MTH 505: Number Theory — Spring 2020
Homework 4 — Drew Armstrong

Problem 1. Computing Legendre Symbols. Use Quadratic Reciprocity and its supplements to compute the Legendre symbol (47/67). [Hint: 47 and 67 are prime.]

$$
\begin{aligned}
\left(\frac{47}{67}\right) &= \left(\frac{67}{47}\right)(-1)^{\frac{47-1}{2}\frac{67-1}{2}} = -\left(\frac{67}{47}\right) && \text{QR} \\
&= -\left(\frac{20}{47}\right) = -\left(\frac{2^2 5}{47}\right) && 67 = 20 \bmod 4 \\
&= -\left(\frac{2}{47}\right)^2\left(\frac{5}{47}\right) = -(\pm 1)^2\left(\frac{5}{47}\right) = -\left(\frac{5}{47}\right) && \text{multiplicative} \\
&= -\left(\frac{47}{5}\right)(-1)^{\frac{5-1}{2}\frac{47-1}{2}} = -\left(\frac{47}{5}\right) && \text{QR} \\
&= -\left(\frac{2}{5}\right) && 47 = 2 \bmod 5 \\
&= -(-1) = +1 && 2 \text{ is nonsquare mod } 5
\end{aligned}
$$

We conclude that 47 is square mod 67. Since 67 is prime this means that 47 has exactly two square roots mod 67. My computer says that $\sqrt{47} = 28$ or $39 \bmod 67$.

Problem 2. Quadratic Character of -2. Let p be an odd prime. We proved in class that

$$
\left(\frac{-1}{p}\right) = \begin{cases} +1 & \text{if } p = 1 \bmod 4, \\ -1 & \text{if } p = 3 \bmod 4, \end{cases} \quad \text{and} \quad \left(\frac{2}{p}\right) = \begin{cases} +1 & \text{if } p = 1,7 \bmod 8, \\ -1 & \text{if } p = 3,5 \bmod 8. \end{cases}
$$

Compute the Legendre symbol $(-2/p)$. [Hint: We know that $(-2/p) = (-1/p)(2/p)$.]

Since $(-2/p) = (-1/p)(2/p)$ we see that

$$
\begin{aligned}
\left(\frac{-2}{p}\right) &= \begin{cases} +1 & p = 1 \bmod 4 \text{ and } p = 1,7 \bmod 8 \\ +1 & p = 3 \bmod 4 \text{ and } p = 3,5 \bmod 8 \\ -1 & p = 1 \bmod 4 \text{ and } p = 3,5 \bmod 8 \\ -1 & p = 3 \bmod 4 \text{ and } p = 1,7 \bmod 8 \end{cases} \\
&= \begin{cases} +1 & p = 1 \bmod 8 \\ +1 & p = 3 \bmod 8 \\ -1 & p = 5 \bmod 8 \\ -1 & p = 7 \bmod 8 \end{cases} = \begin{cases} +1 & p = 1,3 \bmod 8 \\ -1 & p = 5,7 \bmod 8 \end{cases}
\end{aligned}
$$

Problem 3. Quadratic Character of 3. For any odd prime p, Quadratic Reciprocity says

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

Use this to compute the Legendre symbol $(3/p)$. [Hint: First observe that $(p/3) = 1$ when $p = 1$ mod 3 and $(p/3) = -1$ when $p = 2$ mod 3. Observe also that $(-1)^{(p-1)/2} = 1$ when $p = 1$ mod 4 and $(-1)^{(p-1)/2} = -1$ when $p = 3$ mod 4. Now use the Chinese Remainder Theorem.]

First we write down the CRT bijection $(x \bmod 12) \mapsto (x \bmod 3, x \bmod 4)$ from the group $(\mathbb{Z}/12\mathbb{Z})^\times$ to the group $(\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/4\mathbb{Z})^\times$:

$x \bmod 12$	$(x \bmod 3, x \bmod 4)$
1	$(1,1)$
5	$(2,1)$
7	$(1,3)$
11	$(2,3)$

Next, since 1 is square mod 3 and 2 is nonsquare mod 3 we observe that[1]

$$\left(\frac{p}{3}\right) = \begin{cases} +1 & p = 1 \bmod 3 \\ -1 & p = 2 \bmod 3 \end{cases}$$

