p_1) & log(p_2) & \dots & log(p_{\omega(n)}) \end{bmatrix} A(\mathcal{F}(n)) \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} = log(\overline{\sigma}(n))$$

In 2000, David Wagner wrote a paper ***The critical group of a directed graph*** extending the work by Biggs in 1995 on the critical group/graph laplacian/chip firing game of undirected graphs. The Laplacian of an undirected graph is the difference between its degree matrix and its adjacency matrix, $L = D - A$. The only difference we really need to make for a directed graph is that we use the out-degree matrix.

However, defining the critical group $\mathcal{K}(G)$ of an undirected graph comes from looking at the torsion part of the cokernel $\mathbb{Z}^{|V|}/L^t\mathbb{Z}^{|V|}$, where L^t is the transpose of L. The dual group $\mathcal{K}^*(G)$ is the cokernel of L itself. These are not just isomorphic but literally equal, since $L^t = L$ for an undirected graph. But in general, $\mathcal{K}^*(G)$ is non-canonically isomorphic to $\mathcal{K}(G)$, depending on a choice of transformation matrices to the smith normal form of L.

By the fundamental theorem of finitely generated abelian groups, the critical group can be written as a product of cyclic groups of order $g_1, g_2, \dots,$. We picked these factors up by looking at the smith normal form. This is why $\mathcal{K}^*(G) \cong \mathcal{K}(G)$, because L and L^t have the same smith normal form.

The values $g_1, g_2, \dots,$ satisfy $g_1|g_2|g_3| \dots$ with $\prod g_i$ equaling, for an undirected graph, the number of spanning trees. The number of $g_i = 1$ is the rank of

the cokernel of L, and is equal to the number of strongly connected components of G.

ASIDE: Earlier (page 17), when looking at $\ell(n) = \sum_{k=1}^{\alpha(n)} rad_k(n)$, we discussed how looking at how many n satisfy $\ell(n) = L$ for some fixed L corresponds to looking at *square-free, divisible partitions* of L. That is, the number of solutions is the number of ways to write $L = a_1 + \cdots + a_t$ with $a_i \neq 1$ square-free and $a_{i+1} | a_i$. Then $n = \prod a_i$. Seeing the condition above reminded me of this and maybe SNF could be helpful in counting or working with square-free, divisible partitions?

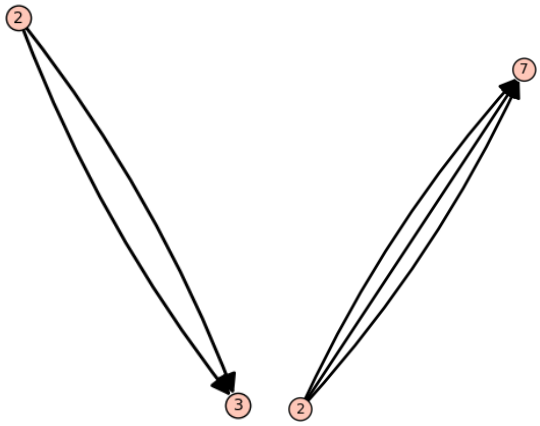
Let's go ahead and code up something to compute some of these critical groups. Note that in Sage, we use "elementary divisors" instead of "invariant factors", but they mean the same thing.

```
n = 2*3*5
P = [p[0] for p in list(factor(n))]
A = matrix.zero(om(n))
for i in range(om(n)):
    for j in range(om(n)):
        A[i,j] = (sigma(P[j]^(n.valuation(P[j])))).valuation(P[i])
D = matrix.zero(om(n))
for i in range(om(n)):
    D[i,i] = sum(A[i])
L = (D - A).transpose()
L.elementary_divisors()
```

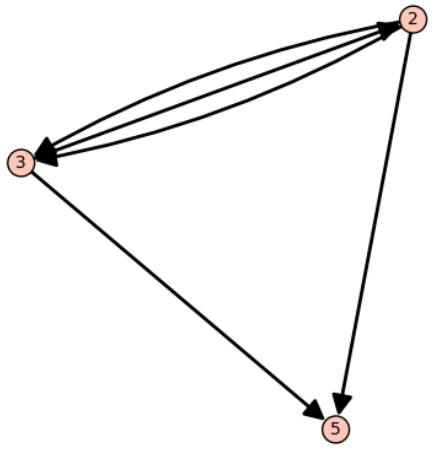
Clearly, if n is a prime power, then $\mathcal{F}(n)$ consists of a single vertex. The first two non-trivial graphs are $n = 6$ and $n = 10$, both of which have trivial critical groups. The following two, $n = 12$ and $n = 14$ have non-trivial critical groups, with

$$\mathcal{K}(\mathcal{F}(12)) = \mathbb{Z}/2\mathbb{Z}$$
$$\mathcal{K}(\mathcal{F}(14)) = \mathbb{Z}/3\mathbb{Z}$$

There matrices are $\begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}$. Here are the graphs for $n = 12, 14$.



For $n = 30$, we get matrix $\begin{bmatrix} 0 & 2 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$ and graph



15 A Unitary Twist

So I came across an interesting variation on the sigma function, which is the sum of *unitary divisors* $\sigma^*(n)$. A divisor is called unitary if $gcd(d, n/d) = 1$, and therefore

$$\sigma^*(n) = \sum_{\substack{d|n \\ gcd(d,n/d)=1}} d$$

So we could define an analogue to the abundancy index and see what happens! We'll define the *unitary abundancy index* to be

$$\mathcal{A}^*(n) = \frac{\sigma^*(n)}{n}$$

Naturally, we call n and m *unitary-friends* if their unitary abundancy indices are equal. The property "$n|m \Rightarrow \mathcal{A}(n) < \mathcal{A}(m)$" does not hold for the unitary index! For example

$$\mathcal{A}(6) = \frac{1+2+3+6}{6} = 2 \qquad \mathcal{A}(12) = \frac{1+3+4+12}{12} = \frac{5}{3}$$

However, if d is a unitary divisor of n, then any unitary divisor $e|d$ is a unitary divisor of n as well, so we do get the following fact that ***If*** d ***is a unitary divisor of*** n***, then***

$$\mathcal{A}^*(d) < \mathcal{A}^*(n)$$

This means the unitary abundancy index is multiplicative just like the usual one, since $p^{\nu_p(n)}$ is always a unitary divisor of n for all $p|n$. For $n = p^a$, we have

$$\mathcal{A}^*(p^a) = \frac{1+p^a}{p^a} = 1 + \frac{1}{p^a}$$

A really cool thing that this means is that for fixed a,

$$\prod_p \mathcal{A}^*(p^a) = \prod_p \left(1 + \frac{1}{p^a}\right) = \prod_p \frac{\left(1 - \frac{1}{p^{2a}}\right)}{\left(1 - \frac{1}{p^a}\right)} = \prod_p \frac{\left(1 - \frac{1}{p^a}\right)^{-1}}{\left(1 - \frac{1}{p^{2a}}\right)^{-1}} = \frac{\zeta(a)}{\zeta(2a)}$$

So this converges for $a > 1$. While the equivalent product for $\mathcal{A}(p^a)$ diverges for all a:

$$\prod_p \mathcal{A}(p^a) = \prod_p \left(1 + \frac{1}{p} + \cdots + \frac{1}{p^a}\right) > \prod_p \left(1 + \frac{1}{p}\right)$$

And we can see that the final product diverges by using Merten's estimate.

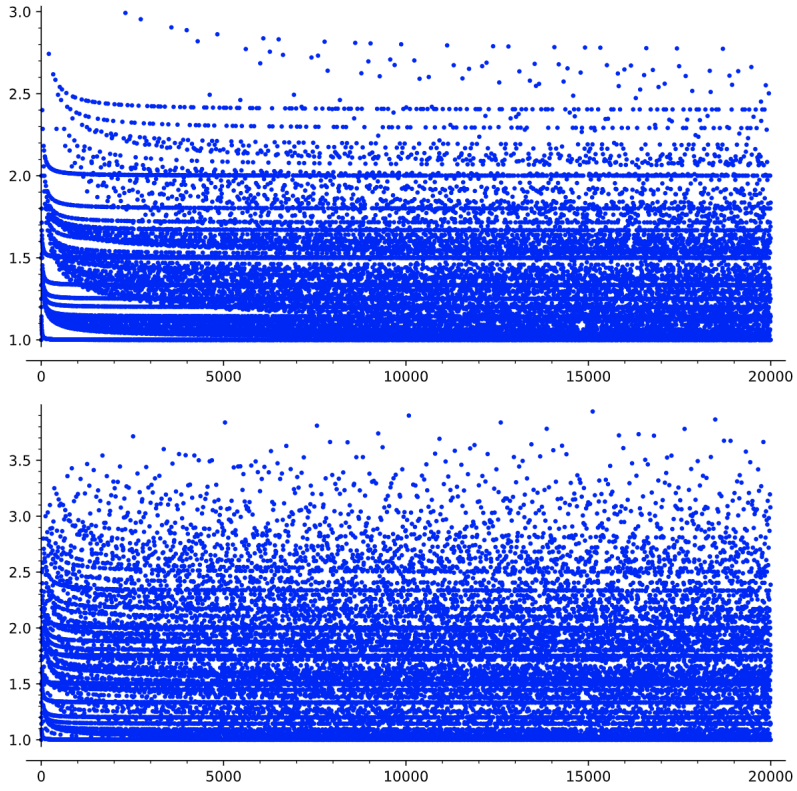
$$\prod_p \left(1 + \frac{1}{p}\right) = \prod_p \frac{\left(1 - \frac{1}{p^2}\right)}{\left(1 - \frac{1}{p}\right)} = \prod_p \frac{\left(1 - \frac{1}{p}\right)^{-1}}{\left(1 - \frac{1}{p^2}\right)^{-1}} = \frac{1}{\zeta(2)} \prod_p \left(1 - \frac{1}{p}\right)^{-1} \sim \frac{e^{\gamma_0}}{\zeta(2)} log x$$

where Merten's product formula gives the last asympototic.

So with even the basic test for solitary numbers gone, I wonder how hard it is to find unitary-friendly numbers? We can code this up as follows:

```
def Astar(n):
    D = divisors(n)
    Dstar = []
    for d in D:
        if gcd(d,n/d) == 1:
            Dstar.append(d)
    return sum(Dstar)/n
```

and plot it on top, with the plot of the regular abundancy index on the bottom. We can see that it pretty much looks the same, but the unitary plot might have a bit more white space in certain areas.



The list of the first few unitary-friendly pairs is

```
[(12, 18), (2, 20), (2, 24), (3, 45), (6, 60), (4, 72), (6, 90),
(10, 120), (84, 126), (14, 140), (14, 168), (12, 180), (132, 198)]
```

with a few indices worked out:

$$\mathcal{A}^*(2) = \frac{1+2}{2} = \frac{3}{2} \qquad A^*(6) = \frac{1+2+3+6}{6} = 2$$

$$\mathcal{A}^*(12) = \frac{1+3+4+12}{12} = \frac{5}{3} \qquad A^*(20) = \frac{1+4+5+20}{20} = \frac{3}{2}$$

In general, using multiplicativity,

$$\mathcal{A}^*(n) = \prod_p \frac{p^{\nu_p(n)}+1}{p^{\nu_p(n)}}$$

So any reduction of the fractions comes from a pair of primes $p \neq q$ both dividing n so that $p|(q^{\nu_q(n)}+1)$. This is exactly why I believe the graph we defined above

is better suited to the unitary abundancy index! It naturally only includes the primes dividing n, while $\sigma(n)$ could be divisible by other prime, and that isn't accounted for in $\mathcal{F}(n)$. But let's continue with the unitary stuff for now.

Now we know that sometimes you have to search very hard to find friendly numbers. But in a search up to 20000, here are the first 200 unitary-friendly numbers. They have a density of 0.565.

```
[2, 3, 4, 6, 7, 8, 10, 12, 14, 15, 18, 20, 21, 22, 24, 26, 27, 28,
32, 33, 34, 35, 38, 39, 40, 42, 44, 45, 46, 48, 50, 51, 52, 54, 56,
57, 58, 60, 62, 63, 66, 68, 69, 70, 72, 74, 76, 78, 82, 84, 86, 87,
88, 90, 92, 93, 94, 96, 98, 100, 102, 104, 106, 108, 110, 111, 114,
116, 118, 120, 122, 123, 124, 126, 129, 130, 132, 134, 135, 136,
138, 140, 141, 142, 146, 147, 148, 152, 154, 156, 158, 159, 162, 164,
166, 168, 170, 172, 174, 177, 178, 180, 182, 183, 184, 186, 188, 190,
192, 194, 196, 198, 200]
```

In contrast, the first 200 friendly numbers up to the same bound are

```
[6, 12, 28, 30, 40, 42, 56, 60, 66, 78, 80, 84, 102,
114,120, 132, 135, 138, 140, 150, 168, 174, 186, 200]
```

and have density 0.12. I wonder how good a lower bound on the density of unitary-friendly numbers we can get? We can pull the same trick Greening and others did in the original 6020 article.

If $gcd(k, 10) = 1$, then

$$\frac{3}{2}\mathcal{A}^*(k) = \mathcal{A}^*(20)\mathcal{A}^*(k) = \mathcal{A}^*(20k) = \mathcal{A}^*(2k) = \mathcal{A}^*(2)\mathcal{A}^*(k) = \frac{3}{2}\mathcal{A}^*(k)$$

Then the density of the set of unitary-friendly numbers is at least

$$\frac{\phi(10)}{10}\left(\frac{1}{2}\right) = \frac{1}{5} = 0.20$$

If we use a different pair, say $(12, 18)$, we need $gcd(k, 6) = 1$, then $\mathcal{A}^*(12k) = \mathcal{A}^*(18k)$, which gives a density bound of

$$\frac{2}{6}\left(\frac{1}{12} + \frac{1}{18} - \frac{1}{36}\right) = \frac{1}{27}$$

Characterizing which primes divide $\sigma^*(n)$ goes in a very similar way. For example,

Proposition 2 *$\sigma^*(n)$ is odd if and only if n is a power of two.*

Proof 3 *For a general n, we have*

$$\sigma^*(n) = \prod_{p|n}(1 + p^{\nu_p(n)}),$$

so $\sigma^*(n)$ is even if any odd prime divides n. Therefore, n must be a power of 2.

So can we prove that any number is unitary-solitary? $n = 5$ is the first number to not appear in the list. I ran it again searching up to 100000, which made the density of the first 200 unitary-friendly numbers equal to 0.60. The number 5 still doesn't appear, and neither do

$$9, 11, 13, 16, 17, 19, 23, 25, 29, 30, 31, 37, 41, 43, 47, 49$$

So perhaps prime powers are unitary-solitary except for the first few. Let's see.

$$\mathcal{A}^*(p^a) = \frac{p^a + 1}{p^a}$$

which means any friend m of p^a must be divisible by p^a. Write $m = p^b m'$ with $b \geq a$ and $gcd(p, m') = 1$, so

$$\mathcal{A}^*(m') = \frac{(p^a + 1)p^b}{p^a(p^b + 1)} = \frac{p^{b-a}(p^a + 1)}{p^b + 1}$$

Within the first 5000 integers, the prime powers we have found to be unitary-friendly are

$$[2, 3, 2^2, 7, 2^3, 3^3, 2^5, 2^7]$$

which means that if any other prime powers have friends, they are larger than 100000. Which again isn't unreasonable, given the classic example of 24's smallest friend being $91,963,648$. Let's look at $16 = 2^4$. Then we need some odd m' with

$$\mathcal{A}^*(m') = \frac{2^{b-4}(2^4 + 1)}{2^b + 1} = \frac{2^{b-4}17}{2^b + 1}$$

If $b = 5$, this becomes

$$\mathcal{A}^*(m') = \frac{34}{33}$$

Now $\sigma^*(33) > 34$, so does the same kind of theorem work here?

Suppose a/b is in reduced form and $b < a < \sigma^*(b)$. Without the star, this is easily proved using the divisibility test for solitary numbers (for example, Lemma 2.2.5 in Dris' ***Solving the Odd Perfect Number Problem***).

But now the divisibility test only works for unitary divisors. Let's see how it goes. Assume a/b is in reduced form (meaning $gcd(a, b) = 1$) and $b < a < \sigma^*(b)$. If we suppose we have some n with $\mathcal{A}^*(k) = a/b$. Then

$$b\sigma^*(k) = ak,$$

so $b|k$ and $a|\sigma^*(k)$.

Actually, this just isn't true! For example, $\sigma^*(30) = 72$ yet $41/30$ is a unitary-abundancy index for 3240. Similarly, $\sigma^*(15) = 24$ but $\mathcal{A}^*(30240) = 22/15$. Another example is $\mathcal{A}^*(80) = 51/40$, despite $\sigma^*(40) = 54$. Let's go ahead and list out the abundancy indices we find by computation up to 500000, ordered by denominator.

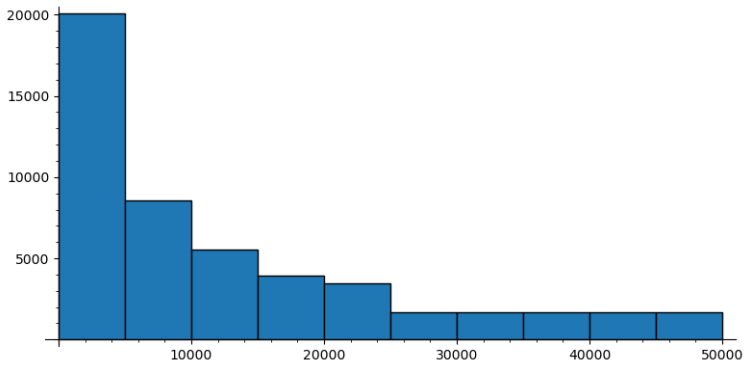
$$
\begin{array}{ccccccccccccc}
 & & & & & 1 & & & & & & & \\
 & & & & & \frac{3}{2} & & & & & & & \\
 & & & & \frac{4}{3} & , & \frac{5}{3} & & & & & & \\
 & & & & \frac{5}{4} & , & \frac{7}{4} & & & & & & \\
 & & \frac{6}{5} & , & \frac{7}{5} & , & \frac{8}{5} & , & \frac{9}{5} & , & \frac{12}{5} & & \\
 & & & & & \frac{7}{6} & & & & & & & \\
\frac{8}{7} & , & \frac{9}{7} & , & \frac{10}{7} & , & \frac{11}{7} & , & \frac{12}{7} & , & \frac{13}{7} & , & \frac{16}{7} \\
 & & & & \frac{9}{8} & , & \frac{11}{8} & , & \frac{13}{8} & & & & \\
 & & \frac{10}{9} & , & \frac{11}{9} & , & \frac{13}{9} & , & \frac{14}{9} & , & \frac{16}{9} & & \\
 & & & & & \frac{13}{10} & , & \frac{17}{10} & & & & &
\end{array}
$$

Looking at something like this would push us towards looking at Farey sequences, and perhaps that can help in figuring out how many indices should appear in each row. But just looking at some possible patterns, one interesting thing happens when you look for a denominator of 12. There are 48 and 720 with $\mathcal{A}^* = 17/12$, but nothing bigger. Most other numbers had a few larger ones as well.

We can look at the denominators of $\mathcal{A}^*(n)$ for $n \leq 50000$, and we get the following counts for $d = 1, 2, \ldots, 100$.

```
[4, 9, 7, 6, 16, 4, 23, 7, 10, 3, 21, 2, 26, 1, 10, 2, 22,
1, 27, 4, 10, 4, 27, 2, 22, 6, 10, 5, 29, 1, 23, 7, 8, 3,
19, 4, 23, 7, 14, 1, 33, 3, 28, 5, 9, 3, 28, 4, 20, 4, 7,
5, 26, 3, 20, 1, 13, 7, 31, 1, 17, 1, 8, 2, 20, 1, 22, 8,
9, 3, 28, 3, 12, 3, 7, 3, 22, 2, 26, 4, 5, 5, 33, 0, 18,
5,10, 3, 31, 2, 13, 4, 11, 4, 15, 0, 24, 5, 10, 6]
```

with histogram



Let's isolate those values that never appear as a denominator for the first 50000 integers. There seem to be quite a lot but we're also not looking very high.

$$[84, 96, 126, 132, 138, 156, 198, 204, 210, 245, 246, 258, 270, 300]$$

Fixing 84, we just needed to look a bit farther: $\mathcal{A}^*(122304) = \frac{125}{84}$.

15.1 Unitary divisors for other functions

Another direction we could go is to see how other arithmetic functions react when restricted to unitary divisors. First of all, here's a fun application of unitary divisors to group theory.

Theorem 25 *If G of order n has a normal subgroup H whose order is a unitary divisor d, then H is the unique such subgroup, and there exists a subgroup K of order n/d so that G is a direct product: $G = K \times H$.*

Proof 4 *Since H is normal, the quotient group G/H is well defined, and since d is a unitary divisor, the orders of H and G/H are relatively prime. If H' is any other subgroup of order d, the quotient map $\phi : G \to G/H$ will send H' to a subgroup of G/H, which means $|\phi(H')|$ divides $|G/H|$. But $|\phi(H')|$ also divides $|H'|$, which is relatively prime to $|G/H|$, so $|\phi(H')| = 1$. This means $H' \subseteq ker(\phi)$. But we know, since ϕ is the quotient map, that $ker(\phi) = H$, and since they are the same size, this shows $H' = H$, which shows uniqueness.*

Let $i : G/H \to G$ be the inclusion map. Then $K = Im(i)$ is a subgroup of G whose order is a unitary divisor, so it is unique, and therefore normal. Because their orders are relatively prime, $K \cap H = \{e\}$, so $|K \times H| = |K||H| = |G|$, with the obvious inclusion map being an isomorphism between G and $K \times H$.

The divisor sum for Euler's totient function

$$n = \sum_{d|n} \phi(d)$$

usually comes from looking at the cyclic group C_n of order n and noting that each element generates some subgroup. Conversely, for each divisor $d|n$, the

number of generators for the subgroup $C_d \subset C_n$ is $\phi(d)$. These two points of views give us the sum. Written out using sums:

$$n = \sum_{g \in C_n} 1 = \sum_{d|n} \sum_{<g>=C_d} 1 = \sum_{d|n} \phi(d)$$

What does restricting to unitary divisors do? Clearly counts the number of generators of cyclic subgroups of unitary divisor order. But any other way to look at it? Well the cyclic group C_n is abelian, so can be written as a direct product. But $C_a \times C_b = C_{ab}$ if and only if $gcd(a, b) = 1$, which means the only decompositions of C_n into the direct product of two groups are $C_d \times C_{n/d}$ for a unitary divisor d. So restricting to unitary divisors counts the generators of those subgroups that appear in direct product decompositions of length 2. Maybe it would be fun to generalize in that direction, by allowing longer length decompositions. Or we could extend to counting generators of subgroups that appear in a semi-direct product decomposition of G.

