MATH 314 Spring 2024 - Class Notes

02/12/2024

Scribe: Aja Curry

Ciphertext Only Attack Against the Hill Cipher

- If the block size is 2 or 3, we can use frequency analysis on blocks
- Find the most frequently occuring blocks
- Guess that its one of the most requent bigrams (trigrams)
  - "th" is the most frequent bigram
    - Tie between "er" and "he"

Moving Beyond (mod 26)

- **Residue (mod n): The collection of all integers that have the same remainder (mod n)**
  - Usually represented using the remainder between 0 and n
    - Residue S (mod 8) is all numbers {-3,5,13,21,...}
- Z_m for the set of all residues (mod m)
  - Ring
    - $Z_6 = \{0,1,2,3,4,5\}$
- Can add, subtract, and multiply residues
  - Can pick any representative of the residue class to do arithmetic
- Ring: Any collection of things can be added, subtracted, and multiplied (with regular arithmetic rules)
- When possible, do division, and find inverses
  - Fact: A (mod m) has an inverse a^{-1} (meaning $a(a^{-1}) \equiv \pmod{m}$), if gcd(a,m)=1

Euclid's Algorithm

- How do we compute gcd's quickly?

    1. Factor both numbers (slow)

Euclid's Observations

- Division with remainder (long division) of a by b and always get a remainder r smaller than b
    - $a = bq + r, 0 \leq r < b$ (Cannot have a negative remainder)
- If d divides a and b, then d divides $a - bq = r$, so do divides r
    - Similarly, any d that divides both b and r divides $qb + r = a$
        * Meaning gcd (a,b) = gcd (b,r) (Euclid's Observation)
        * gcd (a,b) should be large
        * gcd (b,r) should be small
    - Iterate this and each time, the numbers get smaller
    - Once you get a remainder of 0 the previous remainder is the gcd
- gcd(119,91)
    - 91 goes into 119 1 time with a remainder of 28, so $119 = 1(91) + 28$

gcd(119,91)=gcd(91,28)

- gcd(91,28). Keep going until a remainder of 0.
    - 28 goes into 91 3 times with a remainder of 7 ($91 = 3(23) + 7$)
    - 7 goes into 28 4 times with a remainder of 0 ($28 = 4(7) + 0$)

gcd(28,7)=7

gcd(119,91)=7

Extended Euclid's Algorithm

- If gcd(a,b) = d, then there exists. integers x and y so that $ax + by = d$ (linear combination)