Math 25 — Assignment 5

Due Thursday, November 3rd, *beginning of class*.

1. The far more common approach to Quadratic Reciprocity is via Gauss' Lemma.

   Lemma (Gauss)**.** Let p be an odd prime, let $s = \frac{p-1}{2}$, let $P = \{1, \dots, s\}$, and let $N = \{s+1, s+2, \dots, 2s\}$. Then
$$\left(\frac{a}{p}\right) = (-1)^{\mu}$$
   where $\mu = \#(aP \cap N)$.

   By definition
$$aP = \{a \pmod{p}, 2a \pmod{p}, \dots, as \pmod{p}\}.$$

   (a) Show that $\#(aP \cap N) = \#(P \cap aN)$.

   (b) Use Gauss' lemma to determine whether -1, 2, 5 are quadratic residues modulo 29.

   Solution:

   (a) For ease of notation, we omit the "mod p" in each step with the understanding that we always reduce our elements modulo p. Notice
$$(-1)P = \{-x : x \in P\} \equiv \{p - x : x \in P\} = \{p-1, p-2, \dots, p-s\} = N.$$
   Notice
$$(-1)(aP) = (-1)\{ax : x \in P\} = \{-ax : x \in P\} = a\{-x : x \in P\} = aN.$$
   It is a general fact about injective functions f and sets X, Y that $f(X \cap Y) = f(X) \cap f(Y)$. (I'll include this result in an appendix, but you don't need to prove it.) Since multiplication-by-(-1) is a bijection from $\mathbb{Z}/p\mathbb{Z}^{\times}$ to $\mathbb{Z}/p\mathbb{Z}^{\times}$, we have that
$$(-1)(aP \cap N) = (-1)(aP) \cap (-1)N = aN \cap P.$$
   Again, multiplication-by-(-1) is a bijection, so these sets have the same size.

   Alternate Solution: Notice that multiplication-by-a induces a bijection on $\mathbb{Z}/p\mathbb{Z}^{\times}$. In other words, because P, N are disjoint, we see aP and aN are disjoint and
$$\mathbb{Z}/p\mathbb{Z}^{\times} = P \cup N = aP \cup aN.$$
   We consider the four sets $P \cap aP, P \cap aN, N \cap aP, N \cap aN$. Notice,
$$P = P \cap (aP \cup aN), \quad N = N \cap (aP \cup aN),$$
   so by disjointness of aP and aN we have
$$\#(P \cap aP) + \#(P \cap aN) = \#P = \frac{p-1}{2}.$$

Similarly, we see the sum of any row or column of the 2×2 square

$$\begin{matrix} \#(P \cap aP) & \#(P \cap aN) \\ \#(N \cap aP) & \#(N \cap aN) \end{matrix}$$

is $\frac{p-1}{2}$. Thus

$$\#(P \cap aN) = \#(N \cap aP) = \frac{p-1}{2} - \#(P \cap aP)$$

and the result is proven.

(b) We already know in general that $(-1)P = N$, so $\#((-1)P \cap N) = \#N = s$. Notice s is even if and only if $p \equiv 1 \pmod 4$, so by Gauss' Lemma we see that -1 is a square modulo 29.

One computes $2P \cap N = \{16, 18, 20, 22, 24, 26, 28\}$, so 2 is not a square mod 29.

One computes $5P \cap N = \{15, 16, 20, 21, 25, 26\}$, so 5 is a square mod 29. Indeed, $18^2 \equiv 5 \pmod{29}$.

2. In this exercise we prove the second supplement to quadratic reciprocity.

Theorem (Quadratic Reciprocity – second supplement)**.** *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \pmod 8.$$

It is a supplement, in the sense that now the prime 2 is involved in the reciprocity law. To prove this result, we consider the s equations:

$$\begin{aligned} 1 &= (-1)(-1) \\ 2 &= 2(-1)^2 \\ 3 &= (-3)(-1)^3 \\ &\vdots \\ s &= ((-1)^s s)(-1)^s \end{aligned}$$

(a) Show that $s! = (-1)^{\binom{s+1}{2}} \cdot \prod_{k=1}^{s} (-1)^k k$.

(b) Let p be an odd prime and set $s = \frac{p-1}{2}$. Show that

$$s! \equiv (-1)^{\binom{s+1}{2}} \cdot \prod_{k=1}^{s} (2k) \pmod p.$$

(c) Prove that $\binom{s+1}{2}$ is even if and only if $s + 1 \equiv 0, 1 \pmod 4$.

