MATH 4400/6400 – Homework #3
posted February 25, 2019; due March 6, 2019

You did a number on me
But, honestly, baby, who's counting?
— T. Swift

Directions. Give complete solutions, providing full justifications when appropriate. Your assignment must be stapled if it goes on beyond one page. Starred problems are required for MATH 6400 students and extra credit for 4400 students.

1. For each odd prime p, show that $\left(\frac{2}{p}\right) = \left(\frac{(p+1)/2}{p}\right)$.

2. Write out the details of the proof of the Generalized Gauss Lemma.

3. Let p be an odd prime, and let $a \in \mathbf{Z}$ where $p \nmid a$. Prove that if a is **even**, then

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{0<k<p/2} \lfloor ak/p \rfloor} \cdot (-1)^{(p^2-1)/8}.$$

4. Deduce from the last exercise that $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ for every odd prime p. Using this, give another proof of the result (discussed earlier in class) that for each odd prime p,

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

5. Find all primes p for which $\left(\frac{6}{p}\right) = 1$, in terms of a list of residue classes p must lie in modulo 24.

The next several exercises concern the **Jacobi symbol**, which is defined as follows. Let b be an *odd* positive integer, and let a be any integer. Factor b into (not necessarily distinct) primes, say $b = p_1 p_2 \cdots p_k$. The Jacobi symbol $\left(\frac{a}{b}\right)$, which takes values 0, 1, or -1, is defined by

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right).$$

It is OK to co-opt the Legendre symbol notation, since if p is an odd prime, then $\left(\frac{a}{p}\right)$ takes the same value if interpreted as either as a Jacobi symbol or as a Legendre symbol.

It is easy to prove that the Jacobi symbol inherits some of the basic properties of the Legendre symbol. For example:

(i) $\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$ if $a_1 \equiv a_2 \pmod b$, *and*

(ii) $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$.

Moreover, we also pick up multiplicativity in the "denominator":

(iii) $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$.

(You are *not* asked to prove these on this assignment — but you should convince yourself that you could prove them if asked!)

6. Let a and b be integers, where b is odd and positive.

(a) Show that $\left(\frac{a}{b}\right) = 0 \iff \gcd(a,b) > 1$.

(b) Show that if $\left(\frac{a}{b}\right) = -1$, then a is **not** a square modulo b. That is, there is no integer x with $x^2 \equiv a \pmod{b}$.

(c) Give an example where $\left(\frac{a}{b}\right) = 1$ and yet a is not a square modulo b.

7. Let r, s be odd, positive integers. Prove that:

(a) $\frac{rs-1}{2} \equiv \frac{r-1}{2} + \frac{s-1}{2} \pmod 2$,

(b) $\frac{(rs)^2-1}{8} \equiv \frac{r^2-1}{8} + \frac{s^2-1}{8} \pmod 2$.

8. Prove that for every odd positive integer b,

$$\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2}, \quad \left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8}.$$

[Hence, $\left(\frac{-1}{b}\right) = 1 \iff b \equiv 1 \pmod 4$, and $\left(\frac{2}{b}\right) = 1 \iff b \equiv \pm 1 \pmod 8$.]

9. Let a, b be odd, positive integers with $\gcd(a,b) = 1$. Prove the **law of quadratic reciprocity for the Jacobi symbol**:

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}.$$

10. Using the law of quadratic reciprocity for the Jacobi symbol and the results of Exercise 8 describing $\left(\frac{-1}{b}\right)$ and $\left(\frac{2}{b}\right)$, one can compute all Jacobi symbols $\left(\frac{a}{b}\right)$. For example,

$$\begin{aligned}
\left(\frac{66}{131}\right) &= \left(\frac{2}{131}\right)\left(\frac{33}{131}\right) \\
&= \left(\frac{33}{131}\right) \qquad \text{using Ex. 8 to compute } \left(\frac{2}{131}\right) \\
&= -\left(\frac{131}{33}\right) \qquad \text{using QR for Jacobi} \\
&= -\left(\frac{-1}{33}\right) \qquad \text{since } 131 \equiv -1 \pmod{33} \\
&= -1 \qquad \text{using Ex. 8 to compute } \left(\frac{-1}{33}\right).
\end{aligned}$$

Since 131 is prime, we can view $\left(\frac{66}{131}\right)$ as a Legendre symbol (not merely a Jacobi symbol), and we are allowed to conclude that 66 is a square modulo 131.

(a) Find $\left(\frac{82}{365}\right)$ by this method. Noting that 365 is not prime, what — if anything — can you conclude (without further calculation) from this about whether 82 is a square mod 365?

(b) Find $\left(\frac{82}{367}\right)$. Noting that 367 is prime, what — if anything — can you conclude from this (without further calculation) about whether 82 is a square mod 367?

11. (*) Let p be a prime number. Show that if p divides a number of the form $x^4 - x^2 + 1$, where $x \in \mathbf{Z}$, then $p \equiv 1 \pmod{12}$.

Hint: Show that -1 and -3 are both squares modulo p.