Math 124 Homework 4 Solutions

by Luke Gustafson

Fall 2003

1. Consider the coefficient of x^p in the expansion of $(1+x)^{2p} = (1+x)^p(1+x)^p$. On the left side, the coefficient of x^p is $\binom{2p}{p}$. On the right side, it is given by

$$\sum_{i=0}^{p} \binom{p}{i}\binom{p}{p-i} = \sum_{i=0}^{p} \binom{p}{i}^2$$

Recall that for $i \neq 0, p$, $\binom{p}{i}$ is divisible by p, so $\binom{p}{i}^2 \equiv 0 \pmod{p^2}$. Hence, we get

$$\binom{2p}{p} \equiv \sum_{i=0}^{p} \binom{p}{i}^2 \pmod{p^2}$$

$$\equiv \binom{p}{0} + \binom{p}{p} + \sum_{i=1}^{p-1} \binom{p}{i}^2 \pmod{p^2}$$

$$\equiv \binom{p}{0} + \binom{p}{p} + 0 \pmod{p^2}$$

$$\equiv 2 \pmod{p^2}$$

2a. If p is a divisor of $mx^2 - 1$, then $mx^2 - 1 \equiv 0 \pmod{p}$, so $mx^2 \equiv 1 \pmod{p}$. Note that if $p|x$, then $mx^2 - 1$ is not divisible by p, a contradiction; so that means x has an inverse modulo p. Therefore, $mx^2 \equiv 1 \pmod{p} \Rightarrow m \equiv (x^{-1})^2 \pmod{p}$, which shows m is a quadratic residue.

2b. Suppose that there are only finitely many such primes. Let their product be P. Use $P = 2$ if there are no such primes. Consider $mP^2 - 1$. This either has prime divisors, or it is ± 1.

In the exceptional case that $mP^2 - 1 = \pm 1$, then we have must have $m = 0$, since P is at least 2. But 0 is a quadratic residue for all primes, so we are finished.

If $mP^2 - 1$ has a prime divisor p, then p cannot divide P. Hence, by construction, m is not a quadratic residue modulo p. However, by part (a), m is a quadratic residue modulo p. This contradiction completes the proof.

2c. Consider $m = -1$. We know that -1 is a quadratic residue modulo an odd prime p if and only if $p \equiv 1 \pmod 4$, i.e., if and only if p is of the form $4k + 1$. Therefore part (b) implies that there are infinitely many primes of the form $4k + 1$.

Consider $m = -3$. From the properties of the Legendre symbol, $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$. We know that $\left(\frac{-1}{p}\right)$ is 1 if and only if $p \equiv 1 \pmod 4$.

Using quadratic reciprocity, $\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)$. $(-1)^{(p-1)/2}$ is 1 if $p \equiv 1 \pmod 4$ and -1 if $p \equiv 3 \pmod 4$. $\left(\frac{p}{3}\right)$ is 1 if $p \equiv 1 \pmod 3$ and -1 if $p \equiv 2 \pmod 3$.

Putting this information together and using the Chinese Remainder Theorem, we can determine $\left(\frac{-3}{p}\right)$ for each residue modulo $3 \cdot 4 = 12$. We find that $\left(\frac{-3}{p}\right)$ is 1 if $p \equiv 1, 7 \pmod{12}$ and -1 if $p \equiv 5, 11 \pmod{12}$. Thus, -3 is a quadratic residue (for $p > 3$) if and only if $p \equiv 1, 7 \pmod{12} \Leftrightarrow p \equiv 1 \pmod 6$. Using part (b) as before, using $m = -3$ implies that there are infinitely many primes of the form $6k + 1$.

3a. Given that $10^k \equiv 1 \pmod p$, then $(10^k - 1)/p$ is an integer $a_1a_2 \ldots a_k$, where some of the initial digits may be 0. Then $0.\overline{a_1a_2 \ldots a_k} = \frac{a_1a_2 \ldots a_k}{10^k - 1} = \frac{1}{p}$ as desired.

Now, suppose $\frac{1}{p} = 0.\overline{a_1a_2 \ldots a_k} = \frac{a_1a_2 \ldots a_k}{10^k - 1}$. Then $10^k - 1 = p \cdot \overline{a_1a_2 \ldots a_k}$, so $10^k \equiv 1 \pmod p$.

This establishes the equivalence of the statements $10^k \equiv 1 \pmod p$ and $\frac{1}{p} = 0.\overline{a_1a_2 \ldots a_k}$ for some k. Since the order of 10 modulo p and the cycle length of the decimal expansion are both defined as the smallest positive k for which these are true, the order of 10 must equal the cycle length of $\frac{1}{p}$.

3b. By problem (2b), there are infinitely many primes such that 10 is a quadratic residue. By Euler's criterion, for such primes p we have $1 \equiv \left(\frac{10}{p}\right) \equiv 10^{\frac{p-1}{2}} \pmod p$. Therefore, the order of 10 is at most $\frac{p-1}{2}$.

3c. Since the order of 10 is even, we may write $10^k - 1 \equiv (10^{k/2} - 1)(10^{k/2} + 1) \equiv 0 \pmod p$. Since the order of 10 is exactly k, we must have $10^{k/2} \not\equiv 1 \pmod p$, so $10^{k/2} - 1 \not\equiv 0 \pmod p$. Therefore, $10^{k/2} + 1 \equiv 0 \pmod p$, i.e. $10^{k/2} + 1$ is divisible by p.

Now, consider

$$\frac{1}{p} + \frac{10^{k/2}}{p} = 0.\overline{a_1a_2 \ldots a_k} + a_1a_2 \ldots a_{k/2}.\overline{a_{k/2+1} \ldots a_k a_1 \ldots a_{k/2}}$$

By the preceding argument, the left side is an integer. Therefore, the right side is also an integer. In particular, by considering the fractional parts, we must have

$$0.\overline{a_1a_2\ldots a_k} + 0.\overline{a_{k/2+1}\ldots a_ka_1\ldots a_{k/2}} = 1$$

$$\frac{a_1a_2\ldots a_k}{10^k-1} + \frac{a_{k/2+1}\ldots a_ka_1\ldots a_{k/2}}{10^k-1} = 1$$

$$a_1a_2\ldots a_k + a_{k/2+1}\ldots a_ka_1\ldots a_{k/2} = 10^k - 1 = 999\ldots 9$$

By considering the last digit of the addition, we can see $a_k + a_{k/2} = 9$. Then, considering the next-to-last digit, $a_{k-1} + a_{k/2-1} = 9$, etc. We find $a_{k/2+i} + a_i = 9$ for $i = 1, 2, \ldots, \frac{k}{2}$. Summing together these equations gives the desired result $a_1 + a_2 + \cdots + a_k = \frac{9k}{2}$.