Math 40520 Theory of Number
Homework 7

Due Wednesday, 10/14

Do 5.

1. Show that there exist infinitely many primes $\equiv 1 \pmod 3$. [You might find useful a problem from the midterm.]

2. Suppose $3^{10} \mid \binom{3n}{n}$ for a positive integer n. Show that $n > 3^8$.

3. Show that there exists an integer solution to $x^3 \equiv 26 \pmod{3^n}$ for any n. [Hint: Write $x = 3y + a$ for some a and simplify before trying to apply Hensel's lemma.]

4. Let a be an odd integer and $n \geq 3$ be an integer. Show that a is a square modulo 2^n if and only if $a \equiv 1 \pmod 8$.

5. This is not a probability question. We've seen in class that 2 is a primitive root modulo about 37.4% of the primes $p > 6$, and the same is true of 3 and 6. If these three conditions were independent random events we would predict that about $14\% = (37.4\%)^2$ of the primes have both 2 and 3 as primite root (or 2 and 6, or 3 and 6). In fact this number is closer to 14.7%. Moreover, it would follow that about $5.2\% = (37.4\%)^3$ of the primes have 2, 3, and 6 as primitive roots. Prove that, in fact, there exists no prime p such that 2, 3, and 6 are primitive roots modulo p. (It is, however, the case that about 6% of the primes have 2, 3, and 7 as primitive roots.) [Hint: Here p is fixed and you may use a fixed primitive root a. What does it mean that 2 is primitive mod p, in terms of a?]

6. Show that the probability that 2 and 3 are primitive roots modulo p is $\prod_q \left(1 - \frac{2q-1}{q^2(q-1)}\right) \approx 14.7\%$ under the following two model assumptions:

   (a) $p \equiv 1 \pmod q$ are independent of q and

   (b) the probability that a and b are primitive roots are independent of a and b (distinct).

7. The sieve of Eratosthenes is a method for determining the primes up to X. You enumerate all numbers from 2 to X. Circle 2 and eliminate all larger evens. Then circle 3 and eliminate all larger multiples of 3. Every iteration you pick out the smallest uncircled number still in play and eliminate all larger multiples. In the end, the remaining numbers are all circled and are precisely the primes up to X. In probability language this states that $\Pr(x < X \text{ is prime}) = \Pr(p \nmid x \text{ for each prime } p < X)$. Assume the following statistical model for primes: the conditions $p \nmid x$ are all independent as p varies among the primes up to X. Take for granted that $\prod_{p<X} \left(1 - \frac{1}{p}\right) \approx \frac{1.12}{\log X}$. Show that the model then implies that $\pi(X) \approx \frac{1.12X}{\log X}$. (Needless to say, this model does not fit reality.)

8. Suppose $2^n - 1$ is a prime. Show that n is also a prime. Such primes are called Mersenne primes. All recent examples of "largest primes" are of this form. It's an open problem whether there are infinitely many Mersenne primes.

9. Suppose $2^n + 1$ is a prime. Show that $n = 2^m$ for some m. Such primes are called Fermat primes. It's an open problem whether there are infinitely many Mersenne primes and only 5 are known to be primes: $2^{2^0} + 1, 2^{2^1} + 1, 2^{2^2} + 1, 2^{2^3} + 1$ and $2^{2^4} + 1$.