Another classic divisor sum is the mobius function, for which

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & else \end{cases}$$

Recall the function $\beta(n) = min_{p|n}\{\nu_p(n)\}$ that we looked at in the first section that returns the minimum exponent of n. Then we get a really cool theorem by restricting to unitary divisors!

Theorem 26

$$\sum_{\substack{d|n \\ unitary}} \mu(d) = \begin{cases} 1 & \beta(n) > 1 \\ 0 & else \end{cases}$$

So where the mobius divisor sum is often used to isolate when something (like a gcd)) is equal to 1, this unitary mobius sum could be used to isolate those n whose exponents are all at least 2. In other words, not only is n not square-free, but it has no square-free part at all. This is really interesting to me because restricting to unitary divisors usually makes that divisor not square-free, while $\mu(d)$ is zero if d is not square-free, so they seem at ends with eachother.

Proof 5 *Let*

$$U(n) = \sum_{\substack{d|n \\ unitary}} \mu(d)$$

Since $p^{\nu_p(n)}$ is a unitary divisor for n for all $p|n$, we can write

$$U(n) = \prod_{p|n} U(p^{\nu_p(n)})$$

because of the multiplicativity of $\mu(n)$. Then

$$U(p^a) = \sum_{\substack{d|p^a \\ unitary}} \mu(d) = \mu(1) + \mu(p^a)$$

and this is equal to 1 if $a > 1$ and 0 when $a = 1$. Therefore, $U(n)$ is 0 if any $\nu_p(n) = 1$, and the statement follows.

And we get something really cool when looking at the Dirichlet generating function for $U(n)$. Clearly for the original mobius divisor sum, the Dirichlet generating function is just $1/n$.

Theorem 27

$$\sum_{n=1}^{\infty} \frac{U(n)}{n^s} = \frac{\zeta(2s)\zeta(3s)}{\zeta(6s)}$$

For example, setting $s = 1$ gives Landau's totient constant, one we've seen a few times here:

$$\frac{\zeta(2)\zeta(3)}{\zeta(6)} \approx 1.943596$$

Using the notation defined in the first few sections,

$$rad_k(n) = \prod_{\substack{p|n \\ p^k|n}} p$$

we can say the sum of reciprocals of those n with $rad_1(n) = rad_2(n)$ converges to the above constant.

Proof 6 *We start by writing*

$$\sum_{n=1}^{\infty} \frac{U(n)}{n^s} = \sum_{\substack{n=1 \\ \beta(n)>1}}^{\infty} \frac{1}{n^s}$$

and then rewrite it as its Euler Product.

$$= \prod_{p|n} \left(1 + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \dots\right) = \prod_{p|n} \left(\left(1 - \frac{1}{p^s}\right)^{-1} - \frac{1}{p^s}\right)$$

$$= \prod_{p|n} \left(\frac{p^s}{p^s - 1} - \frac{1}{p^s}\right) = \prod_{p|n} \frac{p^{2s} - p^s + 1}{p^s(p^s - 1)}$$

We'll now arrive at the same product by starting with the zeta function quotient.

$$\frac{\zeta(2s)\zeta(3s)}{\zeta(6s)} = \prod_{p|n} \frac{\left(1 - \frac{1}{p^{2s}}\right)^{-1} \left(1 - \frac{1}{p^{3s}}\right)^{-1}}{\left(1 - \frac{1}{p^{6s}}\right)^{-1}} = \prod_{p|n} \frac{\left(1 - \frac{1}{p^{6s}}\right)}{\left(1 - \frac{1}{p^{2s}}\right)\left(1 - \frac{1}{p^{3s}}\right)}$$

$$= \prod_{p|n} \frac{\left(1-\frac{1}{p^{3s}}\right)\left(1+\frac{1}{p^{3s}}\right)}{\left(1-\frac{1}{p^{2s}}\right)\left(1-\frac{1}{p^{3s}}\right)} = \prod_{p|n} \frac{\left(1+\frac{1}{p^{3s}}\right)}{\left(1-\frac{1}{p^{2s}}\right)} = \prod_{p|n} \frac{\left(\frac{p^{3s}+1}{p^{3s}}\right)}{\left(\frac{p^{2s}-1}{p^{2s}}\right)}$$

$$= \prod_{p|n} \frac{p^{2s}(p^{3s}+1)}{p^{3s}(p^{2s}-1)} = \prod_{p|n} \frac{(p^s+1)(p^{2s}-p^s+1)}{p^s(p^s-1)(p^s+1)} = \prod_{p|n} \frac{p^{2s}-p^s+1}{p^s(p^s-1)}$$

and we're done!

And of course, we could really restrict to any subset of divisors and see how these go. For example, what if we looked at what we previously called *maximal divisors* of n? Those $d|n$ s.t. for at least one p, we have $\nu_p(d) = \nu_p(n)$. These sit between unitary divisors and all divisors:

$$\{d|n \ unitary\} \subseteq \{d|n \ maximal\} \subseteq \{d|n\}$$

with equality when n is square-free. We used this to decompose $n/\phi(n)$ into a sum of abundancy indices and phi ratios. For the mobius sum, any maximal divisor is of the form $d = p^{\nu_p(n)}d'$, so if $\nu_p(n) > 1$, then $\mu(d) = 0$.

Let $sf(n)$ be the square-free part of n (explicitly $sf(n) = rad(n)/rad_2(n)$). A divisor d will only contribute to the sum if $d|rad(n)$, so a maximal divisor must have $gcd(d, sf(n)) \neq 1$. So $d = gcd(d, sf(n))s'$ where $gcd(sf(n), s') = 1$ and $s'|rad(n)/sf(n)$. Then

$$\sum_{\substack{d|n \\ maximal}} \mu(d) = \sum_{\substack{s|sf(n) \\ s\neq 1}} \sum_{s'|rad(n)/sf(n)} \mu(ss') = \sum_{\substack{s|sf(n) \\ s\neq 1}} \sum_{s'|rad(n)/sf(n)} \mu(s)\mu(s')$$

$$= \left(\sum_{\substack{s|sf(n) \\ s\neq 1}} \mu(s)\right)\left(\sum_{s'|rad(n)/sf(n)} \mu(s')\right)$$

If $rad(n)/sf(n) \neq 1$, then the second sum will be 0. So our divisor sum is 0 if n is not square-free. When n is square-free, the first sum is just the usual sum of divisors of n, minus $\mu(1) = 1$. We can phrase this using $\alpha(n) = max_{p|n}\{\nu_p(n)\}$ to mirror the unitary divisor sum:

$$\sum_{\substack{d|n \\ maximal}} \mu(d) = \begin{cases} 1 & \alpha(n) = 0 \\ -1 & \alpha(n) = 1 \\ 0 & else \end{cases}$$

We could also define a *maximal abundancy index* and look at the same things we did before. We could also consider the subsets of divisors in a fixed residue class (e.g. $\{d|n \ : \ d \equiv 1 \ mod \ 5\}$), which I definitely want to get to!

But for now, I want to go back to the unitary divisors. I'd really like to understand which indices a/b are unitary-outlaws. A few indices that didn't

appear in our search are $11/5, 11/6, 15/7$, but our search wasn't terribly far, so this doesn't mean too much.

If $gcd(a,b) = 1$, then a/b being a unitary-abundancy index means there is some $n \in \mathbb{Z}^+$ so that

$$\frac{\sigma^*(n)}{n} = \frac{a}{b}.$$

Then $n = bk$ and $\sigma^*(n) = ak$ for some $k \in \mathbb{Z}^+$. Putting these together, we need some k so that $\sigma^*(bk) = ak$.

If $gcd(b,k) = 1$, then $\sigma^*(bk) = \sigma^*(b)\sigma^*(k)$, so

$$\frac{a}{b} = \frac{\sigma^*(n)}{n} = \frac{\sigma^*(b)\sigma^*(k)}{bk} = \mathcal{A}^*(b)\mathcal{A}^*(k)$$

which means we need a k with

$$\mathcal{A}^*(k) = \frac{a}{\sigma^*(b)}$$

So if $\sigma^*(b) > a$, this is impossible.

Note that is only if $gcd(b,k) = 1$. For example,

$$\mathcal{A}^*(100) = \frac{1+4+25+100}{100} = \frac{130}{100} = \frac{13}{10}$$

where $b = 10$ and $k = 10$, despite $\sigma^*(10) = 18$. Let's look at that specific case where n is square-free and we want to determine $\mathcal{A}^*(n^2)$. Any divisor of n, squared, will be a unitary divisor of n^2. And any unitary divisor of n^2 must equal the squares of some subset of primes diving n. So

$$\sigma^*(n^2) = \sum_{\substack{d|n^2 \\ unitary}} d = \sum_{d|n} d^2$$

Cool! Recall that $\sigma_k(n)$ is the sum of k^{th} powers of divisors of n. Then for square-free n, we have

$$\sigma^*(n^k) = \sigma_k(n)$$

and

$$\mathcal{A}^*(n^k) = \frac{\sigma_k(n)}{n^k}$$

Suppose we want to find a unitary-friend of 100. This friend must look like $m = 2^a 5^b m'$ where $gcd(10, m') = 1$ and $a, b \geq 1$. Then

$$\mathcal{A}^*(m') = \frac{13/10}{\mathcal{A}^*(2^a)\mathcal{A}^*(5^b)} = \frac{(13)(2^{a-1})(5^{b-1})}{(2^a+1)(5^b+1)}$$

Let's go through a few cases.

$$\underline{a = 1, b = 1} \qquad\qquad \underline{a = 1, b = 2}$$

$$\mathcal{A}^*(m') = \frac{13}{18} < 1 \qquad \mathcal{A}^*(m') = \frac{65}{78} < 1$$
$$\underline{a = 2, b = 1} \qquad \underline{a = 2, b = 2}$$
$$\mathcal{A}^*(m') = \frac{26}{30} < 1 \qquad \mathcal{A}^*(m') = \frac{130}{130} = 1$$
$$\underline{a = 1, b = 3} \qquad \underline{a = 3, b = 1}$$
$$\mathcal{A}^*(m') = \frac{26}{30} < 1 \qquad \mathcal{A}^*(m') = \frac{26}{27} < 1$$
$$\underline{a = 2, b = 3} \qquad \underline{a = 3, b = 2}$$
$$\mathcal{A}^*(m') = \frac{65}{63} < 1 \qquad \mathcal{A}^*(m') = \frac{10}{9}$$

These last two give plausible indices. Lets start with the right one. If $\mathcal{A}^*(m') = 10/9$, then $m' = 3^c m''$ for some m'' with $gcd(30, m'') = 1$. This gives us

$$\mathcal{A}^*(m'') = \frac{10/9}{\mathcal{A}^*(3^c)} = \frac{3^{c-2}10}{3^c + 1}$$

For $c = 1$, this is < 1, and for $c = 2$, we get that $\mathcal{A}^*(m'') = 1$, so we have a friend! With $(a, b, c) = (3, 2, 2)$, which gives $m = 2^3 3^2 5^2 = 1800$.

Just by computation, we have a few other friends: $100, 1800, 61200, 79200$. None of these match the left case $(a, b) = (2, 3)$. So let's explore that. $\mathcal{A}^*(m') = 65/63$ means $m' = 3^c 7^d m''$ for some $c \geq 2$ and $d \geq 1$ and $gcd(210, m'') = 1$. And this means

$$\mathcal{A}^*(m'') = \frac{65/63}{\mathcal{A}^*(3^c)\mathcal{A}^*(7^d)} = \frac{(65)(3^{c-2})(7^{d-1})}{(3^c + 1)(7^d + 1)}$$

I just realized something. This will never be < 1 since $\lim_{a\to\infty} \mathcal{A}^*(p^a) = \lim_{a\to\infty} \frac{1+p^a}{p^a}$ approaches 1 from above. So for the above example, when c and d are big enough (which $c \geq 2, d \geq 1$ is in this case), this index will always be bigger than 1. So if there is any disqualification, it must come from somewhere else.

Let's go to the next obvious option, divisibility. As we go along this process, we build up a number that must be relatively prime to a larger number, e.g. at first we needed $gcd(10, m') = 1$ and then the next step gave us $gcd(210, m'') = 1$, and this will continue. If we contradict this at any point, this would prove the non-existence of such a friend.

The denominator is $(3^c + 1)(7^d + 1)$, so let's see whether 2 or 5 divide these. If they do, but don't divide the top, then this will give us our contradiction! As both are odd, both are always divisible by 2, so the denominator is divisible by 4. But the numerator is odd! Therefore, this would force $4|m''$, a contradiction! So we can't have a friend with $(a, b) = (2, 3)$.

Going back to the $(3, 2)$ case, we'd need

$$gcd(30, m'') = 1 \;\; and \;\; \mathcal{A}^*(m'') = \frac{3^{c-2}10}{3^c + 1}$$

Since $3 \equiv -1 \ mod\ 4$, the denominator will be divisible by 4 whenever c is odd. Since the numerator is only divisible by 2, this contradicts $gcd(m'', 2) = 1$. So c must be even.

Let $c = 2c'$ with c' odd, then our equation becomes

$$\mathcal{A}^*(m'') = \frac{3^{2c'-2}10}{3^{2c'}+1} = \frac{9^{c'-1}10}{9^{c'}+1}.$$

Since $9^5 \equiv -1 \ mod\ 25$, we have a contradiction whenever c' is an odd multiple of 5, which means $gcd(c', 5) = 1$. So we can say that if $3|m$, then it's exponent must be even but not divisible by 5. So let's test $c = 4$. Then

$$\mathcal{A}^*(m'') = \frac{3^2 10}{3^4+1} = \frac{90}{82} = \frac{45}{41}$$

So $m'' = 41^d m'''$ where $gcd(2 * 3 * 5 * 41, m''') = 1$. Then

$$\mathcal{A}^*(m''') = \frac{45/41}{\mathcal{A}^*(41^d)} = \frac{41^{d-1}45}{41^d+1}$$

For any d, the denominator is even, and the numerator is not, which contradicts $gcd(2, m''') = 1$. Awesome! Since no such m''' can exist, we have no m'' for $c = 4$.

In general, if $c \equiv 4 \ mod\ 8$, then the denominator will be divisible by 41, as $3^4 \equiv -1 \ mod\ 41$. The numerator will be $-10 \not\equiv 0 \ mod\ 41$, so we get that $m'' = 41^d m'''$ with $gcd(2 * 3 * 5 * 41, m'') = 1$, so

$$\mathcal{A}^*(m''') = \frac{3^{c-2}10(41^d)}{(3^c+1)(41^d+1)}$$

Both terms on the denominator (even after dividing $3^c + 1$ by 41) are even, so the denominator is divisible by 4. The numerator is only divisible by 2, so this implies $2|m'''$, a contradiction!

So the only possibilities are $c \equiv 0, 2, 6 \ mod\ 8$. One important thing we should note and return to is the fact that we're looking modulo 8 because $Ord_{41}(3) = 8$, and we had the idea that 41 would cause a contradiction after one more step.

So we have that $c \equiv 0, 2, 6 \ mod\ 8$ and $c \equiv 1, 2, 3, 4 \ mod\ 5$.

16 Fresh Start

I did some work on paper and just wanted to start this with a fresh start! We worked out a semi-solitary proposition...

Proposition 3 *If a/b is in reduced form and a is odd, then any n with $\mathcal{A}^*(n) = a/b$ must be even.*

Proof 7 *If n is odd, then $\sigma^*(n)$ is even, so $\mathcal{A}^*(n) = EVEN/ODD$ in reduced form. Since a is odd, n cannot be odd.*

This also shows that if both a, b are odd, then any n with $\mathcal{A}^*(n) = a/b$ must have $\nu_2(\sigma^*(n)) = \nu_2(n) \geq 1$. We pick up at least one prime factor for each odd prime dividing n, which gives the bound

$$\nu_2(n) \geq \omega(n) - 1.$$

For example, we have

$$\mathcal{A}^*(2^6 * 3^3 * 5 * 7) = \frac{13}{9} \qquad \mathcal{A}^*(2^4 * 3^2 * 11 * 17) = \frac{15}{11}$$

If we wanted to find such an n with $\nu_2(n) = \omega(n) - 1$, we'd need primes $p|n$ so that $p^{\nu_p(n)} \neq -1 \ mod\ 4$. Which means we have two possibilities:

- $p \equiv 1 \ mod\ 4$ or
- $p \equiv -1 \ mod\ 4$ and $\nu_p(n)$ is even.

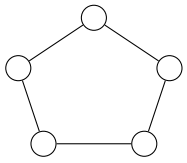
How about $n = 2^3 * 5 * 13 * 17$? Then $\mathcal{A}^*(n) = \frac{1701}{1105}$, which is what we wanted, ODD/ODD. Another is

$$\mathcal{A}^*(2^3 * 3^2 * 5 * 13) = \frac{21}{13}.$$

17 Connections between graph theory and number theory

There are dozens of really good papers, books, and talks on connections between graph theory and number theory. I will focus here on a few of the connections that always really fascinated me.

The first is the study of ***Ramsey Graphs***. Recall the 2-color case of Ramsey's Theorem: There exists a minimal integer $R(a, b)$ so that any edge-coloring of a graph on $n \geq R(a, b)$ vertices contains either a clique of size a or an independent set of size b. This means finding any graph with no a-clique or b-independent set gives a lower bound on $R(a, b)$. Such a graph is called a ***Ramsey Graph*** for $R(a, b)$.

For example, the 5-cycle  contains no triangle (3-clique) and the largest independent set has size 2. Since it contains 5 vertices, this shows

$$R(3, 3) > 5$$

Along with upper bounds, this could allow us to determine a Ramsey number. For example, Erdos showed

$$R(a, b) \leq \binom{a + b - 2}{a - 1}$$

For $a = b = 3$, this shows $R(3,3) \leq 6$. Therefore, $5 < R(3,3) \leq 6$, so $R(3,3) = 6$.

Brendan McKay has done a lot of work and computation on Ramsey Graphs, and has a page dedicated to important facts about them. My first exposure to these was through an off-hand comment in some book I can't quite remember (maybe J.H. van Lint's *A Course in Combinatorics*?), where they stated $R(3,5) = 14$ and $R(4,4) = 18$.

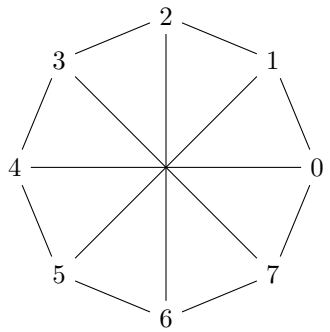
I remembered the book I first saw the Paley graphs out of, in the second part of this document. Murty and Bondy's Graph Theory.

Where this comes from is a paper by Greenwood and Gleason from 1955. Note that $14 - 1 = 13$ and $18 - 1 = 17$, which hints at the method they use to construct these Ramsey graphs: look at the finite fields $\mathbb{F}_{13}$ and $\mathbb{F}_{17}$.

But let's actually start with $R(3,4) = 9$. By the recurrence

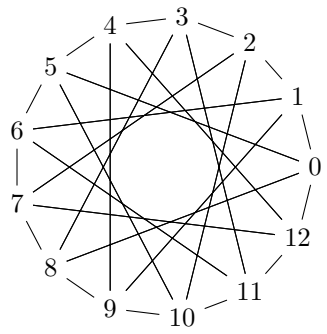
$$R(a,b) \leq R(a,b-1) + R(a-1,b) - 1,$$

we get that $R(3,4) \leq R(3,3) + R(2,4) - 1 = 6 + 4 - 1 = 9$. For the lower bound, we construct a graph on 8 vertices by identifying those vertices with the elements of $\mathbb{F}_8$ and connecting two if their difference is ± 1 or 4 mod 8.



This has no triangles because if $x - y = \pm 1, 4$ and $y - z = \pm 1, 4$, then $x - z = 0, 2, 3, 5, 6$, so there can't be an edge between them. It has no independent subset of size 4. This is easily seen since the largest independent set of the cycle C_8 is 4, and either such set is no longer independent when adding all the diagonals.

With $R(3,5) > 13$, we take a graph G whose vertices are elements of $\mathbb{F}_{13}$, and connect x and y if $x - y$ is a ***cubic residue*** mod 13. Specifically, these are $1, 5, 8, 12$. The fact that -1 is a cubic residue means that this graph is a well-defined undirected graph.

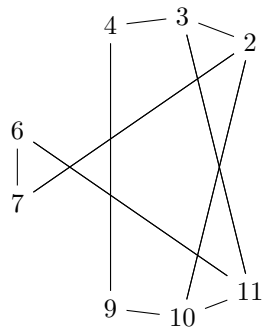


To show this is truly a Ramsey graph, we need to show it has no triangles and no independent set of size 5. For the first fact, note that we can explicitly describe the neighborhood of a vertex x as

$$N(x) = \{x+1, x+5, x-5, x-1\}$$

all taken *mod* 13. If we have a triangle x, y, z, then $y = x + r_1$ and $z = x + r_2$ for two different cubic residues, which means their difference is $r_1 - r_2 = \{3, 4, 7, 11\}$, none of which is a cubic residue, so (y, z) can't be an edge.

If we try to form an independent set of size 5, we can start with 0 by symmetry. Then the remaining four vertices must come from $\{2, 3, 4, 6, 7, 9, 10, 11\}$. Looking at the connectivity of these makes the issue clear.



We need to choose 4 more numbers, and there are three groups, so by the pigeonhole principle, we must choose two numbers in the same group. It can't be $(6, 7)$, so WLOG, assume it is 2 and 4. But then the only remaining vertices are $(6, 11)$, which is an edge. So no independent set of size 5 can exist.

But that was combinatorial and I promised algebraic! The multiplicative group $\mathbb{F}_{13}^{\times}$ is isomorphic to $\mathbb{Z}/12\mathbb{Z}$ and has a generator g, which we can just choose to be 2. Let $R = \{1, 5, 8, 12\}$ be the subgroup of cubic residues. The cosets $gR = \{2, 3, 10, 11\}, g^2R = \{4, 6, 7, 9\}$ partition the set of non-residues into two sets of size 4.

By symmetry, we can suppose our independent set looks like $\{0, v_1, v_2, v_3, v_4\}$, where v_i are all non-residues. We see that gR contains four edges in a square

and g^2R contains two disjoint edges, so we can't have all the v_i in one coset. In fact, it also shows that if we have three v_i in one coset, we're forced to have an edge. So WLOG, let's say $v_1, v_2 \in gR$ and $v_3, v_4 \in g^2R$.

In gR, it has to be either $(2, 11)$ or $(3, 10)$. If $(v_1, v_2) = (2, 11)$, then we have edges $(2, 7)$ and $(11, 6)$ between cosets, which would force $(v_3, v_4) = (4, 9)$, which is an edge, contradicting independence. If $(v_1, v_2) = (3, 10)$, then we get edges $(3, 4)$ and $(10, 9)$ between cosets, which would force $(v_3, v_4) = (6, 7)$, which is an edge, giving a contradiction. So there can be no independent set of size 5.

