Math 25: Solutions to Homework #8

(11.1 # 20) Find all solutions of the congruence $x^2 \equiv 58 \pmod{77}$.

If $x^2 \equiv 58 \pmod{77}$ then $x^2 \equiv 58 \equiv 2 \pmod 7$ and $x^2 \equiv 58 \equiv 3 \pmod{11}$. The two solutions to the first congruence are $x \equiv 3$ or $4 \pmod 7$, and the solutions to the second congruence are $x \equiv 5$ or $6 \pmod{11}$. We use the Chinese Remaider Theorem to find the unique solution mod 77 for the two sets of congruences

$$\begin{aligned} x &\equiv 4 \pmod 7 \\ x &\equiv 5 \pmod{11}, \end{aligned}$$

and

$$\begin{aligned} x &\equiv 4 \pmod 7 \\ x &\equiv 6 \pmod{11}. \end{aligned}$$

These are 60 and 39 mod 77. Then the four solutions are 60, 39, $77 - 60 = 17$, and $77 - 39 = 38$.

(11.2 # 2) Show that if p is an odd prime, then

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

First, $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ if $p \equiv 1 \pmod 4$ and $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ if $p \equiv 3 \pmod 4$. Then $\left(\frac{p}{3}\right) = 1$ if $p \equiv 1 \pmod 3$ and $\left(\frac{p}{3}\right) = -1$ if $p \equiv 2 \pmod 3$. Collecting the cases, we see that $\left(\frac{3}{p}\right) = 1$ if $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 3$, or if $p \equiv 3 \pmod 4$ and $p \equiv 2 \pmod 3$. These cases correspond to $p \equiv \pm 1 \pmod{12}$. Then $\left(\frac{3}{p}\right) = -1$ if either $p \equiv 1 \pmod 4$ and $p \equiv 2 \pmod 3$, or if $p \equiv 3 \pmod 4$ and $p \equiv 1 \pmod 3$. These cases correspond to $p \equiv \pm 5 \pmod{12}$.

(11.2 # 4) Find a congruence describing all primes for which 5 is a quadratic residue.

Since $5 \equiv 1 \pmod 4$, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. Then $\left(\frac{p}{5}\right) = 1$ exactly when $p \equiv 1$ or $4 \pmod 5$, so 5 is a quadratic residue for all odd primes $p \equiv \pm 1 \pmod 5$.

(11.2 # 10) Show that Euler's form of the law of quadratic recprocity implies the law of quadratic reciprocity as stated in Theorem 11.7.

Euler's form of theorem says that if p is an odd integer and a is an integer coprime to p, then if q is prime with $p \equiv \pm q \pmod{4a}$, that $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

Let p and q be distinct odd primes. Then $p \equiv \pm q \pmod 4$ since each is either 1 or 3 mod 4. First suppose that $p \equiv q \pmod 4$. Then $p = q + 4a$ for some integer a, so $p \equiv q$

(mod $4a$), and $p \nmid a$, otherwise $p = q$. So by Euler's version of the theorem, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. Then

$$\left(\frac{p}{q}\right) = \left(\frac{q+4a}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{4}{q}\right)\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{p-q}{p}\right) = \left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right).$$

Then if $p \equiv 1 \pmod 4$, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ and if $p \equiv 3 \pmod 4$ then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Now suppose that $p \equiv -q \pmod 4$. Then $p = -q + 4a$ for some integer a and hence $p \equiv -q \pmod{4a}$ and $p \nmid a$. Then using Euler's version as before,

$$\left(\frac{p}{q}\right) = \left(\frac{-q+4a}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{4a-p}{q}\right) = \left(\frac{q}{p}\right).$$

Putting the three possibilities together, we have

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= \begin{cases} 1 & \text{if either } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \text{ or both} \\ -1 & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases} \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.\end{aligned}$$

(11.3 # 2) For which positive integers n that are relatively prime to 15 does the Jacobi symbol $\left(\frac{15}{n}\right)$ equal 1?

Since $15 \equiv 3 \pmod 4$, then $\left(\frac{15}{n}\right) = \left(\frac{n}{15}\right)$ if $n \equiv 1 \pmod 4$ and $\left(\frac{15}{n}\right) = -\left(\frac{n}{15}\right)$ if $n \equiv 3 \pmod 4$. Then $\left(\frac{n}{15}\right) = \left(\frac{n}{3}\right)\left(\frac{n}{5}\right)$. The only quadratic residue mod 3 is 1, and the residues mod 5 are 1 and 4. Then $\left(\frac{15}{n}\right) = 1$ if

(a) $n \equiv 1 \pmod 4$, $n \equiv 1 \pmod 3$ and $n \equiv 1$ or $4 \pmod 5$, which yields $n \equiv 1$ or $49 \pmod{60}$,
(b) $n \equiv 1 \pmod 4$, $n \equiv 2 \pmod 3$ and $n \equiv 2$ or $3 \pmod 5$, which yields $n \equiv 17$ or $53 \pmod{60}$,
(c) $n \equiv 3 \pmod 4$, $n \equiv 1 \pmod 3$ and $n \equiv 2$ or $3 \pmod 5$, which yields $n \equiv 7$ or $43 \pmod{60}$, and
(d) $n \equiv 3 \pmod 4$, $n \equiv 2 \pmod 3$ and $n \equiv 1$ or $4 \pmod 5$, which yields $n \equiv 11$ or $59 \pmod{60}$.

