Math 115 Problem Set 4

Due July 15, 2010

Do the following exercises from the book: 2.17, 2.29, 3.2, (optional: 3.4, 3.5)

(1) In this problem, we analyze a protocal for "flipping a coin over the phone" with somebody you don't trust. Suppose Jenny and Tommy are on the phone trying to decide who pays the phone bill this month. Since neither one of them trusts the other to truthfully report the outcome of a coin flip, they decide on the following protocol. Jenny picks two large primes p and q which are both of the form $4k+3$ and tells $p \cdot q$ to Tommy. Tommy picks a random number t modulo $p \cdot q$ and tells t^2 modulo $p \cdot q$ to Jenny. Jenny finds all the square roots of t^2 modulo $p \cdot q$, picks one at random, call it s, and tells it to Tommy. If Tommy can find p and q, he wins. Otherwise, Jenny wins.

   (a) Show that if p is a prime of the form $4k + 3$ and a is a square modulo p, then $a^{(p+1)/4}$ is a square root of a modulo p.

   (b) How does Jenny find all the square roots of t^2 modulo $p \cdot q$? How many square roots are there? Remember that she only knows t^2, not t.

   (c) How can Tommy use the square root s given to him by Jenny to efficiently find p and q? Remember that he isn't always able to find p and q, but he should be able to do so half the time. (Hint: use CRT.)

(2) Given two multiplicative functions f and g, define the *convolution product* as $(f*g)(n) = \sum_{d \geq 1, d|n} f(d)g(n/d)$.

   (a) Show that the convolution product of two multiplicative functions is multiplicative.

   (b) Show that the convolution product is commutative. That is, if f and g are multiplicative functions, $(f * g)(n) = (g * f)(n)$ for all n.

   (c) Show that convolution product is associative. That is, show that if f, g, and h are multiplicative functions, then $((f * g) * h)(n) = (f * (g * h))(n)$ for all n.