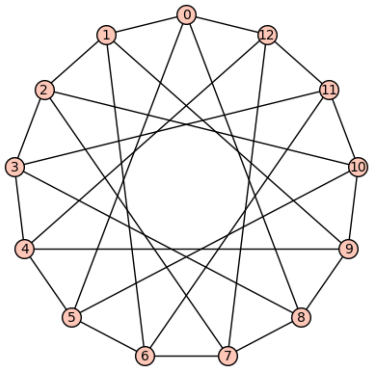
Still doesn't feel totally algebraic, more a reformulation of the combinatorial argument, but I did feel more comfortable arguing with the cosets!...but we'll dive deeper into this ***Finite Field Method*** for Ramsey Graphs and get a better feel.

Let's see if we can do $R(4, 4)$ in the same way. We define our graph G to be on 17 vertices, connecting x and y iff $x - y$ is a quadratic residue mod 17. Note that $-1 = 4^2 \ mod \ 17$ is a quadratic residue, so the graph is again well-defined.

Before actually working on that, let's write some code to create these graphs, since that will be helpful if we want to look at invariants of these graphs later. We'll call it $FFM(p, r)$, where we connect x and y iff $x - y$ is an r^{th} residue mod p. This is pretty easy, code-wise. We generate $Rset$ of r^{th} powers mod p, and then we check that -1 is in this set, and return an error if not. Then we run through all pairs (a, b) and check whether their difference is in Rset. Then $G = Graph(E)$ generates the graph!

```
def FFM(p,r):     #(x,y) in E iff x - y = r^th power mod p
    Rset = list(Set([mod(x^r,p) for x in range(1,p)]))
    if p-1 not in Rset:
        return('Graph not well-defined')
    else:
        E = []
        for a in range(p-1):
            for b in range(a+1,p):
                if mod(b - a,p) in Rset:
                    E.append((a,b))
        G = Graph(E)
        return(G)
```

When we plot it, we want to make sure we add $layout = `circular'$ (but don't copy and paste this because it won't work right). For $p = 13$ and $r = 3$ (what we just worked through), this looks like



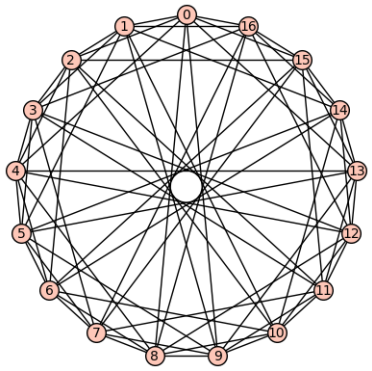
Much nicer than my tikz drawing! And to be explicit, the two functions we want to check are

```
G.clique_number()
G.complement().clique_number()
```

If C is the first number and I is the second, then this means our graph gives a lower bound

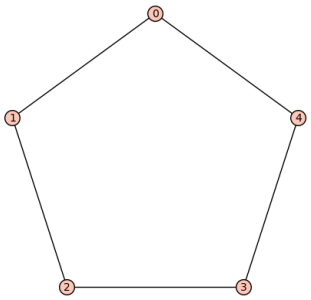
$$R(C+1, I+1) > p.$$

For example, with $FFM(13,3)$, we get $C = 2$ and $I = 4$, which shows $R(3,5) > 13$. To show that $R(4,4) > 17$, we'll use the graph $FFM(17,2)$, and prove $C = I = 3$.



Of course, I'm sure a search over all such graphs to very many vertices has already been done. I did a small search myself years ago and rediscovered a few bounds, which is fun!

Let's fix $r = 2$ and go through a few primes and see what graphs we get. I will color others' bounds in blue to differentiate between what these give and the best current bounds.



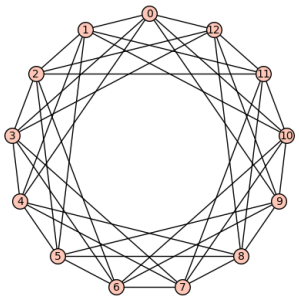
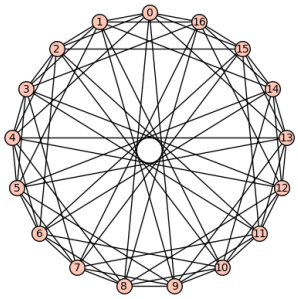


Figure 1: $FFM(5,2)$, $C = I = 2$ Figure 2: $FFM(13,2)$, $C = I = 3$

So we see that the cycle graph bounding $R(3,3) > 5$ comes about in this way, looking at quadratic residues mod 5. The right graph gives the bound $R(4,4) > 13$, which is not as good as $FFM(17,2)$. For completeness, we'll include $FFM(17,2)$ again but also $FFM(29,2)$. I should mention that characterizing quadratic residues mod p tells us that -1 is a residue mod p iff $p \equiv 1 \; mod \; 4$.



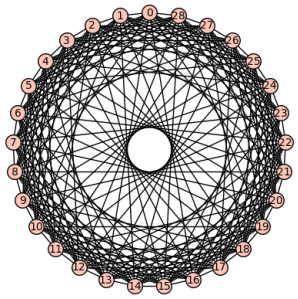


Figure 3: $FFM(17,2)$, $C = I = 3$ Figure 4: $FFM(29,2)$, $C = I = 4$

The bound given by the left graph is tight, but the right graph gives a bound of $R(5,5) > 29$, while we know that $43 \leq R(5,5) \leq 48$. Continuing on, I love the way these graphs look.

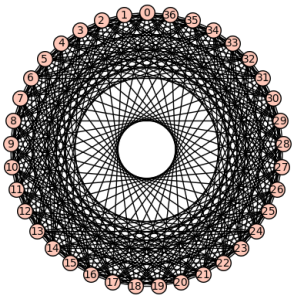


Figure 5: $FFM(37,2)$, $C = I = 4$

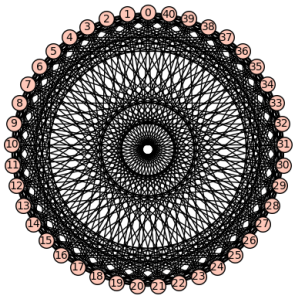
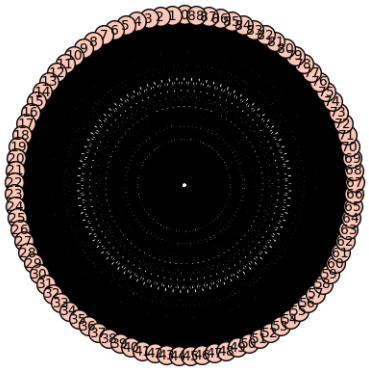


Figure 6: $FFM(41,2)$, $C = I = 5$

This gives the better bound $R(5,5) > 37$, and the right graph gives $R(6,6) > 41$ (with the best current bounds $102 \leq R(6,6) \leq 165$). Though things start to get crowded, we get a better bound of $R(6,6) > 89$ with $FFM(89,2)$:



I'm going to stop plotting them, but here are some results just from these quadratic residue graphs with primes $p < 200$:

$$R(5,5) > 37$$

$$R(6,6) > 101$$

$$R(7,7) > 109$$

$$R(8,8) > 193$$

$$R(9,9) > 197$$

That's awesome! If you notice, $R(6,6) > 101$ is the best lower bound currently known, and we get it from $FFM(101,2)$.

Let's pivot to looking at cubic residues. And more plots!

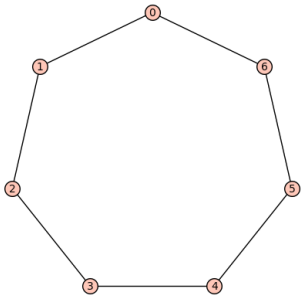


Figure 7:
$FFM(7,3), \quad C = 2, I = 3$

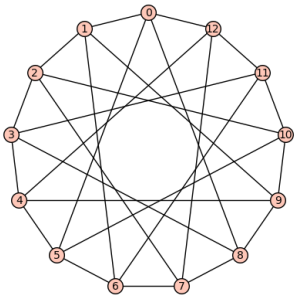


Figure 8:
$FFM(13,3), \quad C = 2, I = 4$

The left gives $R(3,4) > 7$, which isn't as good as our eight-vertex graph, but not bad! The right is, of course, the graph we worked through to show $R(3,5) > 13$, which is a tight bound.

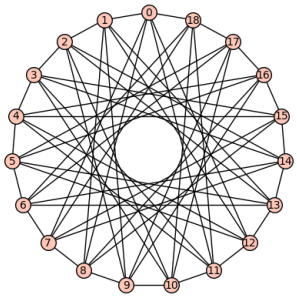


Figure 9:
$FFM(19,3), \quad C = 3, I = 4$

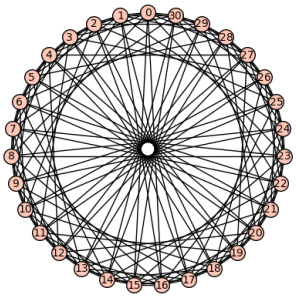


Figure 10:
$FFM(31,3), \quad C = 3, I = 6$

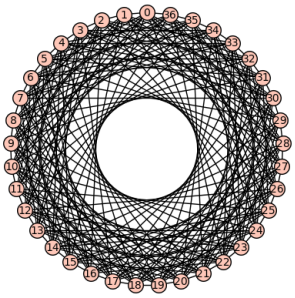


Figure 11:
$FFM(37,3), \quad C = 3, I = 7$

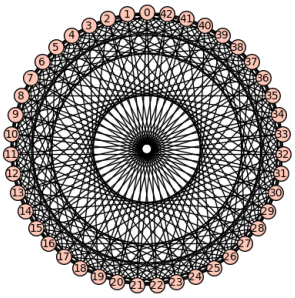


Figure 12:
$FFM(43,3), \quad C = 3, I = 7$

Some further bounds gotten from cubic residue graphs for primes $p < 200$

are:

$$R(4,5) > 19 \qquad R(4,7) > 31$$
$$R(4,8) > 43 \qquad R(4,9) > 67$$
$$R(4,10) > 79 \qquad R(4,12) > 127$$
$$R(5,9) > 73 \qquad R(5,11) > 139 \qquad R(5,14) > 199$$
$$R(6,9) > 97 \qquad R(6,10) > 109 \qquad R(6,12) > 181$$
$$R(7,11) > 163$$

None of these are optimal.

Quartic residue graphs go as follows:

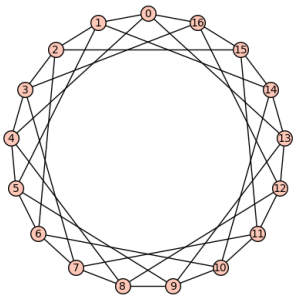


Figure 13:
$FFM(17,4), \quad C = 2, I = 6$

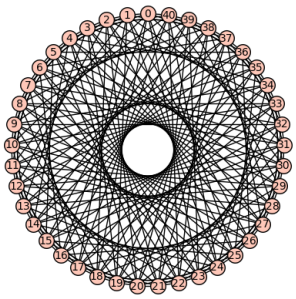


Figure 14:
$FFM(41,3), \quad C = 2, I = 10$

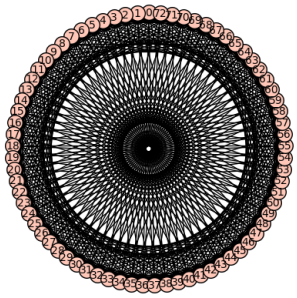


Figure 15:
$FFM(73,3), \quad C = 3, I = 11$

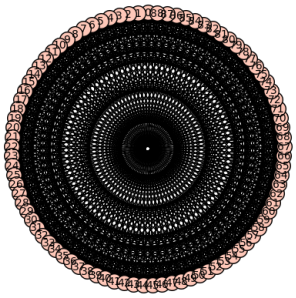


Figure 16:
$FFM(89,3), \quad C = 3, I = 13$

This gives the bounds $R(3,7) > 17$ (and it is known that $R(3,7) = 23$) and $R(3,11) > 41$ (with the best lower bound currently $R(3,11) > 45$). Some other bounds we get are

$$R(6,11) > 137, \qquad R(5,15) > 193$$

Neither of these are optimal. Setting this up in a nice way, let's generate a bunch of bounds and collect the best:

```
r=5
for p in list(primes(200)):
    if -1 in [mod(x^r,p) for x in range(1,p)]:
        G = FFM(p,r)
        print('R('+str(G.clique_number() + 1)+','+str(G.complement().clique_number() + 1)+')
```

The output of this looks like this:

```
R(3,2)>2
R(3,3)>5
R(4,4)>13
R(4,4)>17
R(5,5)>29
R(5,5)>37
R(6,6)>41
R(6,6)>53
R(6,6)>61
R(6,6)>73
R(6,6)>89
R(7,7)>97
R(6,6)>101
R(7,7)>109
R(8,8)>113
R(8,8)>137
R(8,8)>149
R(8,8)>157
R(9,9)>173
R(8,8)>181
R(8,8)>193
R(9,9)>197
R(10,10)>229
R(8,8)>233
R(8,8)>241
R(8,8)>257
R(9,9)>269
R(9,9)>277
R(8,8)>281
R(9,9)>293
R(9,9)>313
R(10,10)>317
R(10,10)>337
R(10,10)>349
R(10,10)>353
R(9,9)>373
```

And we could look for smaller input numbers lower on the list for the best bounds we can get. For example, $FFM(281, 2)$ gives the current best lower

bound of $R(8,8) > 281$. We also get from this further search:

$$R(9,9) > 373, \qquad R(10,10) > 569$$

$$R(11,11) > 577, \qquad R(12,12) > 641$$

It's very exciting watching better and better bounds come in!

Switching to $r = 3$, cubic residues, we get the bounds

$$R(5,15) > 241$$

$$R(6,12) > 229$$

$$R(6,15) > 271$$

I've always thought it would be nice to be able to expand this to all integers. And we can! As long as -1 is an r^{th} residue, then we can form the graph in the exact same way. Do any better bounds arise from these? Not that I can tell. But I cleaned up the code a bit and went a bit further with the prime graphs for $r = 2$.

```
def FFM(p,r): #(x,y) in E iff x - y = r^th power mod p
    Rset = list(Set([mod(x^r,p) for x in range(1,p)]))
    E = [(a,mod(a+r,p)) for a in range(p) for r in Rset]
    G = Graph(E)
    return(G)
```

These are still nowhere near the current best bounds.

$$R(11,11) > 709, \qquad R(12,12) > 829, \qquad R(13,13) > 821 \qquad R(14,14) > 853$$

I take it back! The best known lower bound $R(10,10) < 797$ can be obtained by $FM(797,2)$, which is awesome!

18 Difference Graphs

The previous section made me realize that the set of residues isn't particularly special (although the multiplicative structure was nice). All we really need is a set $D \subseteq \{0,\ldots,n-1\}$ so that $D = -D$ (*centrally symmetric*, as sets) and we can define a graph $G(D)$ with vertex set $\{0,\ldots,n-1\}$ and an edge between x and y iff $x - y \in D$. The fact that $D = -D$ means this is well-defined. Let's do a few examples.

- If $D = \{0,\ldots,n-1\}$, then $G(D) = K_n$.
- If $D = \emptyset$, then $G(D)$ is the trivial graph on n vertices.
- In general, $G(D^c) = G(D)^c$.

- If $D = \{evens\}$, then (x, y) is an edge iff x and y are the same parity. So we get two disjoint cliques, and $G(D) = K_{\lfloor n/2 \rfloor} \sqcup K_{\lceil n/2 \rceil}$.
- Which means that if $D = \{odds\}$, $G(D)$ is a bipartite graph with parts as equal as possible. In other words, $G(D)$ is the Turan graph $T(n, 2)$.
- In general, take $D = \{x \mid x \equiv 0 \ mod \ k\}$. Then (x, y) is an edge iff $x \equiv y \ mod \ k$, so $G(D) = T(n, k)$, the k-multipartite Turan graph on n vertices.
- If $D = \{\pm 1\}$, then $G(D) = C_n$ is the cycle graph on n vertices.

Letting $C(D)$ and $I(D)$ be the clique number and independence number of $G(D)$, we want to minimize $C(D) + I(D)$ over all centrally symmetric subsets D for which $G(D)$ is connected, which should give the smallest Ramsey number $R(C(D) + 1, I(D) + 1)$ that is bounded below by n.

I'll try to work through some probabilistic arguments with the expected value of $C(D)$ and $I(D)$ when choosing a random centrally symmetric subset D. It seems that they're usually not giving great bounds, but I'll work on it more tomorrow!

For now, I want look at the case when $D = \{\pm p \mid p \leq n \ prime\}$. Here are a few plots with their corresponding Ramsey bound:

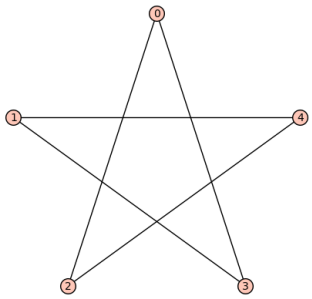


Figure 17: $R(3, 3) > 5$

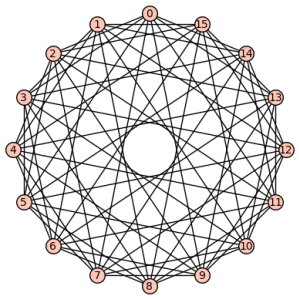


Figure 18: $R(5, 5) > 16$

It seems like these graphs often have very large independent sets, so tend to not make good bounds. Let's go back to the previous stuff. Let's start with counting centrally symmetric subsets mod n and determining the connectivity of $G(D)$.

Every centrally symmetric subset has the form

$$\{m_1, \ldots, m_t, -m_1, \ldots, -m_t \mid m_i \leq \frac{n}{2}\}.$$

This means every centrally symmetric subset D of $\{0, \ldots, n-1\}$ can be written as $D' \cup -D'$ for a subset $D' \subseteq \{0, \ldots, \lfloor \frac{n}{2} \rfloor\}$, which tells us the number of centrally symmetric subsets is just $2^{\lfloor n/2 \rfloor}$.

For example, with $n = 6$, we get four distinct graphs. The empty set, and these three:

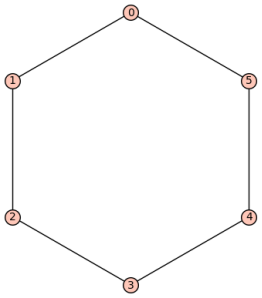


Figure 19: $D = [1, -1]$

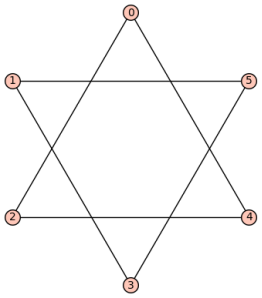


Figure 20: $D = [2, -2]$

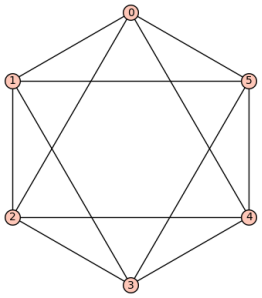


Figure 21: $D = [1, 2, -1, -2]$

The best bounds we get here are $R(3, 4) > 6$. It also visually shows a fact we didn't pick up before,

$$G(D_1 \cup D_2) = G(D_1) \cup G(D_2),$$

where we consider the union of two graphs on the same vertex set to have edge set a union of the edges of $G(D_1)$ and $G(D_2)$. And it shows one fact about connectivity:

Proposition 4 *Let $D = \{\pm k\}$, then $G(D)$ is connected iff $gcd(k, n) = 1$.*

Proof 8 *This isn't too hard - we form $G(D)$ by starting at a vertex and adding k to it until we get back to itself. The length of such an orbit is the size of the subgroup generated by k inside $\mathbb{Z}/n\mathbb{Z}$, which is $n/gcd(n, k)$. Therefore, $G(D)$ is the disjoint union of $\gcd(n, k)$ cycles of length $n/gcd(n, k)$. In symbols,*

$$G(D) = \bigsqcup_{i=1}^{gcd(n,k)} C_{n/gcd(n,k)}$$

and the proposition follows.

All centrally symmetric can be written as $D = \sqcup_i \{\pm m_i\}$ where each $m_i \leq n/2$. And therefore $G(D)$ is the union of each of these individual graphs. Which further means that $G(D)$ is the union of

$$\sum_i gcd(n, m_i)$$

cycles. We should also mention here the well-studied area of ***gcd-sums***. We'll look at this in a moment to see if we can count the number of cycles $G(D)$ is composed of.

But this doesn't really make the study of $G(D)$ any easier - the gluing of each of these subgraphs could be done in non-straightforward way and produce a complicated $G(D)$.

Let's do another example with $n = 7$.

