Ma/CS 6a: Problem Set 1

Due noon, Thursday, October 9

September 27, 2014

1. In class we used induction to prove the prime decomposition property, and we proved by contradiction that there are infinitely many primes. Use contradiction to prove the prime decomposition property, and induction to prove that there are infinitely many primes.

2. In class we showed that for any pair of natural numbers $a, b \in \mathbb{N}$, there exist a quotient and a remainder $q, r \in \mathbb{N}$ such that $a = bq + r$ and $0 \leq r < b$. Prove that the pair q, r is unique (that is, that no other pair of natural numbers satisfies these two conditions).

3. Given $a, b \in \mathbb{N}$, the *least common multiple* of a and b, also written as $LCM(a, b)$, is the smallest natural number $c \in \mathbb{N}$ such that $a|c$ and $b|c$. For example, $LCM(5, 25) = 25$ and $LCM(6, 21) = 42$.
(a) Let $p_1, p_2, \ldots, p_k$ be distinct prime numbers, and let $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k \in \mathbb{N}$. What is $LCM(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k})$? What is $GCD(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k})$?
(b) Prove that for any pair $a, b \in \mathbb{N} \setminus \{0\}$, we have

$$LCM(a, b) \cdot GCD(a, b) = a \cdot b.$$

4. (a) Prove that for any $a \in \mathbb{Z}$, we have $a^2 \equiv r_a \mod 8$, where r_a is either 0,1, or 4.
(b) Use the first part of the question to prove that 1003456789 is not a perfect square (that is, there is no $a \in \mathbb{N}$ such that $a^2 = 1003456789$).
(c) Prove that no number of the form $3^n + 3^m + 1$, where $n, m \in \mathbb{N}$, is a perfect square.

5. Use the RSA algorithm to encrypt and decrypt the very secret number 2014, and write down all the steps of the algorithm. For that purpose, you need to use some mathematical program. The simplest one is perhaps the website `http://www.wolframalpha.com/`.

- Use the program to generate two random four-digit primes p, q. (If you use wolfram alpha, simply write "random prime between 1000 and 9999".)
- Use p, q to generate a public key and a private key. Then use the keys to encrypt and decrypt 2014.
- Use a value of e that is at least four digits. Try arbitrary four-digit numbers. With a very high probability, one of your first choices would work.
- Other command which you might find useful: "phi(1111)" and "solve 12*x-82=167 over the integers".