18.781 Problem Set 1

Thursday, February 16.

Collaboration is allowed and encouraged. However, your writeups should be your own, and you must note on the front the names of the students you worked with.

Extensions will only be given for extenuating circumstances.

1. Let $a > 0$ and b be integers. Show that there is an integer k such that $b + ka > 0$. (Hint: use well-ordering.)

2. Let a and b be positive integers whose gcd is 1. Find the largest positive integer $n(a, b)$ which is *not* a non-negative integer linear combination of a and b. Prove your answer (i.e. show that $n(a, b)$ cannot be represented as $ax + by$ with $x, y \in \mathbb{N} \cup \{0\}$ and that every greater integer can be represented in such a way).

3. Let $a > 1$ be a positive integer, and m, n be natural numbers. Show that $a^m - 1 | a^n - 1$ if and only if $m|n$. Show that the gcd of $a^m - 1$ and $a^n - 1$ is $a^{(m,n)} - 1$.

4. Use the Euclidean algorithm to find an integer solution (x_0, y_0) to $89x + 43y = 1$. Then use your solution to describe all possible integer solutions systematically.

5. Let $1 < a < b$ be integers. Show that the number of division steps involved in the Euclidean algorithm to compute the gcd of a and b is at most a (universal) constant times $\log(a)$. (Hint: observe what happens after two steps of the algorithm).

6. This will be your first exercise using the math software gp/PARI, which specializes in number theory calculations (see the class website for instructions on how to download it, and links to tutorials). Using gp, tabulate the number of primes less than x, for $x = 10000, 20000, \ldots, 100000$. Also tabulate the number of primes less than x and of the form $4k + 1$, and the number of the form $4k + 3$, and finally, tabulate $x/\log(x)$ (natural logarithm). Turn in a printout of your code. What are your observations?

7. A board has squares numbered 1 through n. Two players A and B play the following game: A starts, putting a token on some square a_1. Then B puts a token on some square b_1, which is not allowed to divide a_1. Then A follows with a_2, such that $a_2 \nmid a_1$ and $a_2 \nmid b_1$, and so on (at any stage, the number of the square selected must not divide any of the previous ones). The last person to put down a token wins. Try playing this game for $n = 10, 12, 24$. Who wins? Prove your observation for general n. Bonus: Can you find a winning strategy?

8. Show that there are infinitely many primes of the form $4k + 3$.