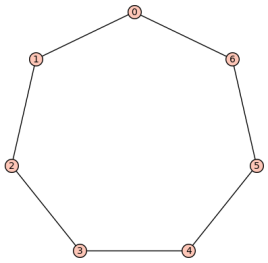


Figure 22: $D = [1, -1]$

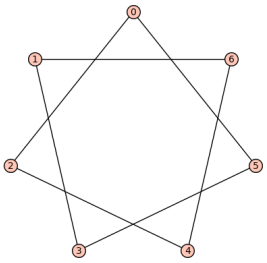


Figure 23: $D = [2, -2]$

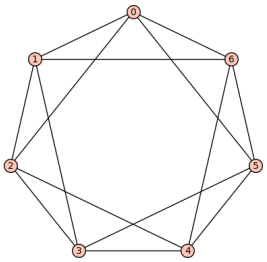


Figure 24: $D = [1, 2, -1, -2]$

And the best bound we get is $R(3, 4) > 7$. Let's do $n = 8$ next. Ignoring the empty and trivial cycle graph, we get

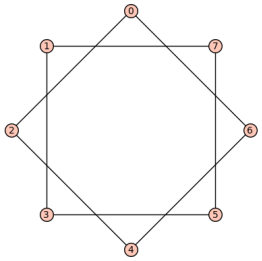


Figure 25: $D = [2, -2]$

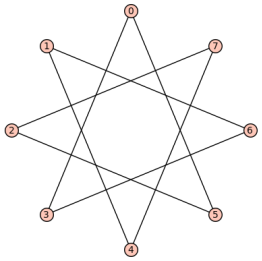


Figure 26: $D = [3, -3]$

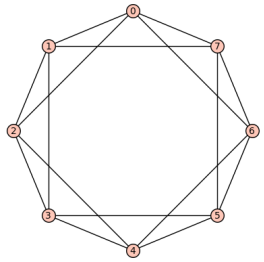


Figure 27: $D = [1, 2, -1, -2]$

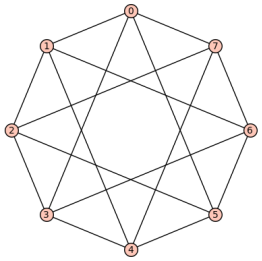


Figure 28: $D = [1, 3, -1, -3]$

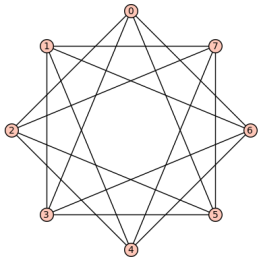


Figure 29: $D = [2, 3, -2, -3]$

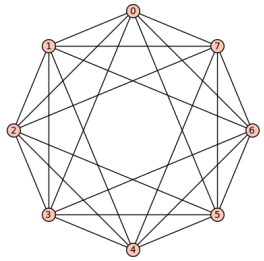


Figure 30: $D = [1, 2, 3, -1, -2, -3]$

with graphs 3 and 5 giving the best lower bound $R(3, 4) > 8$, and graphs 4 and 6 giving the bound $R(3, 5) > 8$. Continuing on with n, I'll list any tight

lower bounds or best-known lower bounds that appear. The first we encounter is $R(3,5) > 13$, which we get with two subsets:

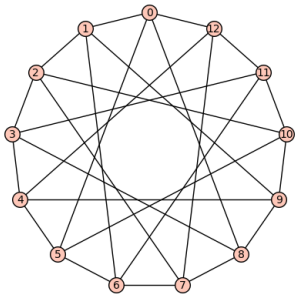


Figure 31: $D = [1, 5, -1, -5]$

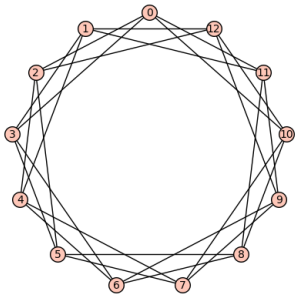


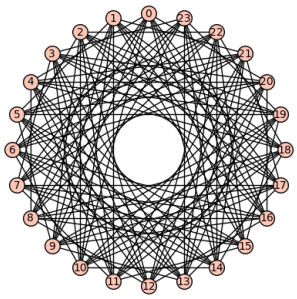
Figure 32: $D = [2, 3, -2, -3]$

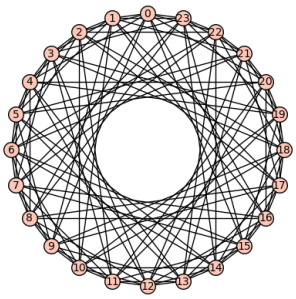
This is a wonderful method! We get four sets D that give a Ramsey graph showing $R(4,5) > 24$, which is the best lower bound since $R(4,5) = 25$. These sets are

$$[1, 2, 4, 8, 9, -1, -2, -4, -8, -9], \qquad [2, 3, 4, 8, 11, -2, -3, -4, -8, -11]$$

$$[3, 4, 5, 8, 10, -3, -4, -5, -8, -10], \qquad [4, 7, 8, 9, 10, -4, -7, -8, -9, -10]$$

And all of these produce an isomorphic graph, two of which look like:





The next best lower bound is $R(4,6) > 35$. Let's give it a go! In a surprising (but probably should not be...) twist, **the search completed with no graphs found!** Which means a difference graph is *not* the type of graph giving the bound $R(4,6) > 35$. A search for difference graphs with $C < 6$ and $I < 6$ on 36 vertices revealed a lot of $C = I = 5$ graphs, which give the bound $R(6,6) > 36$, which is nowhere near the current best. But we also find a few with $C = 4$ and $I = 5$, which give $R(5,6) > 36$, while the current best lower bound is $R(5,6) > 57$. Here are a couple of these graphs.

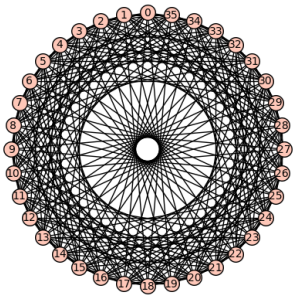


Figure 33:
$[\pm 2, \pm 3, \pm 7, \pm 9, \pm 10, \pm 12, \pm 17]$

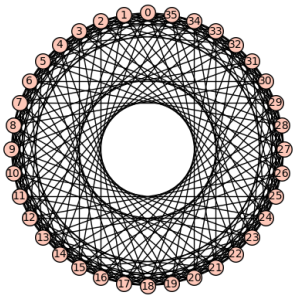


Figure 34:
$[\pm 1, \pm 2, \pm 4, \pm 5, \pm 7, \pm 12, \pm 14]$

We'll go ahead and do an exhaustive search over difference graphs on 36 vertices to see if any $R(4,6)$ Ramsey Graphs appear. In fact, looking through difference graphs on 40 vertices will either produce a Ramsey graph for $R(4,6)$ that is new, or it will return no graph, which means that any maximal Ramsey graph for this number cannot be a difference graph.

Let's try to make this search a little more reasonable. The set giving $R(3,4) > 8$ had $4 = (0.50)(8)$ elements, the set giving $R(3,5) > 13$ had size $4 = (0.308)(13)$. The set giving $R(4,5) > 24$ had size $10 = (0.417)(24)$. It would make sense that if D was too small, then we'd have too large independent sets. So let's restrict to $|D| \geq n/4$.

To try to find a lower bound on $R(4,6)$, we search over difference graphs on 40 vertices with $10 \leq |D| \leq 20$ and check if $(C, I) = (3,5)$ or $(5,3)$. In the meantime, let's try to give a proof that this is sufficient. To be more specific,

Proposition 5 *Given $k \leq n$, there exists $\alpha \in (0,1)$ so that if $|D| < \alpha \frac{n}{2}$, then $C(D) \geq k$ or $I(D) \geq k$.*

First, note that $G(D)$ is always $|D|$-regular, so the handshaking lemma tells us $|E| = \frac{n|D|}{2}$. Turan's theorem tells us that if $|E(G)| > \left(1 - \frac{1}{k}\right) \frac{n^2}{2}$, then G contains a copy of K_k. Then for small $|D|$, the graph $G(D)^c$ has enough edges to guarantee a clique of size k, which shows $I(D) \geq k$. Specifically, if

$$\frac{n(n-1)}{2} - \frac{|D|n}{2} > \left(1 - \frac{1}{k}\right) \frac{n^2}{2},$$

then $I(D) \geq k$. This works out to

$$\text{If } |D| < \frac{n-k}{k}, \text{ then } I(D) \geq k$$

So we can be sure that if $|D| < \frac{40-6}{6} = 5.67$, then $G(D)$ is not a Ramsey graph for $R(4,6)$. Which means our search is missing the cases $6 \leq |D| \leq 11$, which we'll perform separately if the original search ever actually finishes.

And...three and a half hours later, it timed out! Let's try to split it up into smaller chucks and sort by $|D|$, putting a Y when we've checked and an N otherwise. This time, I'm being smarter and printing an update when we're 1/4, 1/2, 3/4, and done, which is very helpful for morale, waiting for a while but eventually seeing a 1/4 pop up.

$\lvert D\rvert$	6	8	10	12	14	16	18	20
Y/N	Y	Y	Y	Y	N	N	N	N

The first three were fairly quick. The subsets of size 12 took an hour and 45 minutes. The subsets of size 14 took almost 7 hours. That makes me worried for the last three!

Before letting that take over my computer, I wanted to try the obvious brute force method of trying to form a Ramsey graph for $R(a, b)$. Sagemath has the IndependentSets module that allows us to randomly choose from a graph G a random maximal clique C and a random maximal independent set I. So our strategy will go as follows:

1. Initialize a graph $\mathcal{R}(n, a, b)$ on n vertices - either empty or choose a random graph.
2. Generate C and I.
3. If $|C| \geq a$, then we randomly choose an edge $e \in C$ and remove it.
4. If $|I| \geq b$, then randomly add an edge to I.
5. Go to (2).

My intuition is that iterating this should naturally push us towards graphs that are Ramsey graphs for $R(a, b)$. In fact, if we reach a point where $R(n, a, b)$ has no a-clique and no b-independent set, then our program stops and we can conclude $R(a, b) > n$. Conversely, if the program runs "long enough", then we could say with high likelihood that $R(a, b) \leq n$.

To formalize this, for a graph G on n vertices, let

$$f(G) = (G - \{e_1\}) \cup \{e_2\}$$

for randomly chosen $e_1 \in C$ and $e_2 \in I$, if $|C| \geq a$ or $|I| \geq b$. Then our question is whether iterating f eventually leads to a fixed point, if such a fixed point exists. I wonder if any of the classic fixed point theorems could apply here to help count the number of Ramsey graphs on n vertices.

One direction this might take us is to consider the symmetric difference on the set of graphs on n vertices. This forms a group and if we take intersection as multiplication, gives us a ring. Further, the symmetric difference is nice enough that we can even consider this set as a metric space.

In this metric space, any Cauchy sequence is eventually constant, and therefore its limit is that graph. This shows the space is complete, which means we

could possibly apply, for example, the Banach fixed-point theorem. This proves what our intuition would imply: Any mapping that is a contraction will fix a unique point.

A contraction is something that shrinks distances between any pair of points. The distance between two graphs is given by the size of their symmetric difference, meaning $d(G_1, G_2) = |E_1| + |E_2| - |E_1 \cap E_2|$. In other words, it is the number of edges belonging to either graph, but not both.

Consider $d(f(G_1), f(G_2))$. Then

$$f(G_1) = (G_1 - \{e_{11}\}) \cup \{e_{12}\}$$

$$f(G_2) = (G_2 - \{e_{21}\}) \cup \{e_{22}\}$$

If both graphs have at least an a-clique and a b-independent set, then both graphs gain an edge and lose an edge, so $|E_1|$ and $|E_2|$ don't change. But if the edge we add is the same for both graphs and the edge we remove is different, $|E_1 \cap E_2|$ will decrease by 1, so the distance increases. So it's not quite a contraction, but still an interesting point of view!

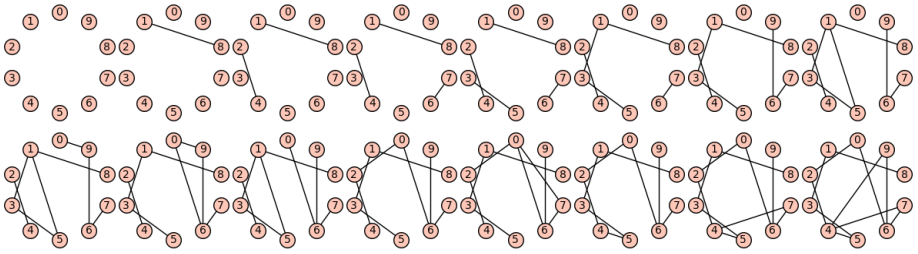
An easier way to see this is that the empty graph has distance n to the complete graph K_n. Applying f to the empty graph adds an edge and applying f to K_n removes an edge. If these are the same edge, then the distance remains the same.

19 Random Ramsey Graphs

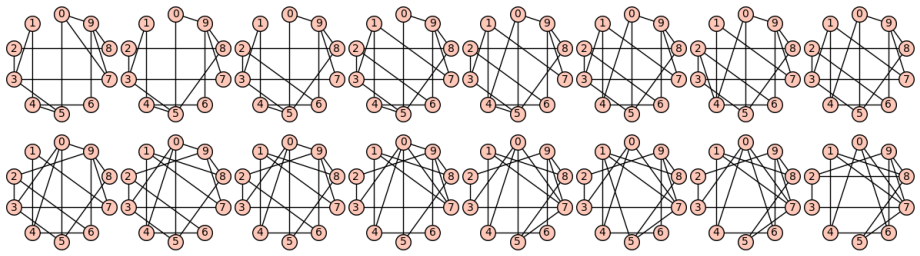
First, I found a blog post that makes all this "difference graph" stuff much clearer! These graphs are actually commonly referred to as *circulant graphs*, and ComputationCombinatorics goes through some wonderful results on the clique number and independence number of these graphs. One nice result that I want to record is on the connectivity of $G(D)$. It's a result that is familiar to another topic I'll touch on later. And it's not particularly hard to prove.

Theorem 28 *Let $D = \{d_1, \ldots, d_t\}$. Then $G(D)$ is connected if and only if $gcd(n, d_1, \ldots, d_t) = 1$*

Let's focus now on coding up the program we talked about in the last section. We'll initialize with the empty graph for now, but maybe later we'll see if there is much of a difference starting with a random (Erdos-Renyi) graph. Here's an example of $RR(10, 3, 3)$, iterated 15 times.



Letting it run further, we can look at a portion where we've gained more edges.



So for completeness, here's the code I used. First we define $RR(n, a, b)$:

```
def RR(n,a,b):
    G = graphs.EmptyGraph()
    G.add_vertices(list(range(n)))
    Glist = [plot(G,layout='circular')]
    for i in range(40):
        G = ICcheck(G,a,b)
        if G == 'done':
            Glist.append(G)
            break
        else:
            Glist.append(plot(G,layout='circular'))
    return(Glist)
```

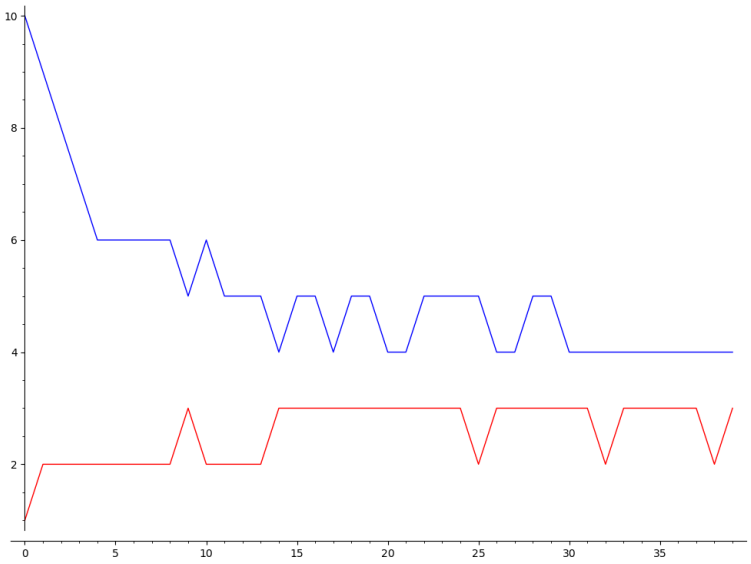
This initializes an empty graph, adds n vertices, begins a list with the plots of each graph, and then iterates however many times we want through performing $ICcheck(G, a, b)$ and then adding that graph to the list. ICcheck is a function we'll define to check a graph for independent sets of size $\geq b$ and cliques of size $\geq a$. If it doesn't find any, it returns the string 'done', which we check for.

```
def ICcheck(G,a,b):
    I = G.independent_set()
    C = G.clique_maximum()
    c = 0
    if len(I) > b-1:
        e1 = sample(I,2)
        G.add_edge(e1)
        c+=1
    if len(C) > a-1:
        e2 = sample(C,2)
        G.delete_edge(e2)
        c+=1
    if c > 0:
        return(G)
    else:
        return('done')
```

One helpful command is $sample(S, k)$ which will choose k elements from S at random. Then to plot it, we want to use $graphics_array$, possibly having to change the figure size when we *show* or *save*.

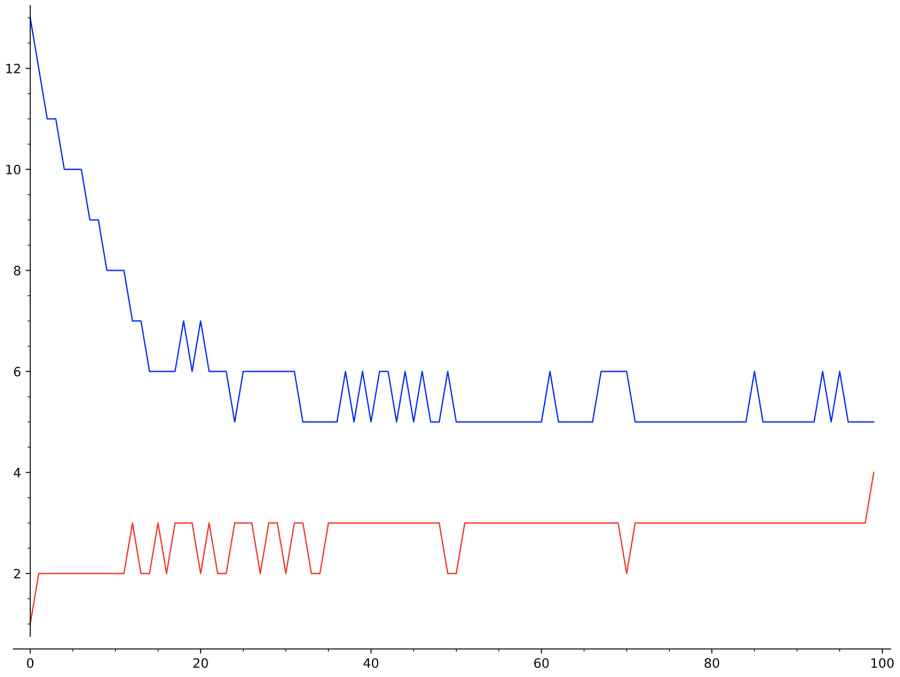
```
GL = RR(10,3,3)
A = graphics_array([GL[24:32],[GL[33:]])
save(A,'RR1033_3.png',figsize=12)
```

We could also redefine $RR(n, a, b)$ with a while loop ending when ICcheck returns 'done', but we'll do it like this so that it doesn't run endlessly. Plotting the independence number (blue) and clique number (red), we see a nice bouncing around 3, which it will keep doing since $R(3, 3) = 6 < 10$.

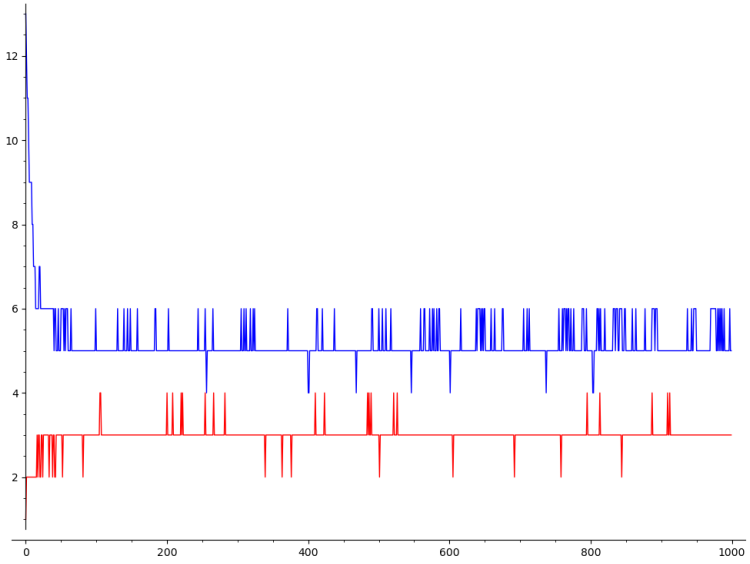


In fact, the independence number won't dip below 4 because $R(3, 4) = 9 < 10$. Let's test some n that we know bound ramsey numbers. For example, since $R(3, 5) = 14$, let's look at $RR(13, 3, 5)$. We check that $FFM(13, 3)$ really does return $'done'$.

```
input:  ICcheck(FFM(13,3),3,5)
output: ('done', 4, 2)
```

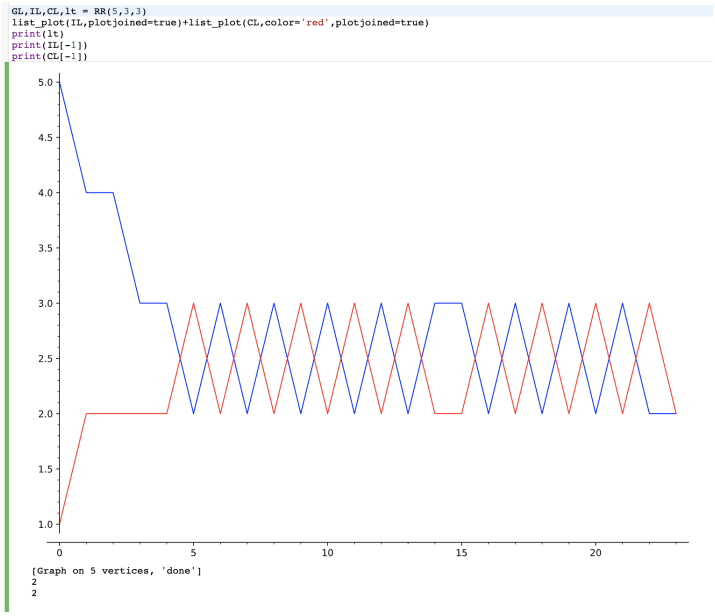


By the end of 100 iterations, we get a graph with independence number 5 and clique-number 4. I'll increase the iteration and let's see if we ever hit a Ramsey graph:

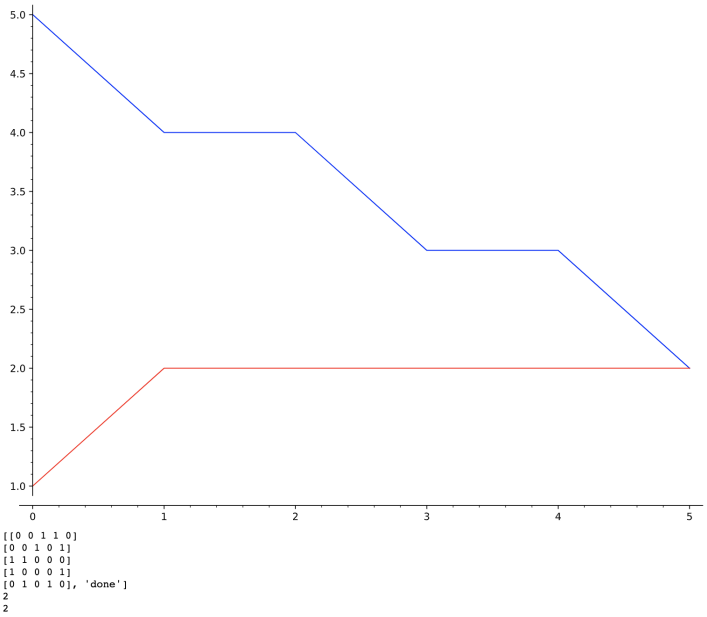


After 1000 iterations, we get close, but never quite hit a graph with $I = 4$ and $C = 2$ at the same time.