(d) Use the previous parts to prove the second supplement to the law of Quadratic Reciprocity.

(e) Use Gauss' Lemma to give a different proof of the second supplement.

Solution:

(a) If we multiply the s left-hand sides together and s right-hand sides together, we get

$$s! = (-1)^{1+2+\cdots+s} \cdot \prod_{k=1}^{s} (-1)^k k.$$

As it happens, $1 + 2 + \cdots + s = \binom{s+1}{2}$.

(b) We use the equation from part (a). Separating the even and odd terms give

$$s! = (-1)^{\binom{s+1}{2}} \cdot \prod_{\substack{k=1\\ \text{even}}}^{s} (-1)^k k \cdot \prod_{\substack{k=1\\ \text{odd}}}^{s} (-1)^k k = (-1)^{\binom{s+1}{2}} \cdot \prod_{\substack{k=1\\ \text{even}}}^{s} k \cdot \prod_{\substack{k=1\\ \text{odd}}}^{s} (-k).$$

We treat the cases of even and odd s separately. First assume that $s = 2t$ is even, in which case we define

$$\begin{aligned} X &:= \{k : 1 \leq k \leq s \text{ and } k \text{ even}\} = \{2, 4, 6, \dots, 2t\}, \\ Y &:= \{p - k : 1 \leq k \leq s \text{ and } k \text{ odd}\} \\ &= \{p - (2t-1), p - (2t-3), \dots, p-3, p-1\} \\ &= \{1 + p - 2t, 3 + p - 2t, \dots, p-3, p-1\} \end{aligned}$$

Because $p + 1 = 2s + 2 = 4t + 2$, we have

$$\begin{aligned} Y &= \{4t + 2 - 2t, 4t + 4 - 2t, \dots, p-3, p-1\} \\ &= \{s+2, s+4, \dots, p-3, p-1\} \\ &= \{2(t+1), 2(t+2), \dots, 2(s-1), 2s\} \end{aligned}$$

In particular

$$\prod_{\substack{k=1\\ \text{even}}}^{s} k \cdot \prod_{\substack{k=1\\ \text{odd}}}^{s} (-k) \equiv \prod_{\substack{k=1\\ \text{even}}}^{s} k \cdot \prod_{\substack{k=1\\ \text{odd}}}^{s} (p-k) = \prod_{k \in X} k \cdot \prod_{k \in Y} k = \prod_{x=1}^{s} (2x) \pmod{p}$$

So in total $s! \equiv (-1)^{\binom{s+1}{2}} \cdot \prod_{x=1}^{s} (2x)$ as required.

We still have the case where s is odd to deal with. In this case $s = 2t + 1$ and as before

$$\begin{aligned} X &:= \{k : 1 \leq k \leq s \text{ and } k \text{ even}\} = \{2, 4, 6, \dots, 2t\}, \\ Y &:= \{p - k : 1 \leq k \leq s \text{ and } k \text{ odd}\} \\ &= \{p - (2t+1), p - (2t-1), \dots, p-3, p-1\} \\ &= \{1 + p - (2t+1), 1 + p - 2t, \dots, p-3, p-1\} \end{aligned}$$

Because $p + 1 = 2s + 2 = 4t + 2$, we have

$$\begin{aligned} Y &= \{4t + 2 - 2t, 4t + 4 - 2t, \dots, p-3, p-1\} \\ &= \{s+1, s+3, \dots, p-3, p-1\} \\ &= \{2(t+1), 2(t+2), \dots, 2(s-1), 2s\} \end{aligned}$$

Exactly as before

$$\prod_{\substack{k=1\\ \text{even}}}^{s} k \cdot \prod_{\substack{k=1\\ \text{odd}}}^{s} (-k) \equiv \prod_{\substack{k=1\\ \text{even}}}^{s} k \cdot \prod_{\substack{k=1\\ \text{odd}}}^{s} (p-k) = \prod_{k \in X} k \cdot \prod_{k \in Y} k = \prod_{x=1}^{s} (2x) \pmod{p}$$

So in total $s! \equiv (-1)^{\binom{s+1}{2}} \cdot \prod_{x=1}^{s} (2x)$ as required.

