BASIC NUMBER THEORY, PROBLEM SET 1

Most of the following problems are taken from *An Introduction to the Theory of Numbers*, by Niven, Zuckerman, and Montgomery. The variables a, b, and c are assumed to be integers throughout.

Properties of Divisibility

1. Show the following basic properties of divisibility:
   (a) $a|b$ implies $a|bc$ for any integer c;
   (b) $a|b$ and $b|c$ imply $a|c$;
   (c) $a|b$ and $a|c$ imply $a|(bx+cy)$ for any integers x any y (and in particular $a|b+c$);
   (d) $a|b$, $a>0$, and $b>0$ imply $a \leq b$.

2. Two integers are said to be of the same *parity* if they are both even or both odd; if one is even and the other odd, they are said to be of opposite parity, or of different parity. Given any two integers, show that their sum and difference are of the same parity.

3. Show that if n is an odd integer, then n^2-1 is divisible by 8.

Properties of GCDs

4. Demonstrate the following properties of greatest common divisors:
   (a) If m is a positive integer, then $(ma, mb) = m(a, b)$.
   (b) If $(a, m) = (b, m) = 1$, then $(ab, m) = 1$.
   (c) For any integer x, $(a, b) = (b, a) = (a, -b) = (a, b + ax)$.
   (d) If $c|ab$ and $(b, c) = 1$, then $c|a$.

5. Compute the greatest common divisor g of 15196 and 3045. Then, express g in the form $15196x + 3045y$ for integers x and y. (Repeat this problem with random pairs of integers until you get the hang of the algorithm.)

6. Let b and $g>0$ be given integers. Show that the equations $(x, y) = g$ and $xy = b$ can be solved simultaneously if and only if $g^2|b$.

7. Show that $(a, a+k)|k$ for all integers a, k not both zero.

8. Provide a sensible definition for what it means to take the GCD of a long(er) list of integers, and try to extend as many of our results as you can to this more general case.

9. Show that $(a, b, c) = ((a, b), c)$.

10. Show that $a|bc$ if and only if $\frac{a}{(a,b)}|c$.

11. Provide a sensible definition of the *least common multiple* (LCM) of two nonzero integers. Denoting the LCM of a and b by $[a, b]$, show that your definition implies that $[a, b](a, b) = |ab|$, where $|x|$ means the absolute value of x.

12. Evaluate $(n, n+1)$ and $[n, n+1]$ where n is a positive integer.

Miscellaneous and Harder problems

13. Show that the Division Algorithm is a very fast way to compute GCDs. Specifically, if you're using the Division Algorithm to compute the GCD of b and c, with $c<b$, show that the process will terminate in fewer than $3\log c$ divisions. Here, log means the natural logarithm, i.e. the logarithm to the base e. (Hint: if r_i is the i^{th} remainder in the process, consider what happens in the two separate cases when $r_i \leq r_{i-1}/2$ or $r_i > r_{i-1}/2$.)

14. If a and $b > 2$ are any positive integers, show that $2^a + 1$ is not divisible by $2^b - 1$.

15. Show that if $(a, b) = 1$ and n is an odd positive integer, then $\left(a + b, \frac{a^n + b^n}{a+b}\right)$ divides n. (What can go wrong here, for even n?)

16. Draw a circle of radius 1 around the origin in the plane, and mark off the point $(4/5, 3/5)$. Let θ be the arc of the circle between that point and the horizontal, so that $\cos\theta = 4/5$ and $\sin\theta = 3/5$. If n is an integer, show that the point on the circle which is an angle of $n\theta$ from the horizontal actually has rational coordinates too. Can you show that this gives you infinitely many rational points on the circle?

17. (Really hard!) Let a and b be positive integers such that $(1 + ab)|(a^2 + b^2)$. Show that the integer $\frac{a^2+b^2}{1+ab}$ must be a perfect square.