Math 124 Homework 5 Solutions

by Luke Gustafson

Fall 2003

1. $-163 \equiv 1^2 \pmod 2$ gives $p = 2$ the smallest prime.

2a. First, consider $q = 2$. We know 2 is not a quadratic residue if and only if $p \equiv 3, 5 \pmod 8$. By Dirichlet's theorem, there are infinitely many primes p of the form $3 + 8n$, so there are infinitely many primes with $q = 2$ not a quadratic residue.

Now consider q an odd prime. Let a be a quadratic non-residue modulo q. By Dirichlet's theorem, there exists an odd prime $r = a + qn$ for some $n \in \mathbb{N}$. Thus $r \equiv a \pmod q$, so r is a quadratic non-residue modulo q.

If $r \equiv 1 \pmod 4$, consider primes of the form $p = r + 4qn$. If $r \equiv 3 \pmod 4$, then consider $p = r + 2q + 4qn$ (notice that $r + 2q$ and $4q$ must be relatively prime). In each case, it is easy to check $p \equiv 1 \pmod 4$. By Dirichlet's theorem, there are infinitely many primes p of this form. Then, use quadratic reciprocity to get

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right)$$

Use the fact that $p \equiv 1 \pmod 4$ and $p \equiv r \pmod q$:

$$= (1) \left(\frac{r}{q}\right)$$

$$= -1$$

That proves there are infinitely many p such that q is a quadratic non-residue.

2b. From part (a), we know that for odd primes q_1, the condition that $p \equiv \alpha \pmod{4q_1}$, where $\alpha = r$ if $r \equiv 1 \pmod 4$ and $\alpha = r + 2q_1$ if $r \equiv 3 \pmod 4$, is sufficient to ensure q_1 is a quadratic non-residue modulo p. We may split this congruence into the equivalent system $p \equiv \alpha \pmod 4$ and $p \equiv \alpha \pmod{q_1}$. Also shown in part (a) is that $\alpha \equiv 1 \pmod 4$, so our system becomes

$$p \equiv 1 \pmod 4$$

$$p \equiv \alpha \pmod{q_1}$$

In the case that $q_1 = 2$, we will use the condition $p \equiv 5 \pmod 8$ to guarantee that 2 is a quadratic non-residue modulo p.

In the case that $q_i = 2$ for $i > 1$, we will use the condition $p \equiv 1 \pmod 8$ to guarantee that 2 is a quadratic residue modulo p.

For odd primes q_i, consider primes of the form $p = 1 + 4q_i n$, where $n \in \mathbb{N}$. Then we have

$$\left(\frac{q_i}{p}\right) = (-1)^{\frac{(p-1)(q_i-1)}{4}} \left(\frac{p}{q_i}\right)$$

Use the fact that $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod{q_i}$:

$$= (1)\left(\frac{1}{q_i}\right)$$

$$= 1$$

Hence, it suffices to impose the restriction $p \equiv 1 \pmod{4q_i}$ to ensure q_i is a quadratic residue modulo p. Equivalently, $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod{q_i}$.

Now we combine all these conditions on p to get a p with the desired properties. We consider the following system of congruences:

(1) $p \equiv 1 \pmod 4$ if $q_i \neq 2$ for all i

(2) $p \equiv 5 \pmod 8$ if $q_1 = 2$

(3) $p \equiv 1 \pmod 8$ if $q_i = 2$, $i > 1$

(4) $p \equiv \alpha \pmod{q_1}$

(5) $p \equiv 1 \pmod{q_i}$ for $i > 1$.

Notice that conditions (2) and (3) cannot occur simultaneously since we insist all the q_i are distinct.

We show that all primes p satisfying the above system satisfy the conditions of the problem. By the preceding arguments, if $q_i = 2$ for some i, then conditions (2) and (3) guarantee that 2 is appropriately a quadratic residue or non-residue. Observe that conditions (1), (2), and (3) guarantee that $p \equiv 1 \pmod 4$. Using this fact plus conditions (4) and (5), our preceding arguments have shown that q_1 is a quadratic non-residue and q_i is a quadratic residue for $i > 2$, as desired.

