Math 437/537—Group Work #6

Tuesday, October 22, 2024

1. Determine whether the following congruences have solutions. You don't have to find the solutions—just decide whether solutions exist. You may use the fact that 41 *and* 227 *are prime.*

(a) $x^2 \equiv 21 \pmod{41}$
(b) $x^2 \equiv 21 \pmod{41^9}$
(c) $5x^2 - x - 1 \equiv 0 \pmod{41^9}$
(d) $x^2 \equiv 137 \pmod{227}$. *Hint:* $137 - 227$ *factors more nicely than* 137.
(e) $x^2 \equiv 11 \pmod{221}$

(a) By multiplicativity, $\left(\frac{21}{41}\right) = \left(\frac{3}{41}\right)\left(\frac{7}{41}\right)$. Since $41 \equiv 1 \pmod 4$, quadratic reciprocity results in no sign changes: $\left(\frac{3}{41}\right) = \left(\frac{41}{3}\right)$ and $\left(\frac{7}{41}\right) = \left(\frac{41}{7}\right)$. By periodicity, $\left(\frac{41}{3}\right) = \left(\frac{2}{3}\right) = -1$ (by brute force, or since $3 \equiv \pm 3 \pmod 8$, for example), while $\left(\frac{41}{7}\right) = \left(\frac{-1}{7}\right) = -1$ (by brute force, or since $7 \equiv 3 \pmod 4$). Therefore $\left(\frac{21}{41}\right) = \left(\frac{2}{3}\right)\left(\frac{-1}{7}\right) = (-1)(-1) = 1$. We conclude that $x^2 \equiv 21 \pmod{41}$ does have solutions.

(b) The derivative of the polynomial $f(x) = x^2 - 21$ is simply $2x$. Therefore the only way a root r of $f(x)$ modulo m could be singular is if $2r \equiv 0 \pmod m$; if m is odd, then 2 is invertible modulo m, and this is equivalent to $r \equiv 0 \pmod m$. In this case, $f(0) = -21 \not\equiv 0 \pmod{41}$, and so the two roots of $f(x) \pmod{41}$ that we found in part (a) are nonsingular. Hensel's lemma then tells us that there are exactly two roots of $f(x) \pmod{41^j}$ for every $j \ge 1$.

(c) The discriminant of $5x^2 - x - 1$ equals $(-1)^2 - 4 \cdot 5 \cdot (-1) = 21$, which is a square modulo 41^9 by part (b); therefore $5x^2 - x - 1 \equiv 0 \pmod{41^9}$ has solutions. (More concretely: since $(20, 41^9) = 1$, the congruence $5x^2 - x - 1 \equiv 0 \pmod{41^9}$ is equivalent to $20(5x^2 - x - 1) \equiv 0 \pmod{41^9}$, or $(10x - 1)^2 - 21 \equiv 0 \pmod{41^9}$. Therefore the solutions to $y^2 \equiv 21 \pmod{41^9}$ can be transformed, via $10x - 1 \equiv y \pmod{41^9}$ or equivalently $x \equiv 10^{-1}(y + 1) \pmod{41^9}$, into solutions to the original congruence.)

(d) By periodicity and then multiplicativity,

$$\left(\frac{137}{227}\right) = \left(\frac{-90}{227}\right) = \left(\frac{-1}{227}\right)\left(\frac{2}{227}\right)\left(\frac{3^2}{227}\right)\left(\frac{5}{227}\right).$$

Since $227 \equiv 3 \pmod 4$ and $227 \equiv 3 \pmod 8$, we have $\left(\frac{-1}{227}\right) = -1$ and $\left(\frac{2}{227}\right) = -1$; we also have $\left(\frac{3^2}{p}\right) = 1$ for any odd prime p. Therefore $\left(\frac{137}{227}\right) = (-1)(-1)1\left(\frac{5}{227}\right) = \left(\frac{5}{227}\right)$. Since $5 \equiv 1 \pmod 4$, quadratic reciprocity gives $\left(\frac{5}{227}\right) = \left(\frac{227}{5}\right)$; periodicity then gives $\left(\frac{227}{5}\right) = \left(\frac{2}{5}\right) = -1$ by the formula for $\left(\frac{2}{p}\right)$. We conclude that $\left(\frac{137}{227}\right) = -1$, and so $x^2 \equiv 137 \pmod{227}$ has no solutions.

(e) First, here is an *incorrect* solution: Since $221 \equiv 1 \pmod 4$, quadratic reciprocity gives $\left(\frac{11}{221}\right) = \left(\frac{221}{11}\right)$; periodicity then gives $\left(\frac{221}{11}\right) = \left(\frac{1}{11}\right) = 1$, and so there are solutions. *(Wrong!)*

Why is that reasoning incorrect? Because $221 = 13 \times 17$ is not prime! Indeed, the congruence $x^2 \equiv 11 \pmod{221}$ has solutions if and only if both the congruences $x^2 \equiv 11 \pmod{13}$ and $x^2 \equiv 11 \pmod{17}$ have solutions. But it turns out that neither congruence has solutions. For example, since $13 \equiv 1 \pmod 4$, quadratic reciprocity gives $\left(\frac{11}{13}\right) = \left(\frac{13}{11}\right)$; periodicity then gives $\left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) = -1$ since $11 \equiv 3 \pmod 8$. (Alternatively, by periodicity and multiplicativity, $\left(\frac{11}{13}\right) = \left(\frac{-2}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{2}{13}\right) = 1(-1)$ since $13 \equiv 1 \pmod 4$ and $13 \equiv 5 \pmod 8$.) Similarly, our algorithm yields

$$\left(\frac{11}{17}\right) = \left(\frac{17}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = (-1)\left(-\left(\frac{11}{3}\right)\right) = \left(\frac{2}{3}\right) = -1.$$

2.

