MATH 315; HOMEWORK # 6

Due Mar. 11, 2015

1. (Exercise 22.7) Suppose that a is a quadratic residue modulo p, and suppose further that $p \equiv 3 \pmod 4$.

(a) Show that $x = a^{\frac{p+1}{4}}$ is a solution to the congruence $x^2 \equiv a \pmod p$. This gives an explict way to find square roots modulo p for primes congruenet to 3 modulo 4.

(b) Find a solution to the congruence $x^2 \equiv 7 \pmod{787}$. (Your answer should lie between 1 and 786).

2. (Exercise 22.8 (a,b)) Suppose that a is a quadratic residue modulo p, and suppose further that $p \equiv 5 \pmod 8$.

(a) Show that one of the values $x = a^{\frac{p+3}{8}}$ or $x = 2a \cdot (4a)^{\frac{p-5}{8}}$, is a solution to the congruence $x^2 \equiv a \pmod p$. This gives an explict way to find square roots modulo p for primes congruenet to 5 modulo 8.

(b) Find a solution to the congruence $x^2 \equiv 5 \pmod{541}$. (Your answer should lie between 1 and 540).

3. (Exercise 22.10 (a)) (a) Euler's criterion says that if p is a prime, then $a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \pmod p$. Use successive squaring to compute $11^{\frac{1729-1}{2}} \pmod{1729}$ and use Quadratic Reciprocity to compute $(\frac{11}{1729})$. Do they agree? What can you conclude concerning the possible primality of 1729?

4. (Exercise 24.2) If the prime p can be written in the form $p = a^2 + 5b^2$, show that $p \equiv 1$ or $9 \pmod{20}$. (Of course, we are ignoring $5 = 0^2 + 5 \cdot 1^2$.)

5. (Exercise 24.4 (a)) Start from $259^2 + 1^2 = 34 \cdot 1973$ and use the descent procedure to write the prime 1973 as a sum of two squares.

6. (Exercise 25.6 (b, c)) For any positive integer m, let $S(m) = (\#$ of ways to write $m = a^2 + b^2$ with $a \geq b \geq 0)$.

(b) If p is a prime and $p \equiv 1 \pmod 4$, what is the value of $S(p)$?

(c) Let p and q be two different primes, both congruent to 1 modulo 4. What is the value of $S(pq)$?