18.781 Problem Set 1

Due Wednesday, February 23

1. (a) Use the Euclidean algorithm to find the gcd of 3960 and 945. Then factor one into a product of primes and use this information to find the gcd again.

(b) Solve the Diophantine equation $ax+by = \gcd\{a, b\}$ (i.e., find all solutions (x, y) with x and y integral), with

(i) $a = 56, b = 35$.
(ii) $a = 309, b = 186$.
(iii) $a = 1024, b = 729$.

2. Let m be a natural number. Show that if m is the square of a rational number, then it is the square of an integer. Equivalently, if m is not a perfect square, then $\sqrt{m}$ is irrational.

3. Show that there are infinitely many primes $p \equiv -1 \pmod 3$. (Hint: Suppose $\{p_1, \ldots, p_s\}$ were a list of all such primes, and consider the primes dividing $n = 3p_1 \cdots p_s - 1$.) For what other positive integers d does this argument work to show that there are infinitely many primes $p \equiv -1 \pmod d$?

4. Assume that a and b are relatively prime integers such that $a^2 - b^2$ is a square.

(a) Show that $\gcd\{a + b, a - b\}$ is either 1 or 2.

(b) Show that either $a + b$ and $a - b$ are both squares or are both twice squares.

5. A prison warden guarded 100 prisoners, in separate cells numbered 1 through 100. The locks were such that a twist of the key locked them if unlocked and *vice versa*. One night, when all were asleep, he found compassion and opened ALL their doors. But when he went back to his room he had second thoughts, decided he'd released too many, returned to twist the key in the even cells, and went back to bed. Then he had third thoughts, returned to twist the key in locks of cells whose numbers were divisible by 3, and returned to bed. Well, it was a long night, and he kept this up till just before daybreak, when he twisted the key in the lock of cell 100. Which prisoners went free? The question for you is: what is the number-theory behind this? What if it were a much larger prison?

6. (The "Chinese remainder theorem") Let $n_1, n_2, \ldots, n_k$ be pairwise relatively prime positive integers, and let $b_1, b_2, \ldots, b_k$ be arbitrary integers. Show that there exists an interger x such that

$$x \equiv b_i \pmod{n_i}$$

for all i. [Hint: Do the case $b_j = 1$, $b_i = 0$ for $i \neq j$, first, using the fact that n_j is relatively prime to the product of the other n's.]

For Fun: I have an old-fashioned balance scale, with two pans. I want to buy n weights, each weighing a whole number of ounces, so that by putting some of them on one pan and some on the other I can weigh out all amounts between 0 and the largest possible number of ounces. What should my set of weights weigh?

Mathematicians are like Frenchmen: whatever you say to them they translate into their own language and forthwith it is something entirely different.— Goethe