Now we show that there are infinitely many primes satisfying our system of congruences. Since the q_i are distinct, all the moduli are relatively prime. Thus, we apply the Chinese Remainder Theorem to rewrite the system as

$$p \equiv x \pmod N$$

where N is the product of the moduli and x is the unique solution. Suppose, for sake of contradiction, that x and N are not relatively prime. Then there exists a prime q dividing x and N. Since q divides N, it is equal to 2 or some q_i. However, our system of congruences guarantees that x is not divisible by 2 (by conditions (1), (2), and (3)) or any of the q_i (by conditions (4) and (5)). Therefore, x and N are relatively prime. Using Dirichlet's theorem,

there are infinitely many primes p of the form $p \equiv x \pmod{N}$, which proves the desired result.

2c. Factor m into primes $p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. Write $a_i = 2b_i + c_i$ where $c_i \in \{0, 1\}$, $1 \leq i \leq r$. Then we have

$$\begin{aligned} m &= p_1^{2b_1+c_1} p_2^{2b_2+c_2} \cdots p_r^{2b_r+c_r} \\ &= (p_1^{b_1} \cdots p_r^{b_r})^2 p_1^{c_1} \cdots p_r^{c_r} \end{aligned}$$

Let $n = p_1^{b_1} \cdots p_r^{b_r}$. Let $q_1 q_2 \cdots q_k = p_1^{c_1} \cdots p_r^{c_r}$ by making the q_j equal to the p_i for which $c_i = 1$. The q_j are distinct because the p_i are. That gives m in the desired form.

2d. Use part (c) to write m in the form $n^2 q_1 \cdots q_k$.

If m is square, then it is a quadratic residue for all primes p.

If m is not square, then $k \geq 1$. By part b, there exists infinitely many primes p for which $\left(\frac{q_1 \cdots q_k}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) \cdots \left(\frac{q_k}{p}\right) = -1$. It follows that there exist infinitely many primes p for which $\left(\frac{n^2 q_1 \cdots q_k}{p}\right) = \left(\frac{n^2}{p}\right)\left(\frac{q_1 \cdots q_k}{p}\right) = -1$ as desired.

3a. Let g be a primitive root modulo q. Consider $\zeta \equiv g^{\frac{q-1}{p}} \pmod{q}$. Then $\zeta^k \equiv g^{\frac{kq-k}{p}} \pmod{q}$, so the order of ζ is the smallest k such that $g^{\frac{kq-k}{p}} \equiv 1 \pmod{q}$. Letting $k < p$ gives an exponent less than $q - 1$, which is the smallest positive exponent for which g is one (since g is a primitive root). Hence, $\zeta^k \not\equiv 1 \pmod{q}$ when $k < p$. Letting $k = p$ gives $\zeta^p \equiv g^{q-1} \equiv 1 \pmod{q}$, so the order of ζ is exactly p.

3b. We have $\zeta^3 \equiv 1 \pmod{q}$ so $(\zeta - 1)(\zeta^2 + \zeta + 1) \equiv 0 \pmod{q}$. Now, $\zeta \not\equiv 1 \pmod{q}$ because its order is exactly 3. Hence $\zeta - 1 \not\equiv 0 \pmod{q}$, and so $\zeta^2 + \zeta + 1 \equiv 0 \pmod{q}$. Therefore, $4\zeta^2 + 4\zeta + 1 \equiv -3 \pmod{q} \Rightarrow (2\zeta + 1)^2 \equiv -3 \pmod{q}$.

4. First, consider the solutions to $x^2 \equiv 1 \pmod{p^a}$ for p an odd prime. x is a solution if and only if $p^a | x^2 - 1 \Leftrightarrow p^a | (x - 1)(x + 1)$. If $p | x - 1$, then p does not divide $x + 1$, and vice versa. Hence, either $p^a | x - 1$ or $p^a | x + 1$. Equivalently, $x \equiv 1 \pmod{p^a}$ or $x \equiv -1 \pmod{p^a}$. That gives us exactly two solutions to the equation $x^2 \equiv 1 \pmod{p^a}$.

Now consider the solutions to $x^2 \equiv 1 \pmod{2^a}$. If $a = 1$, then $x \equiv 1 \pmod{2}$ is the only solution. If $a = 2$, one finds the two solutions $x \equiv \pm 1 \pmod{4}$. Next, consider $a \geq 3$. x is a solution if and only if $2^a | (x - 1)(x + 1)$. Hence $x - 1$ and $x + 1$ are consecutive even numbers. That means one of them is divisible by 2 but not 4. Then, the other number must be divisible by 2^{a-1}. So, the only possible solutions are $x - 1 \equiv 0 \pmod{2^{a-1}}$ and $x + 1 \equiv 0 \pmod{2^{a-1}}$; i.e. $x \equiv \pm 1 \pmod{2^{a-1}}$. That gives us four distinct

possibilities modulo 2^a: $x \equiv \pm 1 \pmod{2^a}$ and $x \equiv \pm 1 + 2^{a-1} \pmod{2^a}$. Checking, we find that all four of these solutions satisfy $x^2 \equiv 1 \pmod{2^a}$. Hence, there are exactly 4 solutions when $a \geq 3$.

