18.781 Problem Set 8 - Fall 2008
Due Tuesday, Nov. 4 at 1:00

1. Evaluate the following Legendre symbols:

   (a) $\left(\frac{85}{101}\right)$

   (b) $\left(\frac{29}{541}\right)$

   (c) $\left(\frac{101}{1987}\right)$.

   It is important to check each number for primality and to check each application of quadratic reciprocity with the two primes' residues $\mod 4$.

   (a) $\left(\frac{85}{101}\right) = \left(\frac{5}{101}\right)\left(\frac{17}{101}\right) = \left(\frac{101}{5}\right)\left(\frac{101}{17}\right) = \left(\frac{1}{5}\right)\left(\frac{16}{17}\right) = 1.$

   (b) $\left(\frac{29}{541}\right) = \left(\frac{541}{29}\right) = \left(\frac{19}{29}\right) = \left(\frac{29}{19}\right) = \left(\frac{10}{19}\right) = \left(\frac{2}{19}\right)\left(\frac{5}{19}\right)$
   $= (-1)^{\frac{19^2-1}{8}}\left(\frac{19}{5}\right) = -\left(\frac{4}{5}\right) = -1.$

   (c) $\left(\frac{101}{1987}\right) = \left(\frac{1987}{101}\right) = \left(\frac{68}{101}\right) = \left(\frac{4}{101}\right)\left(\frac{17}{101}\right) = 1 \cdot 1 = 1.$

2. (Niven 3.2.4abce) Determine which of the following are solvable (the moduli are all primes):

   (a) $x^2 \equiv 5 \pmod{227}$

   (b) $x^2 \equiv 5 \pmod{229}$

   (c) $x^2 \equiv -5 \pmod{227}$

   (d) $x^2 \equiv 7 \pmod{1009}$.

   First, some relevant Legendre symbol calculations:

   (a) $\left(\frac{5}{227}\right) = \left(\frac{227}{5}\right) = \left(\frac{2}{5}\right) = -1.$

   (b) $\left(\frac{5}{229}\right) = \left(\frac{229}{5}\right) = \left(\frac{4}{5}\right) = 1.$

   (c) $\left(\frac{-5}{227}\right) = \left(\frac{-1}{227}\right)\left(\frac{5}{227}\right) = (-1)^{\frac{227-1}{2}} \cdot (-1) = (-1)(-1) = 1.$

   (d) $\left(\frac{7}{1009}\right) = \left(\frac{1009}{7}\right) = \left(\frac{1}{7}\right) = 1.$

   So we have that the first equation is not solvable, but the rest are, by the value of the associated Legendre symbols.

3. Prove that if $p \mid (n^2 - 5)$ for some integer n, then $p \equiv 1$ or $4 \pmod 5$.

   We are given $p|(n^2 - 5)$ for some $n \in \mathbb{Z}$. This gives that $n^2 \equiv 5 \pmod p$, so 5 is a quadratic residue mod p. But then we have, by quadratic reciprociy, that

$$1 = \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 5 \\ -1 & \text{if } p \equiv \pm 2 \pmod 5. \end{cases}$$

So we get that $p \equiv 1$ or $4 \pmod 5$. (We actually must assume that $p \neq 5$ as well)

4. Show that if $p \equiv 3 \pmod 4$, then $x = a^{(p+1)/4}$ is a solution to $x^2 \equiv a \pmod p$.

   (*Correction:*) For this problem, we also need to assume that $\left(\frac{a}{p}\right) = 1$, since otherwise we couldn't possibly find a solution for $x^2 \equiv a \pmod p$.
   So with that extra assumption, we have that

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

   Then multiplying by a, we get

$$a \equiv a^{\frac{p+1}{2}} \equiv \left(a^{\frac{p+1}{4}}\right)^2 \pmod p.$$

   Since $p \equiv 3 \pmod 4$, this inner exponent is an integer, and so the x above does satisfy the equation.

5. (Niven 3.2.6) Determine whether $x^2 \equiv 150 \pmod{1009}$ is solvable.