Then since $(3/p) = (p/3)(-1)^{\frac{p-1}{2}}$, we combine these two facts to obtain

$$\begin{aligned}\left(\frac{3}{p}\right) &= \begin{cases} +1 & p = 1 \bmod 3 \text{ and } p = 1 \bmod 4 \\ +1 & p = 2 \bmod 3 \text{ and } p = 3 \bmod 4 \\ -1 & p = 1 \bmod 3 \text{ and } p = 3 \bmod 4 \\ -1 & p = 2 \bmod 4 \text{ and } p = 1 \bmod 4 \end{cases} \\ &= \begin{cases} +1 & p = 1 \bmod 12 \\ +1 & p = 11 \bmod 12 \\ -1 & p = 7 \bmod 12 \\ -1 & p = 5 \bmod 12 \end{cases} = \begin{cases} +1 & p = 1, 11 \bmod 12 \\ -1 & p = 5, 7 \bmod 12 \end{cases}\end{aligned}$$

[Remark: More generally, it can be proved that for odd primes $p \neq q$ we have

$$\left(\frac{q}{p}\right) = +1 \quad \Leftrightarrow \quad p = \pm\beta^2 \bmod 4q \text{ for some odd integer } 1 \leqslant \beta < \sqrt{4q}.$$

But this is difficult to prove because it is logically equivalent to QR.][2]

Problem 4. Infinitely Many Primes $= 3$ mod 8. Let $p_1, \ldots, p_k$ be a set of primes such that $p_i = 3$ mod 8 for all i, and consider the number

$$N = (p_1 \cdots p_k)^2 + 2.$$

We will use this to show that there exists a prime number $p = 3$ mod 8 that is not in the list.

(a) Show that $N = 3$ mod 8.
(b) Show that every prime divisor $p|N$ satisfies $p = 1$ or $p = 3$ mod 8. [Hint: If $p|N$ then show that $-2 = (p_1 \cdots p_k)^2$ mod p. Now use Problem 2.]
(c) Combine (a) and (b) to show that there exists a prime divisor $p|N$ satisfying $p = 3$ mod 8. [Hint: If all prime divisors $= 1$ mod 8 then $N = 1$ mod 8.]
(d) Show that the prime p from part (c) is not in the list $p_1, \ldots, p_k$. [Hint: $N = 2$ mod p_i.]

[1] We assume that $p \neq 3$.
[2] See David Cox, *Primes of the form $x^2 + ny^2$*, page 14.

(a): (The original version of this said that $N = 2 \bmod 8$, which is wrong. Sorry.) Since $p_i = 3 \bmod 8$ for all i, we have (working mod 8)

$$\begin{aligned} N &= (3 \cdot 3 \cdots 3)^2 + 2 \\ &= 3^2 \cdot 3^2 \cdots 3^2 + 2 \\ &= 1 \cdot 1 \cdots 1 + 2 \\ &= 3. \end{aligned}$$

(b): If $p|N$ then we observe that -2 is square mod p because (working mod p) we have

$$\begin{aligned} N &= 0 \\ (p_1 \cdots p_k)^2 + 2 &= 0 \\ (p_1 \cdots p_k)^2 &= -2. \end{aligned}$$

It follows from Problem 2 that $p = 1, 3 \bmod 8$.

(c): Consider the prime factorization of N:

$$N = q_1 q_2 \cdots q_\ell.$$

From (b) we know that each factor satisfies $q_i = 1 \bmod 8$ or $q_i = 3 \bmod 8$. But if all of the factors are $= 1 \bmod 8$ then (working mod 8) we have

$$N = q_1 q_2 \cdots q_\ell = 1 \cdot 1 \cdots 1 = 1,$$

which contradicts part (a). It follows that there exists some prime factor $q_i = 3 \bmod 8$.

(d): In summary, we have shown that there exists a prime number p such that $p|N$ (i.e., $N = 0 \bmod p$) and $p = 3 \bmod 8$. I claim that this number cannot be in the list $p_1, \ldots, p_k$. Indeed, for any i we have

$$N = p_i(\text{some integer}) + 2 = 2 \bmod p_i.$$

But if $p = p_i$ then this contradicts the fact that $N = 0 \bmod p$.

[Remark: My old professor M. Ram Murty showed[3] that this type of "Euclidean proof" of infinitely many primes $= a \bmod b$ only works for $a^2 = 1 \bmod b$. So we are still very far away from Dirichlet's Theorem.]

[3] *Primes in certain arithmetic progessions*, 1988.