Factor $m = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_r^{a_r}$. Using the Chinese Remainder Theorem, $x^2 \equiv 1 \pmod{m}$ if and only if $x^2 \equiv 1 \pmod{p_i^{a_i}}$ for $1 \leq i \leq r$. Moreover, if x is different modulo any p_i, then x is different modulo m. This establishes an equivalence between the distinct solutions to $x^2 \equiv 1 \pmod{p_i^{a_i}}$ for each i and the distinct solutions to $x^2 \equiv 1 \pmod{m}$. Therefore, the number of solutions to $x^2 \equiv 1 \pmod{m}$ is $\prod_{i=1}^{r} s_i$ where s_i is the number of solutions to $x^2 \equiv 1 \pmod{p_i^{a_i}}$. The preceding arguments prove that each s_i is a power of two, so it follows that the total number of solutions to $x^2 \equiv 1 \pmod{m}$ is a power of two.

5. Define A_i to be the ith symmetric sum of the numbers $\{1, 2, \ldots, p-1\}$; that is,

$$A_i = \sum_{1 \leq j_1 < j_2 < \cdots < j_i \leq p-1} j_1 j_2 \cdots j_i$$

The polynomial $x^{p-1} - 1$ has solutions $1, 2, \ldots, p-1 \pmod{p}$ by Fermat's theorem. Hence, $x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-p+1) \pmod{p}$. Expanding the right side gives $x^{p-1} - 1 \equiv x^{p-1} - A_1 x^{p-2} + A_2 x^{p-3} - \cdots + A_{p-1} \pmod{p}$ (the last term is positive since $p-1$ is even). Comparing coefficients gives $A_i \equiv 0 \pmod{p}$ for $1 \leq i \leq p-2$, and $A_{p-1} \equiv -1 \pmod{p}$.

Next, consider the identity

$$(x-1)(x-2)\cdots(x-p+1) = x^{p-1} - A_1 x^{p-2} + A_2 x^{p-3} - \cdots + A_{p-1}$$

Substitute $x = p$ to get

$$(p-1)! = p^{p-1} - A_1 p^{p-2} + \cdots - A_{p-2} p + A_{p-1}$$

Since $A_{p-1} = (p-1)!$ it follows that

$$0 = p^{p-1} - A_1 p^{p-2} + \cdots - A_{p-2} p$$

$$0 = p^{p-2} - A_1 p^{p-3} + \cdots - A_{p-2}$$

We have $p^2 | p^{p-2}$ because $p \geq 5$, and $p | p^{p-i-2}$ and $p | A_i$ for $1 \leq i \leq p-3$. Thus, $p^{p-2} - A_1 p^{p-3} + \cdots + A_{p-3} p$ is divisible by p^2, which implies $p^2 | A_{p-2}$.

Now substitute $x = 2p$ into the previous identity. We get

$$(2p-1)\cdots(p+1) = (2p)^{p-1} - A_1 (2p)^{p-2} + \cdots - 2A_{p-2} p + A_{p-1}$$

We have $p^3 | (2p)^{p-1}$, $p^2 | (2p)^{p-i-1}$ and $p | A_i$ for $1 \leq i \leq p-3$, and $p^3 | 2A_{p-2} p$. Hence, p^3 divides all terms on the right side except A_{p-1}. Modulo p^3, we get

$$(2p-1)\cdots(p+1) \equiv A_{p-1} \pmod{p^3}$$

so

$$\frac{(2p-1)\cdots(p+1)}{(p-1)\cdots 1} \equiv 1 \pmod{p^3}$$

We have

$$\begin{aligned}\binom{2p}{p} &= \frac{2p(2p-1)\cdots(p+1)}{p(p-1)\cdots 1} \\ &= 2\frac{(2p-1)\cdots(p+1)}{(p-1)\cdots 1}\end{aligned}$$

so finally,

$$\begin{aligned}\binom{2p}{p} &\equiv 2\frac{(2p-1)\cdots(p+1)}{(p-1)\cdots 1} \pmod{p^3} \\ &\equiv 2 \pmod{p^3}\end{aligned}$$