   So here we clearly want to calculate $\left(\frac{150}{1009}\right)$, and this makes sense since 1009 is prime.

$$\left(\frac{150}{1009}\right) = \left(\frac{2}{1009}\right)\left(\frac{3}{1009}\right)\left(\frac{25}{1009}\right) = (-1)^{\frac{1009^2-1}{8}}\left(\frac{1009}{3}\right) \cdot 1 = 1 \cdot \left(\frac{1}{3}\right) = 1.$$

   Hence the equation is solvable.

6. (Niven 3.2.8 & 3.2.9)

   (a) Characterize all primes p such that $\left(\frac{10}{p}\right) = 1$.

   We have that

$$\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{p^2-1}{8}}\left(\frac{p}{5}\right).$$

   Now, we also have the following calculations of each factor.

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8, \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases} \qquad \left(\frac{p}{5}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 5, \\ -1 & \text{if } p \equiv \pm 2 \pmod 5. \end{cases}$$

   Now we can combine these into one set of congruence classes mod $5\dot{8} = 40$ using CRT. We get

$$\left(\frac{10}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40}, \\ -1 & \text{if } p \equiv \pm 7, \pm 11, \pm 17, \pm 19 \pmod{40}. \end{cases}$$

   (b) Characterize all primes p such that $\left(\frac{5}{p}\right) = -1$.

We have, since $5 \equiv 1 \pmod 4$, that

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right).$$

So the primes with $\left(\frac{5}{p}\right) = -1$ are exactly those primes that are congruent to 2 or 3 mod 5, except for $p = 2$.

7. Use quadratic reciprocity to evaluate $(\frac{7}{p})$ based on the residue class of p mod 28.

   Quadratic reciprocity gives

$$\left(\frac{7}{p}\right) = (-1)^{\frac{7-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{7}\right) = \left((-1)^3\right)^{\cdot\frac{p-1}{2}}\left(\frac{p}{7}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{7}\right).$$

   As above, we find the values for each factor.

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases} \qquad \left(\frac{p}{7}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 2, 4 \pmod 7, \\ -1 & \text{if } p \equiv 3, 5, 6 \pmod 7. \end{cases}$$

   Now we can combine them using CRT.

$$\left(\frac{7}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1, \pm 3, \pm 9 \pmod{28}, \\ -1 & \text{if } p \equiv \pm 5, \pm 11, \pm 13 \pmod{28}. \end{cases}$$

8. In this problem you will produce an alternative proof of the formula for $(\frac{2}{p})$ when p is an odd prime.

   (a) Prove that $2 \cdot 4 \cdots (p-3) \cdot (p-1) \equiv \left(\frac{2}{p}\right) \cdot \left(\frac{p-1}{2}\right)! \pmod p$.

   So we want to evaluate

$$\begin{aligned} 2 \cdot 4 \cdot 6 \cdots (p-3)(p-1) &= (2\cdot 1)(2\cdot 2)(2\cdot 3)(\cdots)(2\cdot(\frac{p-1}{2})) \\ &= 2^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \\ &\equiv \left(\frac{2}{p}\right) \cdot \left(\frac{p-1}{2}\right)! \pmod p. \end{aligned}$$

   (b) If u is the number of terms in the product that are larger than $\frac{p-1}{2}$, prove that

$$2 \cdot 4 \cdots (p-3) \cdot (p-1) \equiv (-1)^u \left(\frac{p-1}{2}\right)! \pmod p.$$

   This is a similar calculation to those done in class. We have to reflect the numbers in the left hand side product that are greater than $\frac{p-1}{2}$ about this line. Note that this reflection is done by taking a number x and sending it to $p - x$. Since the numbers x all start out even, and we are subtracting them from an odd p, we get an odd number between 1 and $\frac{p-1}{2}$. So none of the reflections land on numbers already there, which are all even. Also, there are $\frac{p-1}{2}$ numbers after all the reflections, so we have a reordering of exactly $\left(\frac{p-1}{2}\right)!$. Each reflection changed the sign of the product however, so we have exactly the equation above.

(c) Compare (a) and (b) to derive the formula for $(\frac{2}{p})$; you will need to separate into cases based on the value of p mod 8.