(11.3 # 6) Find all the pseudo-squares modulo 35.

An integer a is a pseudo-square modulo 35 if $\left(\frac{a}{35}\right) = 1$ but $x^2 \equiv a \pmod{35}$ has no solution. Since $\left(\frac{a}{35}\right) = \left(\frac{a}{5}\right)\left(\frac{a}{7}\right)$, this occurs if a is a non-residue mod 5 and 7. Then $a \equiv 2$ or $3 \pmod 5$ and $a \equiv 3, 5$ or $6 \pmod 7$. The six residue classes mod 35 satisfying these conditions are 3, 12, 13, 17, 27, and 33.

(11.4 # 4) Show that if n is an Euler pseudoprime to the base b, then n is also an Euler pseudoprime to the base $n - b$.

If n is an Euler pseudoprime then $\left(\frac{b}{n}\right) \equiv b^{\frac{n-1}{2}} \pmod{n}$. First,

$$\left(\frac{n-b}{n}\right) = \left(\frac{-b}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{b}{n}\right).$$

Then

$$\left(\frac{-1}{n}\right)\left(\frac{b}{n}\right) \equiv (-1)^{\frac{n-1}{2}} b^{\frac{n-1}{2}} \equiv (-b)^{\frac{n-1}{2}} \equiv (n-b)^{\frac{n-1}{2}} \pmod{n}.$$

(11.4 # 6) Show that if $n \equiv 5 \pmod{12}$ and n is an Euler pseudoprime to the base 3, then n is a strong pseudoprime to the base 3.

Suppose that $n \equiv 5 \pmod{12}$ and that $\left(\frac{3}{n}\right) \equiv 3^{\frac{n-1}{2}} \pmod{n}$. Then since $n \equiv 1 \pmod{4}$ we see that $\left(\frac{3}{n}\right) = \left(\frac{n}{3}\right)$, and since $n \equiv 2 \pmod{3}$, this is equal to $\left(\frac{2}{3}\right)$, which is -1. That is,

$$3^{\frac{n-1}{2}} \equiv -1 \pmod{n},$$

and thus n passes Miller's test to the base 3.

(13.1 # 2) Show that if x, y, z is a primitive Pythagorean triple, then either x or y is divisible by 3.

Let (x, y, z) be a primitive Pythagorean triple, and suppose that three divides neither x nor y. Then $x^2 \equiv y^2 \equiv 1 \pmod{3}$, and thus we must have $z^2 \equiv x^2 + y^2 \equiv 2 \pmod{3}$. But $z^2 \equiv 2 \pmod{3}$ has no solution, a contradiction. Thus three divides either x or y.

(13.1 # 12) Find formulas for the integers of all Pythagorean triples x, y, z with $z = y + 1$.

Suppose (x, y, z) is a primitive Pythagorean triple. Then there are integers m and n such that $x = m^2 - n^2$, $y = 2mn$, and $z = m^2 + n^2$. So with our hypothesis of $z = y + 1$, we have $m^2 + n^2 = 2mn + 1$. That is,

$$\begin{aligned} 1 &= m^2 - 2mn + n^2 \\ &= (m-n)^2. \end{aligned}$$

Since we know $m - n > 0$, we now see that $m - n = 1$, and thus $m = n + 1$. Thus all primitive triples with $z = y + 1$ have the form, for $n \geq 1$,

$$x = (n+1)^2 - n^2 = 2n + 1,$$

$$y = 2(n+1)n = 2n^2 + 2n,$$

$$z = (n+1)^2 + n^2 = 2n^2 + 2n + 1.$$

Now suppose that (x, y, z) is any Pythagorean triple with $z = y + 1$. Then $(y, z) = 1$, so $(x, y, z) = 1$, and hence (x, y, z) is in fact primitive.

(13.1 # 18) Find the length of the sides of all right triangles, where the sides have integer lengths and the area equals the perimeter.

Set $d = (x, y, z)$. Then we have $x = d(m^2 - n^2)$, $y = 2mnd$, and $z = d(m^2 + n^2)$, for some integers m and n. We need the area of the right triangle to be equal to the perimeter. That is, $\frac{1}{2}xy = x + y + z$. Substituting, we find

$$\begin{aligned}\frac{1}{2}d(m^2 - n^2)(2mnd) &= d(m^2 - n^2) + 2mnd + d(m^2 + n^2)\\ d^2mn(m^2 - n^2) &= d(m^2 - n^2 + 2mn + m^2 + n^2)\\ d^2mn(m^2 - n^2) &= d(2m^2 + 2mn)\\ dn(m - n) &= 2.\end{aligned}$$

Since $m - n \neq 2$, we have $m - n = 1$, or $m = n + 1$. Thus we have two cases. If $n = 1$ and $d = 2$, then $m = 2$ and $(x, y, z) = (6, 8, 10)$. If $n = 2$ and $d = 1$, then $m = 3$ and $(x, y, z) = (5, 12, 13)$. These are the only possibilites.