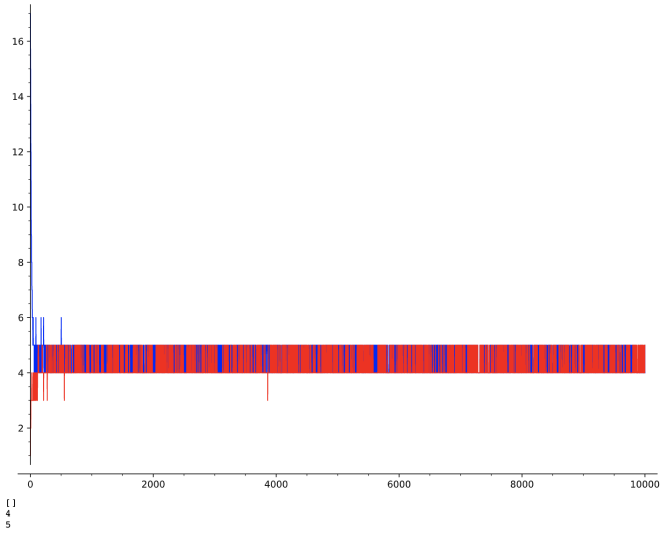
To see what it looks like when we do hit a Ramsey graph, watch the way the independence and clique numbers of $RR(5,3,3)$ swap back and forward until they finally land on $(2,2)$, which is the Ramsey graph for $R(3,3) = 6$.



This is a screenshot including the input and output. One thing I added was ‘lt‘ = last two graphs. That way if we recieve a ’done’, we can see what the previous graph was, in this case it’s a graph object, but in general, I’m outputting the adjacency matrix so that it’s easy to replicate the graph if found. And while the last took about 25 iterations to stop, the following took only 5:

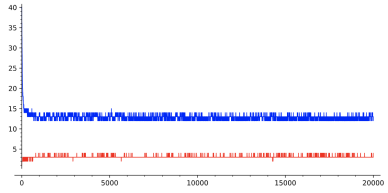


But when trying to find the $R(4,4)$ Ramsey graph, for example, we look at $RR(17,4,4)$, which seems to be stuck with graphs with 4/5-cliques and independent sets.



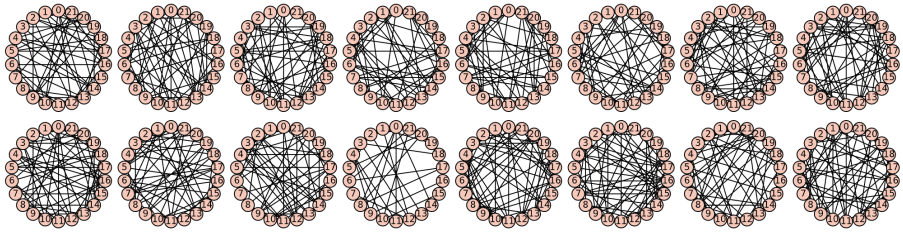
Let's look at one with the inputs further apart. For example, we have the best current bounds $39 < R(3,10) < 44$, so let's look at $RR(40,3,10)$, with 20000 iterations. The best pair we find is $I = 12$ and $C = 3$, which only gives the bound $R(4,13) > 40$, while the current best is $R(4,13) > 132$. It did also find

$R(3,14) > 40$, while the best lower bound is $R(3,14) > 65$, so that's better. The list at the bottom is new pairs (I, C) as we find them.



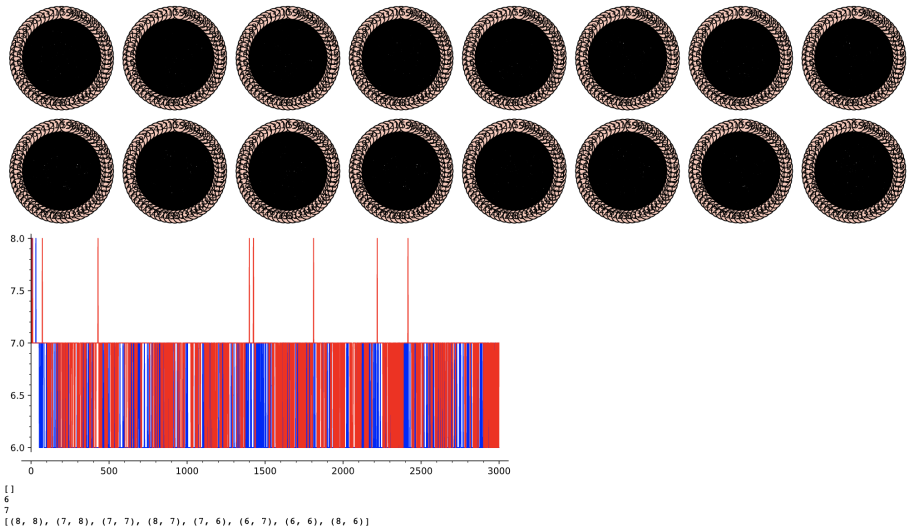

```
[]
13
3
[(40, 1), (39, 2), (38, 2), (37, 2), (36, 2), (35, 2), (34, 2), (33, 2), (32, 2), (31, 2), (30, 2), (29, 2), (28, 2), (27, 2), (26, 2), (25, 2), (24, 2), (23, 2), (22, 2), (21, 2), (20, 2), (19, 2), (19, 3), (18,
2), (18, 3), (17, 2), (17, 3), (16, 3), (16, 2), (15, 2), (15, 3), (14, 3), (14, 2), (13, 3), (13, 2), (12, 3), (13, 4), (12, 4), (14, 4)]
```

The whole plotting part is weighing down the memory a ton, so let's rewrite this to get the (I, C) values explicitly. I also just realized writing it like this is confusing when the inputs look like (C, I). So from now on, we'll always list cliques first. Anyway, here are a few graphs randomly sampled from $RR(22, 3, 7)$, since we know $R(3, 7) = 23$.

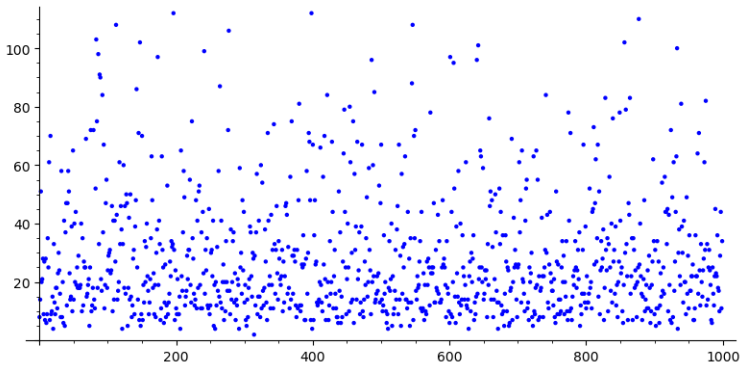


For graphs on larger numbers of vertices, this gets computationally heavy as it just builds more and more sparse graphs until there are enough edges to be interesting. So let's try altering the program by beginning with a Erdos-Renyi graph with $p = 1/2$, meaning we randomly add edges between vertices with independent probability $1/2$. In Sagemath, this command is $graphs.RandomGNP(n, p)$.

In this case, we are looking at $RR(60, 4, 4)$ and the graph we initially generated had $C = I = 8$. This looks ridiculous, but I'll show it anyway. The best bound we get from this is $R(7, 7) > 60$, which is far from the best $R(7, 7) > 204$.



Another thing I'd like to try calculating is the average number of iterations it takes to take a reach a Ramsey graph in a case we know like $RR(5,3,3)$ or $RR(8,3,4)$. Running $RR(8,3,4)$ a thousand times, here are the number of iterations each attempt took, with average 28.101.



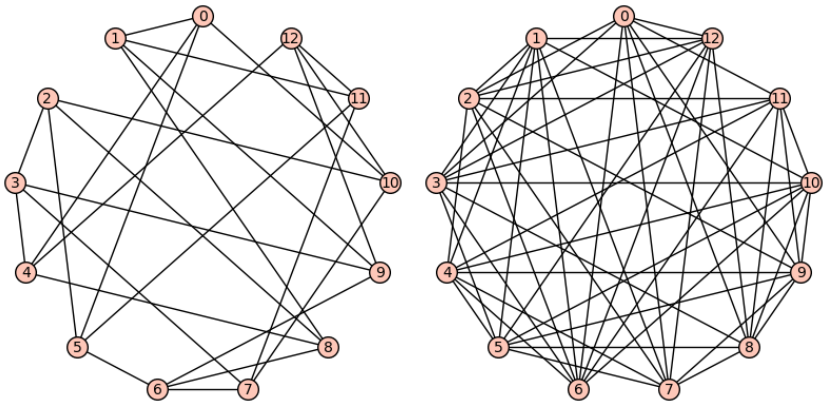
Repeating this sampling ten more times gives the following averages.

$$[27.539, 28.078, 27.206, 28.781, 28.487, 26.687, 26.408, 28.041, 28.963, 27.612]$$

which makes it seem like perhaps the expected number of iterations should be 28. To be more formal, the central limit theorem tells us that as we take more and more samples, the average of the above set will converge to the true average. Letting it run 50 times, our average is 27.65. Another 50 sample means give an estimated population mean of 27.745. And one more time gives 27.691 with a standard deviation of 0.667.

Let's do this with $RR(5,3,3)$ and see what we get. Using 100 sample means, we get an average of 10.445 with standard deviation 0.241.

Rewriting the code to let it run until it hits a Ramsey graph is awesome! For another example, since we know $R(3,5) = 14$, we can look at $RR(13,3,5)$. Doing so returned a Ramsey graph after 88720 iterations. On the left is the graph we got and on the right is its complement.

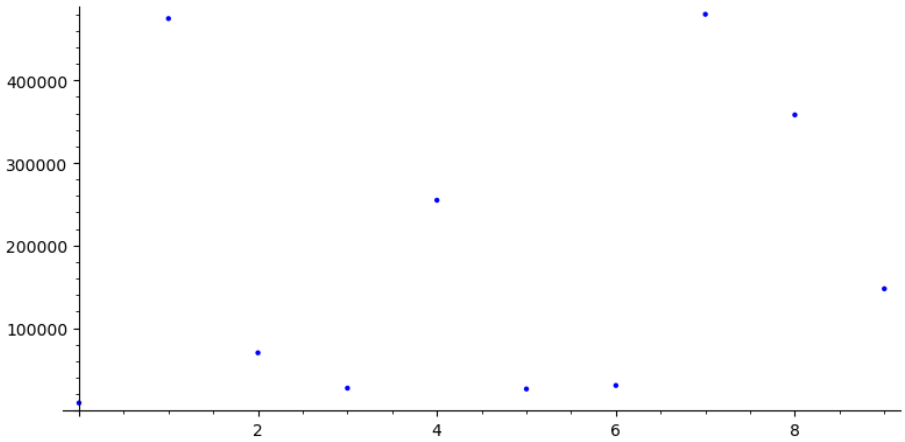


The pairs we hit along the way were

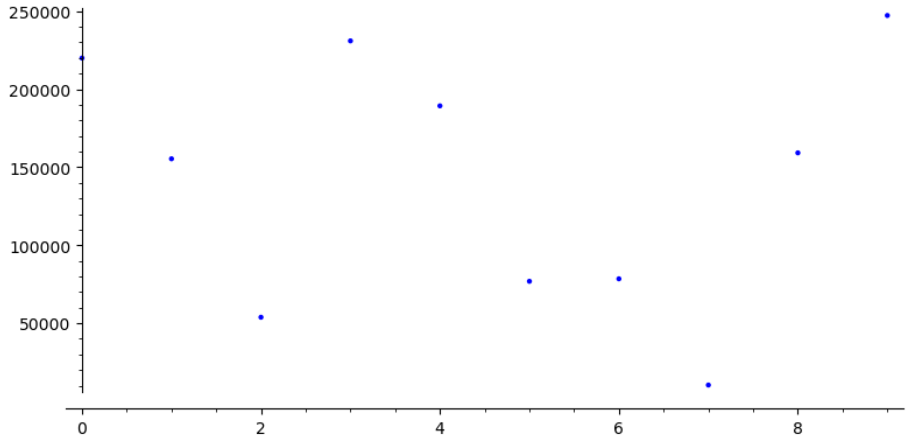
$$[(4,4),(3,4),(3,5),(4,5),(3,6),(2,5),(2,6),(4,6),(3,7),(2,4)]$$

And we can use '$G.is\_isomorphic(F)$' to confirm that this graph is isomorphic to $FFM(13,3)$. But we actually didn't even need that, since McKay has confirmed there exists a unique Ramsey graph on 13 vertices for $R(3,5)$. Another search returned one after 74228 iterations.

This takes a bit longer to return a graph, so doing it 1000 times might be too much. Let's at least do 10 - which gives an average of 187850 with standard deviation 190089. What in the world? The plot of the number of iterations reveals why:

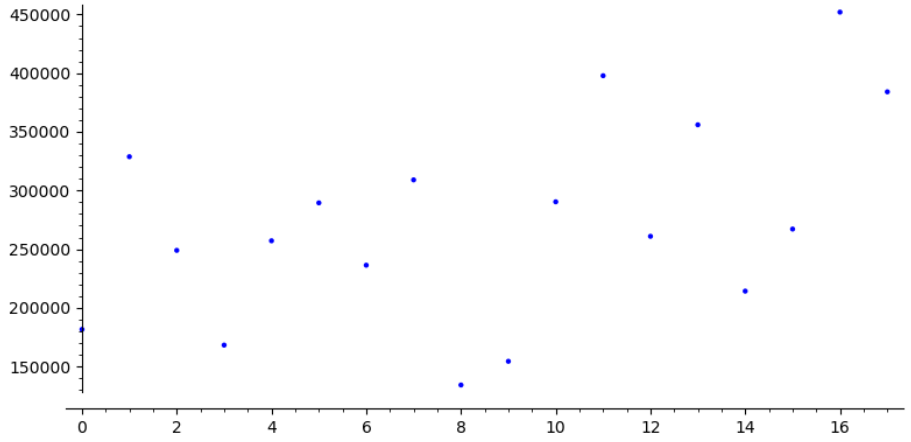


Running this again gives an average of 142153 with a standard deviation of 82406, and plot:



Averaging these gives 165000 iterations. But this is far too small to use the CLT. Generating 10 graphs seems to take about 8 minutes, so we'll do that 30 times, which means it will take around 4 hours!

So let's go ahead and generate a sample with 10 graphs still, but we'll take 30 samples. After four hours, I ran out of memory! But we did generate 18 values, giving an estimated population mean of 273939 and standard deviation of 87526. And here is a plot of the sample means.



$$[181634.1, 328795.2, 248980.7, 168252.9, 257147.8, 289458.2,$$
$$236347.2, 309039.5, 134261.1, 154436.8, 290360.5, 397805.1,$$
$$260961.4, 355983.4, 214247.6, 267138.6, 451991.5, 384073.1]$$

It seems like the standard deviation is so high here because of that fact that we only sampled 10 graphs instead of 1000. The first few took only 70-90 thousand,

while sometimes they take 685323 iterations and go through the following pairs (C, I):

$$[(4,5),(4,4),(3,4),(3,5),(3,6),(2,5),$$
$$(4,6),(2,6),(3,7),(2,7),(4,7),(2,4)]$$

I'm going to go ahead and let $RR(37,4,6)$ run for a bit! Nothing. Now I'll let $RR(36,4,6)$ go. We find no Ramsey graph but the (C, I) pairs we picked up, in order, are

$$[(7,8),(6,7),(6,6),(5,6),(5,5),(6,5),(5,7),(4,6),(4,7),(5,8),(4,8),(6,8),(7,6)]$$

And then it ran out of memory. I'm going to run it again and keep track of the number of iterations: at least . The pairs we got from this in order are:

$$[(6,7),(6,6),(6,5),(5,6),(5,5),(5,7),(4,6),(4,7),(5,8),(7,6),(4,8),(7,7),(6,8)]$$

It's also interesting how similar the two lists look. Though the second picked up $(7,7)$, which was missed the first time around. Still no $(3,5)$.

19.1 Flipped Perspective

Let's flip our perspective from finding bounds for $R(a,b)$ to fixing an n and finding pairs (a,b) for which $R(a,b) > n$. In particular, if we fix an a, then we have a unique smallest b such that $R(a,b) > n$. So let's define

$$R_n^{-1}(a) = min(\{b \mid R(a,b) > n\})$$

to be that minimum b. For example, fixing $n = 20$, we get

$$R_{20}^{-1}(2) = 21$$
$$R_{20}^{-1}(3) = 7$$
$$R_{20}^{-1}(4) = 5$$
$$R_{20}^{-1}(5) = 4$$
$$R_{20}^{-1}(6) = 4$$
$$R_{20}^{-1}(7) = 3$$
$$\vdots$$
$$R_{20}^{-1}(20) = 3$$
$$R_{20}^{-1}(21) = 2$$

Notice that for all n, $R_n^{-1}(a)$ stabilizes to the constant function 2 for $a > n$. Also we could say that $R_n^{-1}(1) = \infty$.

We know relatively few Ramsey numbers, so how many of these can we pin down? The lowest unknown number's bound is $35 < R(4,6) < 42$. This tells us that $R_{37}^{-1}(4)$ is either 5 or 6. Similarly, the values $R_n^{-1}(4)$ are unknown for $n = 38, 39, 40$, but we can definitely say $R_n^{-1}(4) = 6$ for all $n \geq 41$. Here is a table of values, with columns n and rows a, with an entry colored red if its value is unknown.

$n\backslash a$	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2
3	4	3	2	2	2	2	2	2	2	2	2	2	2	2	2
4	5	3	3	2	2	2	2	2	2	2	2	2	2	2	2
5	6	3	3	3	2	2	2	2	2	2	2	2	2	2	2
6	7	4	3	3	3	2	2	2	2	2	2	2	2	2	2
7	8	4	3	3	3	3	2	2	2	2	2	2	2	2	2
8	9	4	3	3	3	3	3	2	2	2	2	2	2	2	2
9	10	5	4	3	3	3	3	3	2	2	2	2	2	2	2
10	11	5	4	3	3	3	3	3	3	2	2	2	2	2	2
11	12	5	4	3	3	3	3	3	3	3	2	2	2	2	2
12	13	5	4	3	3	3	3	3	3	3	3	2	2	2	2
13	14	5	4	3	3	3	3	3	3	3	3	3	2	2	2
14	15	6	4	4	3	3	3	3	3	3	3	3	3	2	2
15	16	6	4	4	3	3	3	3	3	3	3	3	3	3	2
16	17	6	4	4	3	3	3	3	3	3	3	3	3	3	3
17	18	6	4	4	3	3	3	3	3	3	3	3	3	3	3
18	19	7	5	4	4	3	3	3	3	3	3	3	3	3	3
19	20	7	5	4	4	3	3	3	3	3	3	3	3	3	3
20	21	7	5	4	4	3	3	3	3	3	3	3	3	3	3
21	22	7	5	4	4	3	3	3	3	3	3	3	3	3	3
22	23	7	5	4	4	3	3	3	3	3	3	3	3	3	3
23	24	8	5	4	4	3	3	3	3	3	3	3	3	3	3
24	25	8	5	4	4	3	3	3	3	3	3	3	3	3	3
25	26	8	6	5	4	4	3	3							
26															
27															
28	29	9	6	5	4	4	4	3							
29															
30															
31															
32															
33															
34															
35															
36															
37															
38															
39															
40															

Fixing a column, we're looking at how big independent sets can get in a graph with an a-clique, as we increase the number of vertices. Fixing a row, we're looking at how big independent sets can get in a graph with n vertices, while we increase the size of the largest clique.

But another fun way to look at charted data is the diagonals and off-diagonals. In fact, the proof of Ramsey's Theorem for two colors is exactly by induction on $a + b$, which can be interpreted as inducting along the finite-length off-diagonals. We'll list the infinite-length diagonals first, and then do the off-diagonals. The first obvious diagonals are

$$R_n^{-1}(n+k) = 2 \quad for \quad k > 0$$

$$R_n^{-1}(n) = 3$$

Now let's look at $R_n^{-1}(n-k)$ for $k > 0$. This will always stabilize at 3, so we'll stop once we hit one 3.

k	diagonal sequence
1	4,3
2	5,3
3	6,4,3
4	7,4,3
5	8,4,4,3
6	9,5,4,3
7	10,5,4,3
8	11,5,4,3
9	12,5,4,4,3
10	13,5,4,4,3
11	14,6,4,4,3
12	15,6,4,4,4,3
13	16,6,4,4,4,3

To prove it really does stabilize, we can appeal to pretty much any lower bound on the off-diagonal Ramsey numbers (for a good bound, see this blog post by Qiaochu Yuan) to see that $R(n-k, 3) > n$ implies $R(n+1-k, 3) > n+1$.

The following table consists of the finite off-diagonals $R_n^{-1}(k-n)$ for $n = 2, \ldots, k-2$.

k	off-diagonal sequence
4	3
5	4,2
6	5,3,2
7	6,3,2,2
8	7,3,3,2,2
9	8,4,3,2,2,2
10	9,4,3,3,2,2,2
11	10,4,3,3,2,2,2,2
12	11,5,3,3,3,2,2,2,2
13	12,5,4,3,3,2,2,2,2,2
14	13,5,4,3,3,3,2,2,2,2,2
15	14,5,4,3,3,3,2,2,2,2,2,2
16	15,5,4,3,3,3,2,2,2,2,2,2
17	16,6,4,3,3,3,3,2,2,2,2,2,2,2

Some things we could look at:

- Lengths of each sequence and ratios of lengths/sums of consecutive sequences
- Sums and averages of each sequence
- Lengths of arithmetic progressions in sequence of sums

For the off-diagonals, their lengths are clearly just k. But the truncated diagonals seem to not be so regular. We could also consider the off-diagonal truncated at the first 2.

Lengths of Truncated Diagonals

$$2, 2, 3, 3, 4, 4, 4, 4, 5, 5, 5, 6, 6$$

Lengths of Truncated Off-Diagonals

$$1, 2, 3, 3, 4, 4, 5, 5, 6, 6, 7, 7, 7, 8$$

Sums of Truncated Diagonals

k	1	2	3	4	5	6	7	8	9	10	11	12	13
	7	8	13	14	19	21	22	23	28	29	31		

Sums of Off-Diagonals

k	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	3	6	10	13	17	21	25	28	33	37	41	44	45	52

Sums of Truncated Off-Diagonals

k	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	3	6	10	11	15	17	21	22	27	29	33	34	35	40

The first sequence is found in 5 OEIS entries, so we'll have to calculate it further. The second sequence gives 3 OEIS entries. The last three are not in the OEIS but subsequences give various interesting possibilities.

20 Infinite Ramsey Numbers

A fun generalization of Ramsey's Theorem is extending it to infinite sets. Specifically, it tells us that if we have an infinite set X and we color the set of n-element subsets $X^{(n)}$ with c colors, then there exists an infinite subset M so that $M^{(n)}$ is monochromatic. The infinite version implies the finite version, but the infinite version is "stronger" in a set-theoretic sense.

A well-known theorem in this area is the already-mentioned Van der Waerden's theorem, which says that for all positive integers r, k, there is some number N so that any coloring of $\{1, \ldots, N\}$ with r colors contains a monochromatic arithmetic progression of length k. A way to interpret this for the infinite version is that any coloring of the positive integers with r colors contains arbitrarily long monochromatic arithmetic progressions.

Another result in this area is Hindman's Theorem, which says that any coloring of the positive integers with r colors gives an infinite subset A so that there is a color i for which the finite sum of one or more elements of A is always i. Leo Goldmakher gives a wonderful exposition on the proof of this via ultra-filters, which are topology-type collections of subsets for a given set X.