(a) *For which primes p does there exist an integer x such that $x^2 \equiv 5 \pmod p$? State your answer in terms of the last digit of p.*

(b) *For which primes p does there exist an integer x such that $x^2 \equiv -5 \pmod p$? State your answer in terms of the last two digits of p.*

We note that when $p = 2$, both congruences have the solution $x = 1$, while when $p = 5$, both congruences have the solution $x = 0$. During the proofs, therefore, we may assume $p \neq 2, 5$.

(a) Since $5 \equiv 1 \pmod 4$, quadratic reciprocity tells us that $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ for any odd prime $p \neq 5$. It's easy to establish (by brute force even) that $\left(\frac{1}{5}\right) = 1$, $\left(\frac{2}{5}\right) = -1$, $\left(\frac{3}{5}\right) = -1$, and $\left(\frac{4}{5}\right) = 1$. Therefore $\left(\frac{5}{p}\right) = 1$ when $p \equiv \pm 1 \pmod 5$, while $\left(\frac{5}{p}\right) = -1$ when $p \equiv \pm 2 \pmod 5$. Note that these two cases correspond to the last digit being 1 or 9, and 3 or 7, respectively. Therefore $x^2 \equiv 5 \pmod p$ has a solution when the last digit of p is 1, 2, 5, or 9 but not when the last digit of p is 3 or 7.

(b) We know that $\left(\frac{-1}{p}\right) = 1$ when $p \equiv 1 \pmod 4$ and $\left(\frac{-1}{p}\right) = -1$ when $p \equiv 3 \pmod 4$. Therefore $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = 1$ in precisely two cases: either $p \equiv \pm 1 \pmod 5$ and $p \equiv 1 \pmod 4$, or else $p \equiv \pm 2 \pmod 5$ and $p \equiv 3 \pmod 4$. Either by doing a bunch of little Chinese remainder calculations, or else just going through all the reduced residue classes modulo 20 by hand, we see that these cases correspond to the residue classes $p \equiv 1, 3, 7, 9 \pmod{20}$. We conclude, amazingly, that the congruence $x^2 \equiv -5 \pmod p$ has solutions if and only if the second-to-last digit of p is even! (This works for single digit primes too, as long as we call the second-to-last digit 0.)

3. *Let p be an odd prime, and let g be a primitive root modulo p, so that any a that is not a multiple of p can be written as $a \equiv g^k \pmod p$ for some integer k. Prove that $\left(\frac{a}{p}\right) = 1$ if k is even while $\left(\frac{a}{p}\right) = -1$ if k is odd.*

There are multiple ways to see this. If we set $k = 2j + \varepsilon$ with $\varepsilon \in \{0, 1\}$, we can use Euler's criterion to write

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv (g^k)^{(p-1)/2} = (g^{p-1})^j \left(g^{(p-1)/2}\right)^\varepsilon \equiv 1^j(-1)^\varepsilon \pmod p.$$

(Note that $g^{(p-1)/2}$ is a solution to $x^2 \equiv 1 \pmod p$ that is not congruent to $1 \pmod p$, which by Lemma 2.10 forces $g^{(p-1)/2} \equiv -1 \pmod p$.) Both integers $\left(\frac{a}{p}\right)$ and $(-1)^\varepsilon$ are either 1 or -1, and so they differ by at most 2; consequently, no odd prime can divide their difference unless that difference equals 0. We conclude that $\left(\frac{a}{p}\right) = (-1)^\varepsilon$, which is what we want to prove.

Alternatively, if $k = 2j$ is even, then clearly $x^2 \equiv g^{2j} \pmod p$ has solutions, namely $x \equiv \pm g^j \pmod p$; therefore $\left(\frac{a}{p}\right) = 1$ when $a \equiv g^k \pmod p$ with k even. And the $\frac{p-1}{2}$ even integers $\{2, 4, \dots, p-1\}$ give rise to distinct residue classes $g^2, g^4, \dots, g^{p-1} \pmod p$ (or else the quotient of two of them would be $1 \pmod{p}$, contradicting the fact that the order of g is $p-1$) which are all quadratic residues; but we know that there are only $\frac{p-1}{2}$ quadratic residues $\pmod{p}$. Therefore the other $\frac{p-1}{2}$ integers $\{1, 3, \ldots, p-2\}$, which are all odd, must give rise to quadratic nonresidues $g^1, g^3, \ldots, g^{p-2} \pmod{p}$.

Remark: remember our guiding principle that if a modulus m has primitive roots, then multiplication modulo m is just addition modulo $\phi(m)$ in disguise. In this case, the multiplication statement "even powers of a primitive root are squares of something else $\pmod{p}$, while odd powers of a primitive root are nonsquares" is isomorphic to the addition statement "even multiples of 1 are doubles of something else $\pmod{p-1}$, while odd multiples of 1 are not doubles"; and this latter statement is obvious, since $p-1$ is even. (Note, by the way, that if q is odd, then everything is a double of something $\pmod{q}$!)