So now we have to find a formula for u. This is the number of even numbers between $\frac{p-1}{2}$ and p, not inclusive. The number of even numbers less than p is clearly just $\frac{p-1}{2}$, so we have to subtract the number of evens less than or equal to $\frac{p-1}{2}$ which gives

$$u = \frac{p-1}{2} - \lfloor \frac{p-1}{4} \rfloor.$$

Then we can find a formula for $(-1)^u$, which is

$$(-1)^u = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8, \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

So by our two evaluations of the product, we can easily see that we get the normal formula for $\left(\dfrac{2}{p}\right)$, namely exactly the formula above for $(-1)^u$.

9. (Niven 3.3.1) Evaluate using quadratic reciprocity for Jacobi symbols:

(a) $\left(\dfrac{-23}{83}\right)$

(b) $\left(\dfrac{51}{71}\right)$

(c) $\left(\dfrac{71}{73}\right)$

(d) $\left(\dfrac{-35}{97}\right)$.

(a) $\left(\dfrac{-23}{85}\right) = \left(\dfrac{-1}{85}\right)\left(\dfrac{23}{85}\right) = 1\left(\dfrac{85}{23}\right) = \left(\dfrac{16}{23}\right) = 1.$

(b) $\left(\dfrac{51}{71}\right) = -\left(\dfrac{20}{51}\right) = -\left(\dfrac{4}{51}\right)\left(\dfrac{5}{51}\right) = -\left(\dfrac{51}{5}\right) = -\left(\dfrac{1}{5}\right) = -1.$

(c) $\left(\dfrac{71}{73}\right) = \left(\dfrac{73}{71}\right) = \left(\dfrac{2}{71}\right) = 1.$

(d) $\left(\dfrac{-35}{97}\right) = \left(\dfrac{-1}{97}\right)\left(\dfrac{35}{97}\right) = 1 \cdot \left(\dfrac{97}{35}\right) = \left(\dfrac{27}{35}\right) = -\left(\dfrac{35}{27}\right) = -\left(\dfrac{8}{27}\right) = -\left(\dfrac{2}{27}\right) = -(-1) = 1.$

10. (Niven 3.3.7, 3.3.8 & 3.3.9)

(a) For which primes are there solutions to $x^2 + y^2 \equiv 0 \pmod p$ with $(x, p) = (y, p) = 1$?

The answer turns out to be all primes with $\left(\dfrac{-1}{p}\right) = 1$. This is because if (x, y) is a solution to the equation above, then $x\overline{y}$ is a square root of -1 mod p, which can be seen easily by multiplying the equation by $(\overline{y})^2$. So a solution of the equation implies that $\left(\dfrac{-1}{p}\right) = 1$. Conversely, if $\left(\dfrac{-1}{p}\right) = 1$, then there is some z with $z^2 \equiv -1$, so $z^2 + (1)^2 \equiv 0 \pmod p$.

These primes are exactly the primes not conguent to 3 mod 4.

(b) For which prime powers are there solutions to $x^2 + y^2 \equiv 0 \pmod{p^n}$ with $(x, p) = (y, p) = 1$?

If there is a solution for a prime power, it is certainly a solution for the prime, so the only prime powers that could possibly have solutions are those not congruent to 3 mod 4. To check, we can just try to lift our square root of -1. This is lifting the root of the polynomial $x^2 + 1$, whose derivative is $2x$. Clearly the only prime for which the root of the polynomial is singular is when $p = 2$. Otherwise, a root of $2x$ must just be zero, which is clearly not a root of x^2+1. So for any odd prime, that is, the ones congruent to 1 mod 4, Hensel's Lemma guarantees that there is a square root of -1 mod p^n for all n.

The last case is $p = 2$. We can check that mod $2^2 = 4$, there is no square root of -1. In particular, there is no solution of $x^2 + y^2 \equiv 0 \pmod 4$ with neither x nor y congruent to 0, since the only nonzero squares are 1. So the prime powers that work are exactly the set

$$\{p^n \mid p \equiv 1 \pmod 4, n \in \mathbb{Z}^+\} \cup \{2\}.$$

(Bonus) For which integers n are there solutions to $x^2 + y^2 \equiv 0 \pmod n$ with $(x, n) = (y, n) = 1$?

(Bonus) (Niven 3.2.16) Show that if $p = 2^{2^n} + 1$ is prime, then 3 is a primitive root modulo p, and that 5 and 7 are primitive roots when $n > 1$.