Some introductions to this subject take a graph-theoretic point of view, while some are more set-theoretic with ultra-filters and cardinals and all that fun stuff. I can't quite find it now, but I think I remember reading a result that we can even find such an M with the same cardinality of X. I guess this would follow from the countable union of countable sets being countable.

But I have a question that I haven't seen people touch on, possibly because it's easy? We'll see! We'll call the subset $M \subset X$ a *Ramsey Set* for our coloring.

Question 5 *Given a Ramsey set $M \subset X$, what is the relative density of M?*

And now that I wrote it, it really is easy. Given any subset $M \subset X$ with the desired density, we could choose the indicator function for M to be the coloring of X, which grants $M_c = M$ with whatever density we want.

There are various applications of this infinite Ramsey theory in analysis, and of course in number theory. The natural way to try to apply the theorem is to deduce a coloring c that guarantees the set M_c is the one we're interested in. More generally, we could show that no matter what M_c is, the infinite size of this set implies the infinite size of the set we're interested in.

An example of this is Fred Galvin's corollary to Hindman's Theorem that say that there exists an infinite subset A of integers so that any finite sum is

divisible by an odd number of prime factors. We color $\mathbb{Z}$ with a parity function, but not the parity of n, we color n with the parity of $\omega(n)$. Then Hindman's Theorem tells us we have an infinite subset A so that any finite sum of elements of A have the same parity of prime factors. If $c(A) = 1$, then we're done.

If $c(A) = 0$, and we have some prime p that divides no element of A, then letting $pA = \{pa \mid a \in A\}$, we have $pa_1 + \cdots + pa_t = p(a_1 + \cdots + a_t)$, so $c(2A) = 1$. To guarantee such a prime, instead of coloring $\mathbb{Z}$, we can color the subset $\{pn + 1\}$ for all $n \in \mathbb{Z}$. Then we can be sure that $c(A) = 0$ implies $c(pA) = 1$.

That last paragraph is the key! No matter what infinite set we got, it implied there was a subset where the sums have an odd number of prime factors, because of a clever choice of what set to color. Does a simple replacement of $\omega(n)$ above with some other arithmetic function tell us anything interesting?

And I just realized that wasn't actually Galvin's corollary. We proved that there exists an infinite $A \subset \mathbb{Z}$ so that any finite sum has an odd number of distinct prime factors. Galvin's corollary was that any finite sum has an odd number of prime factors, i.e. looking at the parity of $\Omega(n)$. Then if $c(A) = 0$, we easily have $c(2A) = 1$. What if we replaced $\omega(n)$ or $\Omega(n)$ with another arithmetic function $f(n)$, and we chose a coloring defined by the parity of $f(n)$?

Another cool generalization of this comes from looking at $\mathbb{N}$ as a semigroup, which is a group minus the requirement of inverses. The study of semigroups is a very rich area of research, and is a area close to my heart! I spent a while studying certain classes of semigroups arising from number fields with a friend while I was in grad school. Now that I'm reminded of this work, I see a few connections to the things we already discussed.

But first, back to the topic, this paper Hindman's Coloring Theorem in Arbitrary Semigroups by Golan and Tsaban extends the theorem to arbitrary semigroups using a classification by Shevrin of semigroups in ***On the theory of periodic semigroups (1974)***. This classification is something I definitely want to dig deeper into in!

The paper notes a result already known is that if we color the elements of a numerical semigroup with finite colors, then we can find distinct elements $a_1, a_2, \ldots$ such that all but finitely many finite subsets have sum $a_1 + \cdots + a_t$ colored the same color. Golan and Tsaban give a characterization of when we can actually find a *subsemigroup* $T \subset S$ so that all but finitely many members of T are the same color. This is true even for non-abelian semigroups but I like the additive notation since we're talking here mostly about abelian semigroups.

21 To Semigroups

Studying semigroups appeared for me in two ways. The first was the "chicken nugget problem", which asks the question: *If McDonald's sells a 6-pack, a 9-pack, and a 20-pack of McNuggets, then what is the largest number of nuggets we cannot form as some combination of these?*. The second was after I knew a lot more math and worked with a good friend on numerical semigroups when I

went to the University of Michigan for grad school for a few years before leaving. Really, this is a sneaky way to talk about ideals! Recall that a subset $I \subset R$ of a ring R is called an ideal if

$$I \text{ is a subgroup of } R$$

$$\text{For all } r \in R, \text{ we have } rI \subset I.$$

My original Abstract Algebra professor (and later my research mentor) Cassie Williams described ideals as sponges, and the analogy has always stuck.

The ideals of $\mathbb{Z}$ are well understood - $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$ - and the study of ideals of other rings is essentially the basis of algebraic number theory! For example, the class group (the size of which is the class number) of a number field K is a group of ideals that encodes unique factorization in the ring of integers of K. Many of the results we've already dicussed come from such things.

An ideal P is called prime if $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$. Compare this to divisiblity of a prime number in $\mathbb{N}$. The collection of all prime ideals of a ring R is called *the spectrum of* R. We can look at the spectrum of a ring combinatorially by considering the poset their collection forms, ordered by inclusion.

We're often interested in maximal ideals in this poset, and if a ring R has a unique maximal ideal $\mathfrak{m}$, then it is called a *local ring*. As a big topic in Number Theory is the *Local-Global Principle* (also called the *Hasse Principle*), the study of local rings is helpful for studying local properties of different objects.

The spectrum of $\mathbb{Z}$ is the zero ideal and a maximal ideal for each prime p.

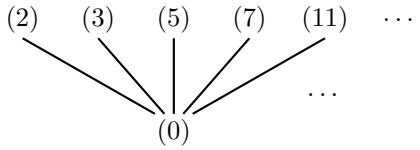


Figure 35: The spectrum of $\mathbb{Z}$

To characterize ideals in $\mathbb{N}$, we use similar reasoning to showing that all ideals in $\mathbb{Z}$ are principal (= generated by 1 element). The way that goes is by considering the ideal generated by $a, b \in \mathbb{Z}$. Then by Euclid's algorithm, there exists integers x, y so that $ax + by = gcd(a, b)$. It follows that every element in (a, b) is a multiple of $gcd(a, b)$, so $(a, b) = (gcd(a, b))$.

For $\mathbb{N}$, ideals are clearly not all principle. For example, the maximal ideal is $(2, 3) = \{0, 2, 3, 4, \dots\}$. In general, if we have a finite subset $A \subset \mathbb{N}$, we can generate an ideal from A and as Euclid's algorithm uses negative numbers, we'll in general get different ideals for different A.

Notice that the complement $(2, 3) = \{1\}^c$. A few more examples are

$$(3, 4, 5) = \{1, 2\}^c$$

$$(2,5) = \{1,3\}^c$$
$$(4,5,6,7) = \{1,2,3\}^c$$

An ideal of $\mathbb{N}$ with finite complement is called a *numerical semigroup*. The ideals of $\mathbb{N}$ can then be characterized as follows:

- Principal ideals with infinite complement.
- Numerical Semigroups

And we can characterize exactly when we generate a numerical semigroup from examining Euclid's Algorithm.

Theorem 29 *The set $A = \{a_1, \dots, a_t\}$ generates a numerical semigroup if and only if $gcd(a_1, \dots, a_t) = 1$*

Proof 9 *The forward direction is easy by contrapositive: If $g = gcd(a_1, \dots, a_t) \neq 1$, then $A \subset g\mathbb{Z}$, so its complement is infinite. The backward direction appeals to Schur's Theorem, which gives asymptotics for the number of ways to represent a number x as a linear combination of elements of A, given $g = 1$. Letting $r_A(x)$ be this number, then*

$$r_A(x) \sim \frac{x^{t-1}}{(t-1)!a_1 \dots a_t}(1 + o(1))$$

Which shows that there exists $z \in \mathbb{N}$ so that $r_A(x) \geq 1$ for all $x \geq z$.

Proof 10 (Proof of Schur's Theorem) *I want to detail this proof here just for completeness! This proof is found on page 98 of Generatingfunctionology by Herbert Wilf.*

First, notice that if $x = b_1a_1 + \dots + b_ta_t$, then we have a partition of x. In fact, we could consider it as

$$x = \underbrace{a_1 + \dots + a_1}_{b_1 \text{ copies}} + \underbrace{a_2 + \dots + a_2}_{b_2 \text{ copies}} + \dots + \underbrace{a_t + \dots + a_t}_{b_t \text{ copies}}$$

and notice that x is a partition of arbitrary length with parts in A. To count the number of partitions with parts in A, we modify the usual partition generating function by only multiplying over those $a \in A$.

$$\prod_{i=1}^{t} \frac{1}{1-q^{a_i}} = \prod_{i=1}^{t}(1+q^{a_i}+q^{2a_i}+\dots) = \sum_{x=0}^{\infty} |\{\text{partitions of } x \text{ with parts in } A\}|q^x$$

But that coefficient is exactly $r_A(x)$, so we've found our generating function

$$\sum_{x=0}^{\infty} r_A(x)q^x = \prod_{i=1}^{t} \frac{1}{1-q^{a_i}}$$

By partial fractions and the fact that each a_i are distinct, we can find C_i so that

$$\prod_{i=1}^{t} \frac{1}{1-q^{a_i}} = \sum_{i=1}^{t} \frac{C_i}{1-q^{a_i}}$$

But we go even further, and decompose it over $\mathbb{C}$, as linear functions with roots the a_i^{th} roots of unity. The contribution of a pole of order r to the total sum is αx^{r-1} for some constant α, since

$$\frac{1}{(1-q)^r} = \sum_{k=0}^{\infty} \binom{k+r}{r},$$

and the binomial coefficient is an $(r-1)^{st}$ degree polynomial over $(r-1)!$, so asymptotically $x^{t-1}/(t-1)!$.

As $gcd(A) = 1$, the orders of the poles at these non-1 roots of unity are less than t. The pole at $q = 1$ has order t, so gives contribution $x^{t-1}/(t-1)!$, which is asymptotically larger than the contribution of any other roots. Therefore,

$$r_A(x) \sim \alpha \left(\frac{x^{t-1}}{(t-1)!} \right)$$

To figure out the value of α, we look at

$$\lim_{q \to 1} \left[(1-q)^t \prod_{i=1}^{t} \frac{1}{1-q^{a_i}} \right] = \frac{1}{a_1 \dots a_t}$$

through repeated applications of L'Hospital's Rule. Therefore,

$$r_A(x) \sim \frac{x^{t-1}}{(t-1)! a_1 \dots a_t}$$

I want to remind you of the comment I made back at the beginning of section 19 on the connectivity of Random Ramsey Graphs. The statements of Theorem 28 and the previous theorem are equivalent. Both are saying that we have to eventually connect if the generators are relatively prime. In the case of numerical semigroups, this guarantees a finite complement.

Which means we have a numerical invariant we can assign to the ideals of $\mathbb{N}$, the cardinality of their complement. This is called the *genus* of the numerical semigroup, and the largest element of the complement is called the *Frobenius number*. Going back to the Chicken Nugget Problem, the answer comes down to determining the Frobenius number of the numerical semigroup generated by $(6, 9, 20)$, which is equal to 43.

One fun direction to go here is in counting numerical semigroups of a fixed genus, for which this paper by Nathan Kaplan is a good reference. A wonderful result here (due to Bras-Amoros) is that the number of numerical semigroups of genus g has Fibonacci-type asymptotic growth!

But continuing on, we've shown that any set A with $gcd(A) = 1$ will generate a numerical semigroup S and in the other direction, we get that any numerical semigroup has some set of generators, and therefore has a minimal set of generators. The size of this minimal set is called the *embedding dimension* of the semigroup and the smallest element is called the *multiplicity*. If you haven't guessed, there is a geometric point of view going on inspiring the study of these semigroups!

Now that we've figured out what the ideals of $\mathbb{N}$ look like, do we get any new prime ideals? Well, the maximal ideal $(2, 3)$ is prime (since it's maximal). Given any other numerical semigroup S, we have a Frobenius number $F(S)$, which is the largest integer not contained in S. So $F(S)^2 \in S$, while $F(S) \notin S$. So S cannot be prime. So the spectrum of $\mathbb{N}$ adds just a single unique maximal ideal.

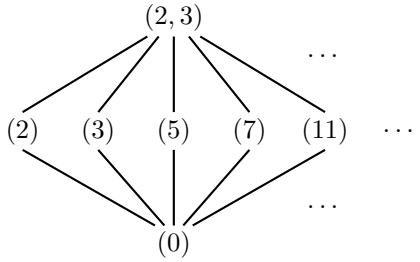


Figure 36: The spectrum of $\mathbb{N}$

The friend I previously mentioned is **Trevor Hyde**. A lot of the following perspective is from him, and I am incredibly thankful for it. There is a lot of algebraic geometry I don't feel I could explain well enough, so I'll skip a lot of that.

We can think of the spectrum of a ring as a topological space when equipped with the ***Zariski Topology***, but we can also think of it as a functor from the *category of rings* to the category of *locally ringed spaces*. One of the things I love is when something we learn in a class "long ago" reappears to give a cool new fact.

In this case, recall a fact proved in a first or second Abstract Algebra course: If $\phi : R \to S$ is a ring homomorphism, then the preimage of a prime ideal is a prime ideal. If $P \subset R$ is a prime ideal, then we want to show $\phi^{-1}(P) \subset R$ is too. So suppose $ab \in \phi^{-1}(P)$. Then $\phi(ab) \in P$, and since ϕ is a ring homomorphism, $\phi(ab) = \phi(a)\phi(b)$. Since $\phi(a)\phi(b) \in P$, we know one of the two must be in P, so WLOG, let $\phi(a) \in P$. Then $a \in \phi^{-1}(P)$, so $\phi^{-1}(P)$ is prime.

This "pulling-back" idea is very common, as it's a helpful way to get information about desired spaces. For the categorical perspective, the previous fact shows that any map $\phi : R \to S$ induces a map $\phi^* : Spec(S) \to Spec(R)$, given by $\phi^*(P) = \phi^{-1}(P)$. Because the sets swap, this is a contravariant functor.

Considered as semirings, the inclusion $\mathbb{N} \hookrightarrow \mathbb{Z}$ induces an injection $Spec(\mathbb{Z}) \to Spec(\mathbb{N})$. But the pre-image of our new prime $(2,3)$ is empty under this map, which means $Spec(\mathbb{Z})$ can't "see it", so to speak. This lead us to hope that studying semirings might reveal important properties of algebraic structures that we can't get from rings.

Maybe I'll get more into it later, but I do want to return to the coloring stuff. So here is a summary of some of the results we found. I'm not claiming any of these as original, and many of these ideas can probably be found in literature on the study of semigroups/semirings/semifields. And of course, I'll see if the coloring perspective of Hindman's theorem could give any insights to these results/questions.

1. The *prime fields* are $\mathbb{Q}$ and $\mathbb{F}_p$, since every field has one of these two as subfields. The *prime semifields* are $\mathbb{F}_p, \mathbb{Q}^+$, and one extra semifield called $\mathbb{B} = \{0,1\}$, the *Boolean semiring*, with $1+1=1$. This is the first example of a semiring with an infinity element ∞. But there are many more examples!

2. Define an additive version of ideals and quotients for semirings, and extend the study of Orders of rings and rings of integers to semirings inside extensions of the semifield $\mathbb{Q}^+$.

3. Calling a *totally positive* extension of $\mathbb{Q}^+$ an *arithmetic semifield* K, we can show that it has a unique maximal ideal $M(K)$. Letting U_K be the semigroup of units in K, then we can explicitly say
$$M(K) = \mathcal{O}_K^+ - U_K$$

4. Defining the *ring of totally positive integers* $\mathcal{O}_K^+$ analogously, the spectrum $Spec(\mathcal{O}_K^+)$ is the cone of $Spec(\mathcal{O}_K)$ with added point $M(K)$.

5. With the additive version of quotients mentioned above, we can show
$$\mathcal{O}_K^+/(M(K) - \{0\}) \cong \overline{U}_K,$$
where $\overline{U}_K$ is called the ***small semiring***, defined set-wise as $U_K \cup \{0, \infty\}$. As a semiring, we define multiplication of units as normal, and define
$$0\infty = 0 \quad \textit{and} \quad u_1 + u_2 = \infty, \ \forall u_i \in U_K$$
We can think of this as (1) 0 kills everything, (2) multiplication of units stays bounded, (3) addition of units is unbounded. Doing an example with the classic semiring: $\mathbb{N}$. We have $M(\mathbb{Q}^+) = (2,3) = \{0,2,3,4,\dots\}$ so
$$\mathbb{N}/\overline{(2,3)} = \{0,1,\infty\}.$$

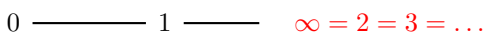


Figure 37: The quotient $\mathbb{N}/\overline{(2,3)}$

6. This point I consider important, so I'm separating it from the previous. Removing additive inverses is exactly what allows this infinity element to exist in semirings! And the addition of this naturally allows for the study of the infinite/archimedean place. This again is near and dear to my heart because one of my first research projects was on evaluating a product formula over the places of $\mathbb{Q}$, and relating it to a ratio of class numbers. The archimedean place had to be dealt with in a fairly different way than the finite places.

7. Finally, we can establish a bijection between numerical semigroups in $\mathbb{N}$ and partitions using hooklengths. A good source on this is this paper by Keith and Nath. This gives an example of when the symmetric difference is helpful, as the generating function

$$D_A(x) = \frac{1}{2} + \frac{1}{2} \sum_{n \in A \Delta (1+A)} x^n$$

determines the partition that corresponds to a given *set of gaps* A (meaning A^c is a numerical semigroup). This generating function can be defined as a ***Hilbert Series***, as detailed in this wonderful paper Numerical Semigroups: Apery Sets and Hilbert Series by Ramirez Alfonsin and Rodseth. We relate this to the additive version of ideals and to the size of their minimal generating set.

8. The previous example shows that numerical semigroups in $\mathbb{N}$ can be thought of as a smooth curve cutting the plane in half, with particular importance of the additive ideals. Then looking at numerical subsemigroups of $\mathcal{O}_K^+$ could (perhaps) be thought of as generalized plane partitions.

22 Back to Hindman (or Distracted by $N(g) \geq N(g-1)$)

That was a very fun reminder! I'd love to see whether Hindman's coloring theorem gives us any insights on semigroups or semirings. In fact, I wonder if a version of Hindman's theorem for semirings is proven? I can't seem to find anything about work on a version for rings, so I'm not sure. One version of this I'd like to investigate is

Question 6 *If we color the elements of a ring R with a finite amount of colors, does there exist an infinite subset $M \subset R$ so that the sum of any finite subset of M is monochromatic and the product of any finite subset of M is monochromatic, with a finite number of exceptions?*

Before thinking about that, does the theorem say anything about numerical semigroups in particular? Shevrin's characterization of semigroups relies on two notions. A semigroup is called *periodic* if the subsemigroup (s) generated by

any $s \in S$ is finite. A semigroup S is called *left (right) zero* if $ab = a$ ($ab = b$) for all $a, b \in S$. The characterization is given as follows:

Theorem 30 (Shevrin) *Every infinite semigroup has a subsemigroup of the following type:*

1. $(\mathbb{N}, +)$
2. *An infinite periodic group*
3. *An infinite right zero or left zero semigroup*
4. $(\mathbb{N},)$, *where* $nm = max(n, m)$.
5. $(\mathbb{N},)$, *where* $nm = max(n, m)$.
6. *An infinite semigroup* S *with* S^2 *finite.*
7. *The fan semilattice* $(\mathbb{N},)$, *where* $nm = 1$ *for distinct* n, m.

Restricting our focus back to numerical semigroups, there is another property that I'm interested in that I haven't seen looked at in the literature. For a numerical semigroup S, let $\pi(S)$ denote the number of gaps that are prime. In other words, $\pi(S)$ counts the number of primes not represented by $a_1x_1 + \cdots + a_tx_t$, for $A = \{a_i\}$ a generating set for S. We'll sort by genus.

S^c	$g(S)$	$\pi(S)$
$\{1\}$	1	0
$\{1, 2\}$	2	1
$\{1, 3\}$	2	1
$\{1, 2, 3\}$	3	2
$\{1, 2, 4\}$	3	1
$\{1, 2, 5\}$	3	2
$\{1, 3, 5\}$	3	2
$\{1, 2, 3, 4\}$	4	2
$\{1, 2, 3, 5\}$	4	3
$\{1, 2, 3, 6\}$	4	2
$\{1, 2, 3, 7\}$	4	3
$\{1, 3, 4, 5\}$	4	2
$\{1, 3, 4, 6\}$	4	1
$\{1, 3, 5, 7\}$	4	3

Looking up partial sequences on OEIS of $\pi(S)$ return some interesting entries, but by $[0, 1, 1, 2, 1, 2, 2, 2, 3, 2, 3, 2]$, it returns nothing. And here is a table for the average of $\pi(S)$ over all numerical semigroups of genus g.

g	1	2	3	4	5	6	7
$avg(\pi, g)$	0	1	7/4	16/7	11/4		

If $S \subset T$, then $T^c \subset S^c$, so

$$S \subseteq T \Longrightarrow \pi(T) \leq \pi(S)$$

It's helpful to be more explicit and write

$$avg(\pi, g) = \frac{1}{N(g)} \sum_{|S|=g} \pi(S)$$

As mentioned before, it has been shown that $N(g)$ has Fibonacci-type growth. Specifically, Zhai (an undergraduate!) proved parts 2 and 3 of a conjecture of Bras-Amoros that said

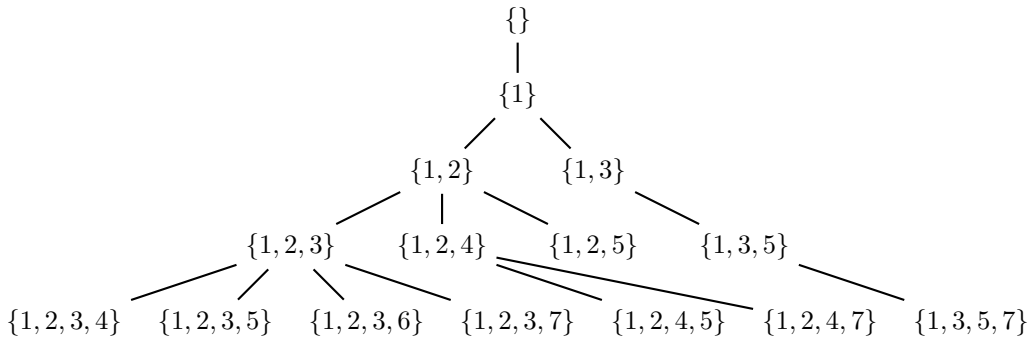
1. $N(g) \geq N(g-1) + N(g-2)$ for $g \geq 2$.
2. $\lim_{g\to\infty} \frac{N(g-1)+N(g-2)}{N(g)} = 1$
3. $\lim_{g\to\infty} \frac{N(g)}{N(g-1)} = \phi = 1.618\ldots.$

The previously mentioned paper by Nathan Kaplan on counting numerical subgroups by genus has a nice outline of Zhai's proof as well as a wealth of other information of numerical semigroups. One thing he notes is that the first part of the conjecture is still completely open. In fact, even the conjecture that the number of semigroups of genus g is *increasing in* g is not proven! That is, no one can prove

$$N(g) \geq N(g-1).$$

Go ahead, give it a shot! A natural attempt would be to find some way to map the set of numerical semigroups of genus $g-1$ to the set of genus g. This is very difficult once you start trying. For example, it's not hard to notice that if S is a numerical semigroup of genus g, then $F(S) = max(S^c)$ can't be written as a combination of elements in S, so $S \cup \{F(S)\}$ is a numerical semigroup of genus $g-1$.

