Math 6 – Number Theory WS #3

Homework:

1. (a) Use the Euclidean algorithm to find an integer x for which $7x = 1$ in $\mathbf{Z}_{193}$. Show your work.

   (b) Use your solution to part (a) to find an integer x for which $7x = 13$ in $\mathbf{Z}_{193}$.

2. One of the most intriguing discoveries in mathematics is the existence of *irrational* numbers; these are numbers which cannot be written as the ratio of integers. Historically, the first example of an irrational number is

$$\sqrt{2} = 1.41421356237309504880168872420 96\ldots$$

   Here we outline the very simple argument that $\sqrt{2}$ is irrational:

   If $\sqrt{2}$ is rational, then we can write it as a fraction p/q. Moreover, by canceling common factors in the numerator and denominator, we can assume that p/q is in lowest terms. (In other words, p and q are positive integers and $\gcd(p,q) = 1$.) We proceed to derive a contradiction; thus our assumption that $\sqrt{2}$ is rational cannot be valid.

   Assuming $p/q = \sqrt{2}$, we have $p^2/q^2 = 2$, so that

$$p^2 = 2q^2. \tag{1}$$

   (a) Explain why p must be even for this equation to be true.

   (b) Assuming p is even, argue that q must also be even for (1) to hold.

   (c) Why does what you proved in (a) and (b) imply that $\sqrt{2}$ is irrational. (Remember, p/q was a fraction *in lowest terms.*)

3. Actually we can prove quite a few other numbers are irrational now that we have shown unique factorization. For example, consider the integer $n = 2^3 \cdot 5^2 \cdot 7^3$. If $\sqrt{n}$ were a rational number p/q, then we would have

$$p^2 = 2^3 5^2 7^3 q^2.$$

   Explain why it is impossible for there to exist positive integers p and q for which this equation holds. (Hint: factor p and q into primes, and compare the unique prime factorizations of both sides.)

   Do you have a guess as to which numbers $1, 2, 3, 4, \ldots$ have rational square roots and which have irrational square roots? (For example, the perfect squares $1, 4, 9, 16, \ldots$ all have rational square roots – in fact even integer square roots. Are there any other positive integers with rational square roots?)