This leads to the idea of the numerical semigroup tree. That paper has a wonderful graphic of the tree up to layer 4 on page 3, but I'll post one here in terms of the set of gaps instead of the generating set.



We form the tree by starting with a numerical semigroup, and continually adding Frobenius numbers until our semigroup is just $\mathbb{N}$. We do this for every semigroup we have.

But this isn't usually how we define rooted trees - what if we wanted a description starting from the root $\mathbb{N}$? Then we need to ask how many S' of genus $g-1$ are of the form $S' = S \cup \{F(S)\}$ for some S of genus g. If we remove an element of $x \in S'$ and $x = s_1 + s_2$, for some $s_1, s_2 \in S'$, then this new set couldn't be a numerical semigroup. If that doesn't happen, then it is. We call an element x *irreducible* if it cannot be written as the sum of two elements in S. Then for $x > F(S')$,

$$S' - \{x\} \textit{ is a numerical semigroup } \Leftrightarrow x \textit{ is irreducible}$$

If x is irreducible, then it must be a generator of S'. Letting $Irr(S')$ be the set of all irreducible elements of S', we see that this must be a minimal generating set. Then the elements we're allowed to remove are exactly those elements in $Irr(S')$ that are bigger than $F(S')$. We call these *effective generators*, and denote the number of them as $h(S')$, the *efficacy* of S'. For example,

- All generators of an *ordinary numerical semigroup* $\{0, g+1, g+2, \dots\}$ are effective.
- The numerical semigroup $(2,5) = \{0, 2, 4, 5, 6, 7, \dots\} = \{1,3\}^c$ has one effective generator, 5, while 2 is not effective since $2 < 3$.
- The numerical semigroup $(3,5) = \{0, 3, 5, 6, 8, 9, 10, \dots\} = \{1, 2, 4, 7\}^c$ has no effective generators since both generators of $(3,5)$ are less than 7.

So starting at a vertex S, its children are $S - \{x\}$ for all effective generators x of S. Which means the number of children of S is $h(S)$. So by analyzing effective generators and getting some hold on $h(S)$, Zhai was able to prove the conjectures about the growth of the tree. Previous work by Bras-Amoros, for example, showed that the semigroup tree below the ordinary semigroup $\{0, g+1, g+2, \dots\}^c$ has a subtree with $2F_g$ nodes at level g, where F_g is a Fibonacci number.

In general, letting $t(g,h)$ be the number of numerical semigroups of genus g with h effective generators, we have that

$$N(g) = \sum_h t(g-1,h)h$$

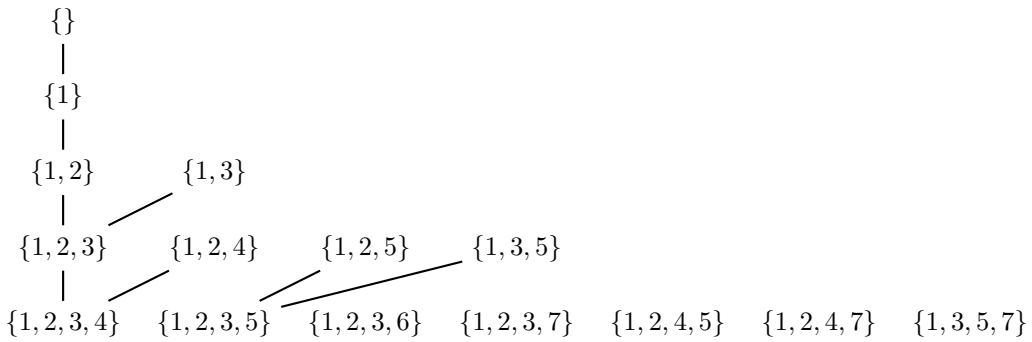
so we can explain the possible failure of $N(g) \geq N(g-1)$ with the fact that there are too many numerical semigroups of genus $g-1$ with no effective generators.

In fact, though initially it may seem like we have lots of choices to remove, a consequence of a theorem of Evan O'Dorney's on the growth of $t(g,h)$ tells us that asymptotically, the probability of a numerical semigroup having no children is $\phi^{-2} \approx 0.382$.

22.1 Ordinarization

Another map we could look at is removing the multiplicity $m(S) = min(S - \{0\})$ from a set S. This increases genus, and we can ask like before when some S' of genus $g+1$ is of the form $S' = S - \{m(S)\}$? Instead of every vertex ending at $\mathbb{N}$, which gave a nice tree structure, this operation returns a single numerical semigroup of genus $g+1$ for each of genus g. But this map isn't injective.

If we just start with $\mathbb{N}$, then we just get a sequence of ordinary numerical semigroups. So we'll form a graph by forming such sequences with each known numerical semigroup and gluing them together.



Maria Bras-Amoros combined the two previous transformations of numerical semigroups and called it the Ordinarization Transform. Sending S to $S \cup \{F(S)\} - \{m(S)\}$ gives a map from genus g to genus g which always stabilizes on the ordinary semigroup $(g+1, g+2, \ldots, 2g+1) = \{1, \ldots, g\}^c$. For example,

$$S = (3,5) = \{1,2,4,7\}^c.$$

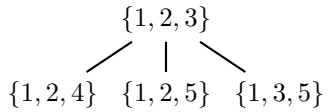
$$S' = (3,5) \cup \{7\} - \{3\} = \{1,2,3,4\}^c = (5,6,7,8,9).$$

Another example,

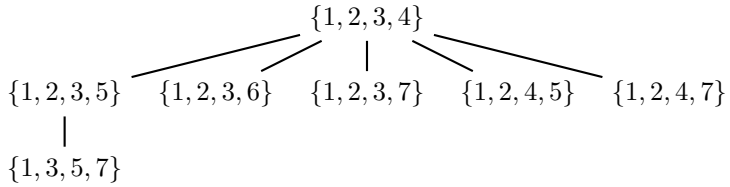
$$S = (2,9) = \{1,3,5,7\}^c$$

$$S' = (2,9) \cup \{7\} - \{2\} = \{1,2,3,5\}^c = (4,6,7,9)$$
$$S'' = (4,6,7,9) \cup \{5\} - \{4\} = \{1,2,3,4\}^c = (5,6,7,8,9)$$

Which means we can form a poset from the numerical semigroups of genus g. For $g = 3$, this looks like



And for $g = 4$, it looks like

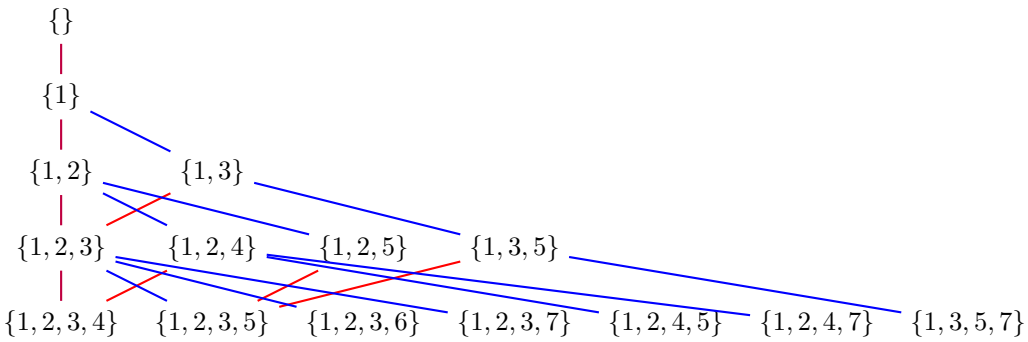


The *Ordinarization Number* of S, which we'll denote $ON(S)$, is its depth in this tree. Letting $N(g,r)$ be the number of numerical semigroups of genus g and ordinarization number r, Bras-Amoros conjectures that

$$N(g,r) \geq N(g-1,r).$$

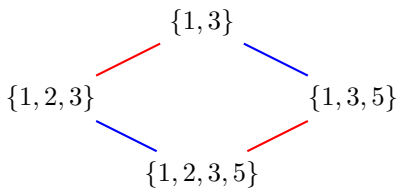
Since $N(g) = \sum_r N(g,r)$, this would imply the inequality $N(g) \geq N(g-1)$.

To try to visualize this, I want to combine the two trees we had before, coloring an edge blue if it comes from adding $F(S)$ and coloring it red if it comes from removing $m(S)$, and purple if it's both.

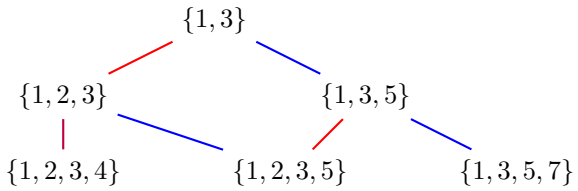


The only purple edges will be those between ordinary semigroups, since S and S' having a red edge means $S' = S - \{m(S)\}$, and having a blue edge means $S = S' \cup \{F(S)\}$. So a purple edge means $m(S) = F(S) + 1$, so S is ordinary.

The ordinarization number of S in terms of this graph is half the length of the shortest path from S of genus g to the ordinary numerical subgroup of genus g. We can start with either blue or red edges. For example, starting with $S = \{1, 3, 5\}$, we see $ON(S) = 1$, since the shortest paths are



and $ON(\{1, 3, 5, 7\}^c) = 2$, given by these paths (and more)



Although the colors don't have to alternate, the fact that we end on the same level means the number of blue edges (up) must be equal to the number of red edges (down).

Looking at a few examples quickly leads you to the following theorem (proven in Bras-Amoros):

Theorem 31 *The maximum value of $ON(S)$ is $\lfloor g/2 \rfloor$, and the unique semigroup that achieves this is*

$$(2, 2g + 1) = \{1, 3, 5, \ldots, 2g - 1\}$$

It's easy to see the numerical semigroup $(2, 2g+1)$ will have a path of length g or $g - 1$ back to $\mathcal{O}_g$.

$$\{1, 3, 5, \ldots, 2g - 1\}^c \to \{1, 3, 5, \ldots, 2g - 3\}^c \to \{1, 2, 3, 5, \ldots, 2g - 3\}^c \to$$

$$\to \{1, 2, 3, 5, \ldots, 2g - 5\}^c \to \{1, 2, 3, 4, 5, 7, \ldots, 2g - 5\} \to \ldots$$

In general, counting paths of length r from u to v in a graph G can be done by looking at the (u, v) entry of A^r. To get a better handle on this, let's define some of what we're talking about more explicitly.

1. The *Ordinarization Graph* Γ is an edge-labeled graph whose vertex set is the set of numerical semigroups, with a blue edge between S and S' if $S' = S \cup \{F(S)\}$, a red edge if $S' = S - \{m(S)\}$, and a purple edge if both.

2. For some fixed g, let Γ_g be the subgraph spanned by numerical semigroups of genus g and $g-1$. Notice that if S is genus g, then we will always be able to recover $ON(S)$ by only looking at numerical semigroups of genus g and $g-1$, since we can remove the multiplicity first, and then add the Frobenius numbers.

We can picture Γ_g as a bipartite graph on $N(g)+N(g-1)$ vertices.

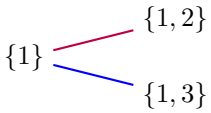


Figure 38: Γ_2

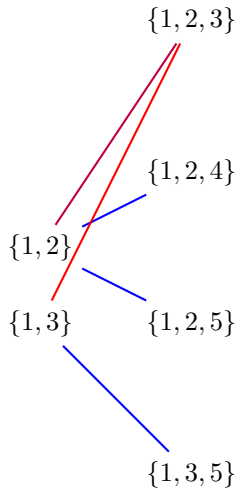


Figure 39: Γ_3

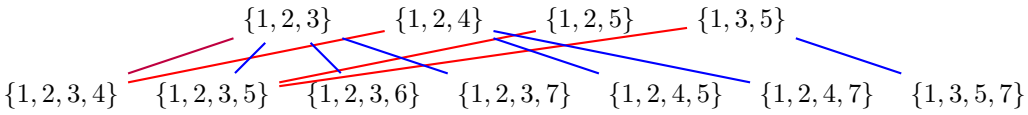


Figure 40: Γ_4

A wonderful memory from taking my first graduate combinatorics course was learning about Hall's Marriage Problem. This is a beautiful characterization of when a bipartite graph has a perfect matching, and has numerous applications to other areas.

First, a *perfect matching* M in a graph G is a choice of edges so that

1. No two edges in M are incident
2. Every vertex is adjacent to an edge in M.

Hall's theorem tells us that for a bipartite graph G with parts A and B,

$$G \text{ has a perfect matching} \iff \forall\, W \subset A,\ |N_G(W)| \geq |W|$$

where $N_G(W)$ is the set of vertices in B adjacent to a vertex in W.

More generally, we call a subset of edges a *matching* if it satisfies the first property, no two edges are incident. We call it a *maximal pairing* if it is maximal with respect to inclusion, and a *maximum pairing* if it has the largest number of edges possible.

So what is a matching of Γ_g, anyway? It's a collection of pairs $\{(S, S')\}$ so that S is genus $g-1$, S' is genus g, and

$$S' = S - \{m(S)\} \quad or \quad S = S' \cup \{F(S')\}$$

and no numerical semigroup appears in any ordered pair more than once.

A dual concept we can consider is a vertex cover, a subset $C \subset V$ so that every edge has at least one endpoint in C. We similarly call C *minimal* if it is minimal with respect to inclusion, and *minimum* if it has the least number of vertices possible.

A wonderful theorem of Koning tells us that for bipartite graphs, the size of a maximum matching is equal to the size of a minimum vertex cover! So we have a dual way of thinking of the above set: A collection of numerical semigroups $C = \{S\}$ of genus g and $g-1$ so that every other numerical semigroup S' of either genus can be written as either $S \cup \{F(S)\}$ or $S - \{m(S)\}$ for some $S \in C$. In this sense, I think it makes sense to look for a minimum such set!

Berge's lemma gives a nice characterization of maximum matchings in terms of paths in our graph. We first define an *augmenting path* with M to be one that starts and ends at unmatched vertices.

Lemma 2 *A matching M is maximum if and only if there is no augmenting path in G with M.*

Proof 11 *The proof uses a wonderful observation of the symmetric difference of two matchings. If M and M' are two matchings of G, let $G' = M \triangle M'$. Then G' consists of connected components of the form:*

1. *An isolated vertex*
2. *An even cycle with edges alternating between M and M'.*
3. *A path whose edges alternate between M and M', with different endpoints.*

Recall that $M \triangle M' = (M \cup M') - (M \cap M')$, so G' will consist of the edges that appear in M or M' but not both. As both sets are matchings, each vertex in G' can have at most 2 edges adjacent to it, one from M and one from M'. It will be isolated if those two edges are the same edge. Otherwise we have some path with edges alternating between M and M'. If this is a cycle, then since a vertex can't be adjacent to two edges in M, we must have an even number of vertices in the cycle.

Then we prove the contrapositive: If M is a matching of G that has an augmenting path, then M can be made larger. If P is our augmenting path, then P starts and ends at vertices that are not adjacent to any edge in M. So taking $P \triangle M$ will be a larger matching. A picture makes it clear.

The red edges are the ones in M and the fact that the two outside vertices are unmatched means the symmetric difference swaps the red with the blues, increasing the number of edges in the matching.

For the other direction, suppose M' has more edges than M. Then consider $M \triangle M'$. By the previous observation, this consists of connected components that are either isolated vertices, even alternating cycles, or alternating paths.

Since M' is larger than M, this is not empty. And further, there must be some component with more edges from M' than M. Such a component can't be an even cycle, so it must be an alternating path that starts and ends at M'. This is an augmenting path for M!

In Γ_g, every path is of the form $S_1, S_2, \ldots, S_t$ alternating between genus g and $g-1$. Given a maximal matching M of Γ_g, we know that any path will either start or end inside M. Remember why we started all this: The graph Γ_g encodes $ON(S)$ for numerical semigroups of genus both g and $g-1$ simultaneously. If we start with a genus g semigroup, then we begin with the operation of adding the Frobenius number. If we start with a genus $g-1$ semigroup, then we start with the operation of removing the multiplicity.

Letting $d(u,v)$ denote the minimum distance between two vertices in a graph, and letting $\mathcal{O}_g = \{0, g+1, g+2, \ldots\}^c$ be the ordinary semigroup of genus g, we have

$$ON(S) = \frac{1}{2} d(S, \mathcal{O}_g)$$

Then the set $\mathcal{C}_{g,r} = \{S \in \Gamma_g \mid ON(S) = r\}$ can be thought of like a circle centered at $\mathcal{O}_g$ of radius $2r$. Its size is the previously defined $N(g,r)$, for which Bras-Amoros conjectured that for all positive integers g, r,

$$N(g,r) \geq N(g-1,r)$$

So this is equivalent to showing that $|\mathcal{C}_{g,r}| \geq |\mathcal{C}_{g-1,r}|$.

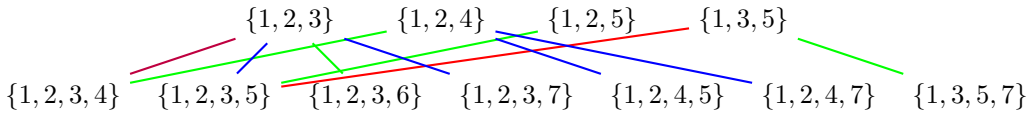


Figure 41: Maximum matching (green) in Γ_4

And let's go ahead and do Γ_5, why not.

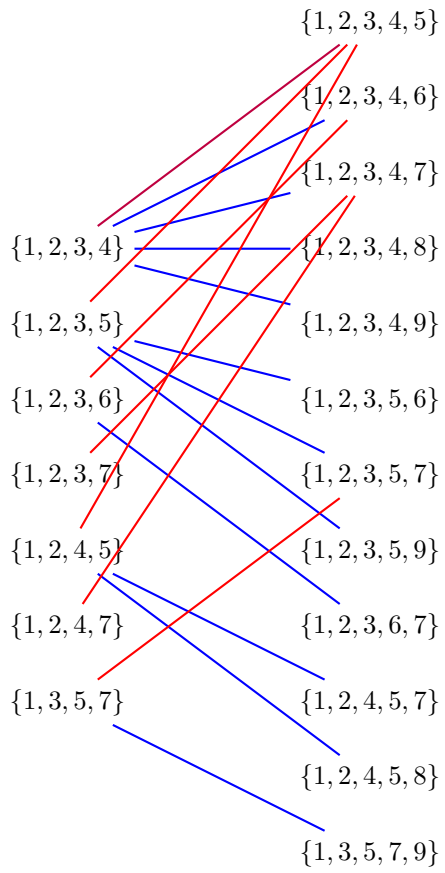


Figure 42: Γ_5

So what's the matching number for Γ_g? Recall the condition in Hall's Marriage problem: That for all $W \subset A$, we have $|N_G(W)| \geq |W|$. In general, for a bipartite graph $G = (A, B, E)$, we can define the *deficiency* of $W \subset A$ as

$$D(W) = \max(0, |W| - |N_G(W)|)$$

and define

$$D_A(G) = \max_{W \subset A} D(W)$$

Then Hall's Theorem is equivalent to saying that

$$D_A(G) = 0 \iff G \textit{ has a perfect matching}$$

And we can say something more generally about matchings and deficiency of subsets.

Proposition 6 *The matching number of G is equal to $|A| - D_A(G)$, which is also equal to $|B| - D_B(G)$.*

For Γ_g, this means

$$N(g-1) - D_{\mathcal{N}_{g-1}} = N(g) - D_{\mathcal{N}_g},$$

so

$$N(g) - N(g-1) = D_{\mathcal{N}_g} - D_{\mathcal{N}_{g-1})}$$

This gives us another way to interpret why $N(g) \geq N(g-1)$ might fail: If $\mathcal{N}_{g-1}$ is more deficient than $\mathcal{N}_g$. And we get the other direction. Altogether, we have

$$N(g) \geq N(g-1) \Longleftrightarrow D_{\mathcal{N}_g} \geq D_{\mathcal{N}_{g-1}}$$

So why might deficiency decrease? If $D_{\mathcal{N}_g} < D_{\mathcal{N}_{g-1}}$, then there exists $W \subset \mathcal{N}_{g-1}$ so that $D(W) > D(W')$ for all $W' \subset \mathcal{N}_g$.

This means $|W| - |N_G(W)| > |W'| - |N_G(W')|$ for all $W' \subset \mathcal{N}_g$. So we'd want W as big as possible while keeping $N_G(W)$ small. Remember that

$$N_G(W) = \{S \in \mathcal{N}_g \mid \exists S' \in W \text{ } st \text{ } S' = S - \{m(S)\} \text{ } or \text{ } S = S' \cup \{F(S')\}\}.$$

Exactly one will be $S' = S - \{m(S)\}$, so keeping $N_G(W)$ small means choosing a subset $W \subset \mathcal{N}_{g-1}$ so that very few $S \in \mathcal{N}_g$ have $S \cup \{F(S)\} \in W$.

For example, in Γ_5, we could choose $W = \{\{1,2,3,7\},\{1,2,4,7\}\}$ on the left and then $D(W) = 2 - 1 = 1$. But on the right, we could choose

$$\{\{1,2,3,4,8\},\{1,2,3,4,9\},\{1,2,3,5,6\},\{1,2,3,5,9\},\{1,2,4,5,7\},\{1,2,4,5,8\}\}$$

and get $D = 6 - 3 = 3$.

Remember an effective generator of S is a member of the minimal generating set that is larger than $F(S)$. The number of these is denoted $h(S)$. Effective generators x are exactly the ones for which $S - \{x\}$ is a numerical semigroup. And we write $t(g,h)$ for the number of numerical semigroups of genus g with h effective generators. We can then write

$$N(g) = \sum_h t(g-1,h)h.$$

From a dual point of view, we want to know how many $S \in \mathcal{N}_g$ are of the form $S = S' - \{m(S')\}$ for some $S' \in \mathcal{N}_{g-1}$. Well for $x \in S^c$, when do we have $S \cup \{x\}$ a numerical semigroup? If there is an $s \in S$ so that $s + x \in S^c$, then we run into a problem. Call a gap x *fragile* if $x \neq 1$ and for all $s \in S$, we have $x + s \in S$. Then

$$S \cup \{x\} \text{ } is \text{ } a \text{ } numerical \text{ } semigroup \text{ } of \text{ } genus \text{ } g-1 \Leftrightarrow x \text{ } is \text{ } fragile$$

Let's define $\overline{h}(S)$ to be the number of fragile gaps in S^c and $\overline{t}(g,\overline{h})$ to be the number of numerical semigroups of genus g with $\overline{h}(S) = \overline{h}$. Let's see how these two concepts interact.

Looking at complements, it makes $\overline{h}(S)$ very clear, it's the number of elements $x \in S^c$ so that $S^c - \{x\}$ is the complement of an earlier numerical semigroups. In general, S being a numerical semigroup means S^c satisfies the following property:

$$x \in S^c \Longrightarrow d \in S^c \; for \; all \; d|x$$

In other words, if S is a numerical semigroup, then S^c is closed under taking divisors. Call the gaps that are not divisors of any other gaps the *maximal gaps* of S.

Then it's immediate that $x \; fragile \implies x \; maximal \; gap$, since any non-maximal gap will have a multiple of itself as a gap. The converse is not necessarily true - For example, in $\{1, 2, 5\}^c$, the maximal divisors are 2 and 5, but 2 isn't fragile since $2 + 3 = 5$ is a gap.

23 A Fresh Start 2

Sometimes I get a bit overwhelmed with information and it's nice to start fresh and copy all the important bits discovered in the last section to the same spot. Throughout, S is a numerical semigroup of genus g and S' is a numerical semigroup of genus $g - 1$.

- **Definitions**

  1. An element x of S is *irreducible* if it cannot be written as $x = s_1 + s_2$ for two elements $s_1, s_2 \in S$.
  2. An element y of S^c is *fragile* if $y \neq 1$ and $s + y \in S$ for all $s \in S \cup \{y\}$.
  3. Given a minimum generating set A of S, the *effective generators* of S are the elements of A bigger than $F(S)$.
  4. The number of effective generators of S is denoted $h(S)$, and the number of numerical semigroups of genus g with h effective generators is denoted $t(g, h)$, so

  $$N(g) = \sum_h t(g-1, h)h$$

  5. The *removable gaps* are the fragile gaps of S that are smaller than $m(S)$.
  6. The number of removable gaps of S is denoted $\overline{h}(S)$, and the number of numerical semigroups of genus g with $\overline{h}$ removable gaps is denoted $\overline{t}(g, \overline{h})$, so

  $$N(g-1) = \sum_{\overline{h}} \overline{t}(g, \overline{h})\overline{h}$$

- **Consequences**

  1. $S - \{x\} \in \mathcal{N}_{g+1} \iff x$ is irreducible.

2. $S \cup \{x\} \in \mathcal{N}_{g-1} \iff x$ is a fragile gap.
3. $S' \in \mathcal{N}_{g-1}$ is of the form $S' = S \cup \{F(S)\} \iff S = S' - \{x\}$ for an effective generator x
4. $S \in \mathcal{N}_g$ is of the form $S = S' - \{m(S')\} \iff S' = S \cup \{x\}$ for a removable gap x.

- **Proofs**

1. $S - \{x\} \in \mathcal{N}_{g+1}$ means there does not exist $s_1, s_2 \in S$ so that $s_1 + s_2 = x$. So x irreducible. Other direction the same.
2. $S \cup \{x\} \in \mathcal{N}_{g-1}$ means $s + x \in S$ for all $s \in S \cup \{x\}$, so x is a fragile gap. Other direction the same
3. If $S' = S \cup \{F(S)\}$, then $F(S') < F(S)$, so whatever element x we removed from S' must have been bigger than $F(S)$, and therefore is an effective generator. In the other direction, if $S = S' - \{x\}$ for an effective generator x, then x is irreducible and $x > F(S')$, so $x = F(s)$.
4. If $S = S' - \{m(S')\}$, then $m(S) > m(S')$, so whatever element we add to S has to be less than $m(S)$, so it is a removable gap. In the other direction, if $S' = S \cup \{x\}$ for a removable gap, then x is fragile and $x > m(S)$, so $m(S') = x$.

Let's see what a few of these $N(g)$ decompositions look like. First, we'll collect a bunch of data.

S	(1)	$(2,3)$	$(3,4,5)$	$(2,5)$	$(4,5,6,7)$	$(3,5,7)$	$(3,4)$	$(2,7)$
S^c	$\{\}$	$\{1\}$	$\{1,2\}$	$\{1,3\}$	$\{1,2,3\}$	$\{1,2,4\}$	$\{1,2,5\}$	$\{1,3,5\}$
$h(S)$	1	2	3	1	4	2	0	1
$\overline{h}(S)$	0	0	1	0	2	0	0	0

S	$(5,6,7,8,9)$	$(4,6,7,9)$	$(4,5,7)$	$(4,5,6)$	$(3,7,8)$	$(3,5)$	$(2,9)$
S^c	$\{1,2,3,4\}$	$\{1,2,3,5\}$	$\{1,2,3,6\}$	$\{1,2,3,7\}$	$\{1,2,4,5\}$	$\{1,2,4,7\}$	$\{1,3,5,7\}$
$h(S)$	5	3	1	0	2	0	1
$\overline{h}(S)$	2	2	0	0	0	0	0

5	0	0	0	0	0	0	
4	0	0	0	0	0	0	
3	0	0	0	0	0	1	
2	0	0	0	1	2	1	
1	0	0	1	0	0	2	
0	1	1	1	3	5	8	
$\overline{h}$							
$\overline{t}(g,\overline{h})$							
g	0	1	2	3	4	5	6
$t(g,h)$							
h							
0	0	0	1	1	2		
1	1	0	1	1	2		
2	0	1	0	1	1		
3	0	0	1	0	1		
4	0	0	0	1	0		
5	0	0	0	0	1		

We'll format the sums like so, starting with $g = 1$.

$$\sum_h t(g-1,h)h = N(g) = \sum_{\overline{h}} \overline{t}(g+1,\overline{h})\overline{h}$$

$$\begin{aligned}
(0)0 + (1)1 &= 1 = (1)0 + (1)1 \\
(0)0 + (0)1 &= 2 = (3)0 + (2)1 \\
(1)0 + (1)1 + (0)2 + (1)3 &= 4 = (5)0 + (0)1 + (2)2 \\
(1)0 + (1)1 + (1)2 + (0)3 + (1)4 &= 7 = (8)0 + (2)1 + (1)2 + (1)3
\end{aligned}$$

This feels like a nice connection between $\mathcal{N}_{g-1}, \mathcal{N}_g$, and $\mathcal{N}_{g+1}$. For example, if $N(g) < N(g-1)$, then

$$\sum_{\overline{h}} \overline{t}(g+1,\overline{h})\overline{h} < \sum_h t(g,h)h,$$

And of course, h and $\overline{h}$ are just two placeholders for an integer n, so we can rewrite this as

$$\sum_n \overline{t}(g+1,n)n < \sum_n \overline{t}(g,n)n$$

$$\Updownarrow$$

$$\sum_n \left[\overline{t}(g+1,n) - \overline{t}(g,n)\right] n < 0$$

Note that $t(g-1,n)=0$ for $n \geq g$ since the ordinary semigroup $\mathcal{O}_{g-1} = (g,\ldots,2g-3)$ maximizes the number of effective divisors for a fixed g, and this is all $g-1$ of them.

On the other hand, maximizing $\overline{h}(S)$ comes from having lots of gaps below $m(S)$. So $\mathcal{O}_{g+1}$ with all its gaps below $m(S)$ will maximize this value.

Proposition 7

$$\overline{h}(\mathcal{O}_g) = \left\lceil \frac{g}{2} \right\rceil$$

Proof 12 *If $S = \mathcal{O}_g - \{x\}$ is a numerical semigroup, then x is a removable gap of $\mathcal{O}_g$, which means it is fragile, so $s+x \in \mathcal{O}_g$ for all $s\mathcal{O}_g \cup \{x\}$. But if $s \in \mathcal{O}_g$, then this is clearly true for any x. So the condition comes down to whether $x+x \in \mathcal{O}_g$. Then*

$$\overline{h}(\mathcal{O}_g) = |\{x \leq g \mid 2x > g\}| = \left\lceil \frac{g}{2} \right\rceil$$

Looking back at the original inequality

$$\sum_n \left[\overline{t}(g+1,n) - \overline{t}(g-1,n)\right] n < 0$$

This looks like something ripe for generating functions, so let's define

$$T(x,y) = \sum_{n\geq 0}\sum_{g\geq 0} \overline{t}(g,n) x^n y^g$$

Then

$$\frac{x}{y}\frac{\partial}{\partial x}T(x,y) = \sum_{n\geq 0}\sum_{g\geq -1} \overline{t}(g,n) n x^n y^{g+1} = \sum_{n\geq 0}\sum_{g\geq 0} \overline{t}(g-1,n) x^n y^g$$

$$yx\frac{\partial}{\partial x}T(x,y) = \sum_{n\geq 0}\sum_{g\geq 1} \overline{t}(g,n) n x^n y^{g-1} = \sum_{n\geq 0}\sum_{g\geq 0} \overline{t}(g+1,n) n x^n y^g$$

And this means

$$yx\frac{\partial}{\partial x}T(x,y) - \frac{x}{y}\frac{\partial}{\partial x}T(x,y) = \sum_{n\geq 0}\sum_{g\geq 0} \left[\overline{t}(g+1,n) - \overline{t}(g-1,n)\right] n x^n y^g$$

Let's write

$$C(g) = \sum_n \left[\overline{t}(g+1,n) - \overline{t}(g-1,n)\right] n$$

As a reminder, we have

$$N(g) < N(g-1) \Rightarrow C(g) < 0$$

Then setting $x=1$ gives

$$\left(y - \frac{1}{y}\right) \frac{\partial}{\partial x}T(x,y)\Big|_{x=1} = \sum_{g\geq 0} C(g) y^g$$

Let's compute a few of these terms.

$$C(0) = [\overline{t}(1,0) - \overline{t}(-1,0)]0$$
$$= 0$$
$$C(1) = [\overline{t}(2,0) - \overline{t}(0,0)]0 + [\overline{t}(2,1) - \overline{t}(0,1)]1$$
$$= [1-1]0 + [1-0]1$$
$$= 1$$
$$C(2) = [\overline{t}(3,0) - \overline{t}(1,0)]0 + [\overline{t}(3,1) - \overline{t}(1,1)]1 + [\overline{t}(3,2) - \overline{t}(1,2)]2$$
$$= [3-1]0 + [0-0]1 + [1-0]2$$
$$= 2$$
$$C(3) = [\overline{t}(4,0) - \overline{t}(2,0)]0 + [\overline{t}(4,1) - \overline{t}(2,1)]1 + [\overline{t}(4,2) - \overline{t}(2,2)]2$$
$$= [5-1]0 + [0-1]1 + [2-0]2$$
$$= 3$$

Let's take a look at that last one. We finally got a negative term: $[\overline{t}(4,1) - \overline{t}(2,1)]1 = -1$, but the the next compensates for it.

$$C(4) = [\overline{t}(5,0) - \overline{t}(3,0)]0 + [\overline{t}(5,1) - \overline{t}(3,1)]1 + [\overline{t}(5,2) - \overline{t}(3,2)]2 + [\overline{t}(5,3) - \overline{t}(3,3)]3$$
$$= [8-3]0 + [2-0]1 + [1-1]2 + [1-0]3$$
$$= 5$$

Let's compute the necessary values for $g = 6$ so we can calculate $C(5)$. And eventually, we'll just write up some code. I've been struggling a ton getting the GAP interface to work through SageMath, but The Combinatorial Object Server is a savior for generating numerical semigroups!

S^c	$\{1,2,3,4,5,6\}$	$\{1,2,3,4,5,7\}$	$\{1,2,3,4,5,8\}$	$\{1,2,3,4,5,9\}$	$\{1,2,3,4,5,10\}$	$\{1,2,3,4,5,11\}$	$\{1,2,3,4,6,7\}$	$\{1,2,3,4,6,8\}$
$\overline{h}(S)$	3	3	2	2	0	0	1	0

S^c	$\{1,2,3,4,6,9\}$	$\{1,2,3,4,6,11\}$	$\{1,2,3,4,7,8\}$	$\{1,2,3,4,7,9\}$	$\{1,2,3,4,8,9\}$	$\{1,2,3,5,6,7\}$	$\{1,2,3,5,6,9\}$	$\{1,2,3,5,6,10\}$
$\overline{h}(S)$	0	0	0	0	0	0	0	0

S^c	$\{1,2,3,5,7,9\}$	$\{1,2,3,5,7,11\}$	$\{1,2,3,6,7,11\}$	$\{1,2,4,5,7,8\}$	$\{1,2,4,5,7,10\}$	$\{1,2,4,5,8,11\}$	$\{1,3,5,7,9,11\}$
$\overline{h}(S)$	1	0	0	0	0	0	0

so

$$\overline{t}(6,0) = 17 \quad \overline{t}(6,1) = 2$$
$$\overline{t}(6,2) = 2 \quad \overline{t}(6,3) = 2$$

and

$$C(5) = [\overline{t}(6,0) - \overline{t}(4,0)]0 + [\overline{t}(6,1) - \overline{t}(4,1)]1 + [\overline{t}(6,2) - \overline{t}(4,2)]2 + [\overline{t}(6,3) - \overline{t}(4,3)]3$$
$$= [17-5]0 + [2-0]1 + [2-2]2 + [2-0]3$$

$$= 8$$

And for $g = 7$, we have

$$\overline{t}(7,0) = 26 \quad \overline{t}(7,1) = 6$$

$$\overline{t}(7,2) = 5 \quad \overline{t}(7,3) = 1$$

$$\overline{t}(7,4) = 1$$

and

$$C(6) = [\overline{t}(7,0) - \overline{t}(5,0)]0 + [\overline{t}(7,1) - \overline{t}(5,1)]1 + \cdots + [\overline{t}(7,4) - \overline{t}(5,4)]4$$

$$= [26-8]0 + [6-2]1 + [5-1]2 + [1-1]3 + [1-0]4$$

$$= 12$$

If we get anything for $T(x,y)$, we can use that to maybe make more sense of these coefficients.

$$T(x,y) = \sum_{n\geq 0}\sum_{g\geq 0} \overline{t}(g,n)x^n y^g$$

Recall that $\overline{h}(S)$ is maximized when $S = \mathcal{O}_g = \{1,2,\ldots,g\}^c$, which gives $\overline{h}(\mathcal{O}_g) = \lceil g/2 \rceil$, so we can rewrite the sum with n dependent on g:

$$T(x,y) = \sum_{g\geq 0}\sum_{n=0}^{\lceil g/2\rceil} \overline{t}(g,n)x^n y^g$$

So

$$T(1,y) = \sum_{g\geq 0}\left(\sum_{n=0}^{\lceil g/2\rceil} \overline{t}(g,n)\right) y^g = T(1,y) = \sum_{g\geq 0} N(g)y^g$$

A natural question is what $T(x,1)$ is? For an example of such values being significant, the *Tutte polynomial* of a graph is a 2-variable polynomial associated to a graph that encodes massive amounts of information. I will write $F_G(x,y)$ for this polynomial instead of T, to avoid confusion when we return to the discussion above. Although it can be defined in various ways, one is in terms of connected components of G when removing sets of edges. If $k(A)$ is the number of components of $G - A$, then

$$F_G(x,y) = \sum_{A\subset E} (x-1)^{k(E)-k(A)}(y-1)^{k(A)+|A|-|V|}$$

Then a few specializations give

- $F_G(x,y)$ encodes the chromatic polynomial $\chi_G(x)$ by

$$(-1)^{|V|-k(G)}x^{k(G)}F_G(1-x,0) = \chi_G(x)$$

- As a result of the beautiful connection that $\chi_G(-1)$ counts the number of Acyclic Orientations of G, we can also get this from $F_G(x,y)$ by looking at $F_G(2,0)$.
- $F_G(1,1)$ counts the number of spanning trees in G. This is also the size of the critical group $\mathcal{K}(G)$.
- $F_G(2,2) = 2^{|E|}$.
- Along the hyperbola $xy = 1$, $F_G(x,y)$ is the Jone's polynomial of the associated alternating knot.

So going back to $T(x,y)$, we have $T(1,y)$ the generating function for $N(g)$, and

$$T(x,1) = \sum_{n\geq 0}\left(\sum_{g\geq 0}\bar{t}(g,n)\right)x^n$$

and the inner sum is infinite. For example, when $n=0$, we get

$$1+1+1+3+5+8+\ldots$$

$$T(x,y) = \sum_{n\geq 0}\sum_{g\geq 0}\bar{t}(g,n)x^n y^g$$

...what to do?

Well suppose S is a numerical semigroup of genus g with n removable gaps. Then removing one of those gaps gives another numerical semigroup S' of genus $g-1$, and how many removable gaps does S' have? Write $S' = S\cup\{x\}$.

If y is a removable gap of S, then first, $y < m(S)$. Removing such a gap doesn't decrease multiplicity, so $m(S) = m(S')$, so we have $y < m(S')$. Second, y is fragile in S, meaning for all $s\in S\cup\{y\}$, we have $s+y\in S$. So the only way we'd have $s'+y\notin S'$ for $s'\in S'$ is if $s' = x$. This means

$$y \textit{ is fragile in } S\cup\{x\} \quad\Leftrightarrow\quad x+y\in S$$

So $\overline{h}(S') = |\{y < m(S) \mid x+y\in S\}| - 1$.

Ok, I can't lie, I'm definitely looking towards constructing some graphs! The equivalence is symmetric, so it seems only natural: let $\mathcal{T}(S)$ be the graph with

$$V = \{\textit{removable gaps of } S\}$$

$$E = \{(x,y) \mid x+y\in S\}$$

Before I code this up and post some examples, I wanted to record a couple facts.

1. The number of vertices of $\mathcal{T}(S)$ is $\overline{h}(S)$.
2. The degree of $x\in V$ is $\overline{h}(S\cup\{x\})$.

3. By the handshaking lemma, the number of edges is

$$\frac{1}{2}\sum_{\substack{x \text{ removable} \\ \text{gap of } S}} \overline{h}(S \cup \{x\})$$

For example, if $S = \{1,2,3,4,5\}^c$, then the sum is

$$\overline{h}(\{1,2,3,4\}) + \overline{h}(\{1,2,3,5\}) + \overline{h}(\{1,2,4,5\}) = 2+2+0 = 4$$

Notice that the value is equal to $N(3)$. For $S = \{1,2,3,4,5,6\}^c$, we get

$$\overline{h}(\{1,2,3,4,5\}) + \overline{h}(\{1,2,3,4,6\}) + \overline{h}(\{1,2,3,5,6\}) = 3+1+2 = 6$$

Which is $N(4)-1$. The one we missed was $\{1,3,5,7\}$, since that only comes from removing 2 from $\{1,2,3,5,7\}$, and that set cannot be obtained by removing a removable divisor from $\mathcal{O}_6$.

Let $\mathcal{N}_g^x$ be the numerical semigroups of genus g with x as a removable gap and let $\rho_x : \mathcal{N}_g^x \to \mathcal{N}_{g-1}$ given by $\rho_x(S) = S \cup \{x\}$. Suppose that $\rho_x(S_1) = \rho_x(S_2)$. Then $S_1 \cup \{x\} = S_2 \cup \{x\}$, so $S_1 = S_2$. Therefore, this map is injective. Which shows for all x,

$$|\mathcal{N}_g^x| \leq N(g-1)$$

WILL CONTINUE

24 Duality

I started the graph idea with this idea of "duality" between *effective generators* and *removable gaps*, in the sense that they are exactly the elements that can be added and removed from a numerical semigroup to produce another numerical semigroup to invert the operations of removing multiplicities and adding Frobenius numbers.

Alternating the operations of adding Frobs and removing mults for a numerical semigroup S of genus g will always stabilize on $\mathcal{O}_g$, and gives a path from S to $\mathcal{O}_g$ alternating with sets $S' \in \mathcal{N}_{g-1}$. Therefore, starting from $\mathcal{O}_g$, we should be able to produce every $S \in \mathcal{N}_g$ by alternating adding removable gaps and removing effective divisors.

So one numerical semigroup S gives us $ON(S) - 1$ other numerical semigroups of genus g and $g-1$. But as soon as we choose another S, we might not get totally distinct numerical semigroups. Understanding this underlap is key to understanding which side is larger.

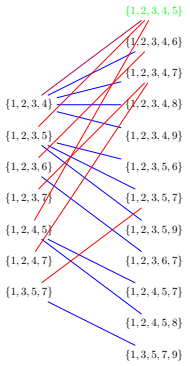


Figure 43: Step 0

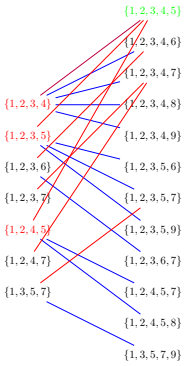


Figure 44: Step 1

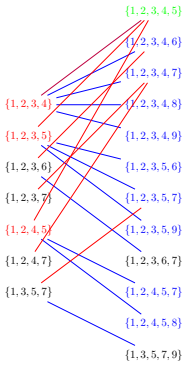


Figure 45: Step 2

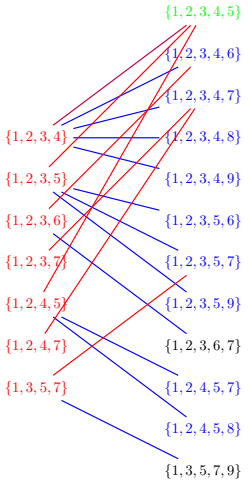


Figure 46: Step 3

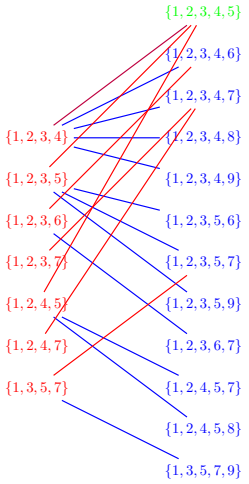


Figure 47: Step 4

The sum over removable gaps of S of $\overline{h}(S)$ was to characterize a relationship between the three values $N(g-2), N(g-1), N(g)$. I guess a more direct way to understand the duality of these operations is to look at the two sums

$$U(S) = \sum_{\substack{x \text{ removable} \\ \text{gap of } S}} h(S \cup \{x\})$$

$$L(S) = \sum_{\substack{x \text{ effective} \\ \text{generator of } S}} \overline{h}(S - \{x\})$$

In essence, we look at all the ways to move from one side to the other, and then all the ways to go back on a different colored edge. Actually defining the union of these is so bulky, so thinking about it in terms of the graph Γ_g is much easier!

25 A New Document

This has gotten very long and takes awhile to compile, so I'm starting a fresh document (Arithmetic Explorations 2), which will naturally reference back to this document.