(c) Note $\binom{s+1}{2}$ is even if and only if $0 \equiv 2\binom{s+1}{2} \equiv s(s+1) \pmod{4}$; the latter occurs exactly when $s + 1 \equiv 0, 1 \pmod{4}$.

(d) We take the equation from part (b) and factor out the 2's, giving

$$s! \equiv (-1)^{\binom{s+1}{2}} \cdot 2^s \cdot s! \pmod{p}.$$

Since $\frac{p-1}{2} = s < p$, we see $s!$ is a unit mod p, so dividing gives

$$(-1)^{\binom{s+1}{2}} \equiv 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod p$$

the last equality being Euler's criterion. In other words,

$$\left(\frac{2}{p}\right) = 1 \iff \binom{s+1}{2} \text{ is even } \iff \frac{p-1}{2}+1 \equiv 0,1 \pmod 4 \iff p \equiv \pm 1 \pmod 8.$$

(e) We partition $\mathbb{Z}/p\mathbb{Z}^\times = P \cup N$ as in Gauss' Lemma and compute $\#(2P \cap N)$. The elements of P sent to N are the elements of

$$X := \left\{ a \in P : \frac{p+1}{4} \leq a \leq \frac{p-1}{2} \right\}.$$

We have

$$\#X = \begin{cases} \frac{p-1}{2} - \frac{p+1}{4} + 1 & \frac{p+1}{4} \in \mathbb{Z} \\ \frac{p-1}{2} - \left\lfloor \frac{p+1}{4} \right\rfloor & \frac{p+1}{4} \notin \mathbb{Z} \end{cases}$$

Writing $p = 8t + r$ for some $r \in \{1, 3, 5, 7\}$, we see

$$\#X = \begin{cases} 2t & r = 1 \\ 2t+1 & r = 3 \\ 2t+1 & r = 5 \\ 2t+2 & r = 7 \end{cases}.$$

By Gauss' Lemma, we have

$$\left(\frac{2}{p}\right) = (-1)^{\#X} = \begin{cases} 1 & p \equiv 1,7 \pmod 8 \\ -1 & p \equiv 3,5 \pmod 8 \end{cases}.$$

3. You're probably wondering what the first supplement to quadratic reciprocity is. We've actually already covered it.

Theorem (Quadratic Reciprocity – first supplement)**.** *Let p be an odd prime. Then*

$$\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod 4.$$

Here's the question: Let p be a prime congruent to $1 \pmod 8$. Show that

$$\left(\frac{p-56}{p}\right) = \left(\frac{p}{7}\right).$$

Solution: Using properties of the Legendre symbol

$$\begin{aligned} \left(\frac{p-56}{p}\right) &= \left(\frac{-56}{p}\right) \\ &= \left(\frac{-1}{p}\right) \cdot \left(\frac{8}{p}\right) \cdot \left(\frac{7}{p}\right). \end{aligned}$$

Because 8 is a cube

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

By the first supplement and $p \equiv 1 \pmod 8$

$$= \left(\frac{2}{p}\right) \cdot \left(\frac{7}{p}\right).$$

By the second supplement and $p \equiv 1 \pmod 8$

$$= \left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) \quad \text{by quadratic reciprocity.}$$

As required.

4. What was the most confusing part of Rousseau's proof for you?

   Prof. K's answer: As the professor, I can follow the proof without much difficulty. Nevertheless, I'll say something that confused me by expanding the context. There are several proofs of quadratic reciprocity at varying levels of abstraction. There's a version of the story to be told with square roots. For example, I can't factor primes, unless I allow square roots

$$\begin{aligned} 3 &= (4+\sqrt{13})(4-\sqrt{13}), \quad & 13 &= (4+\sqrt{3})(4-\sqrt{3}) \\ 5 &= (\sqrt{41}-6)(\sqrt{41}+6), \quad & 41 &= (3\sqrt{5}+2)(3\sqrt{5}-2). \end{aligned}$$

   Huh. Weird pattern. Turns out this is quadratic reciprocity! *So, what is Rousseau's proof saying in the land of square roots?*

A. (Appendix) Let X, Y be subsets of the domain of an injective function f. Then

$$f(X \cap Y) = f(X) \cap f(Y).$$

Proof. By definition

$$f(X) = \{f(x) : x \in X\}.$$

If $a \in X \cap Y$, then $a \in X$ and $a \in Y$. Thus $f(a) \in f(X)$ and $f(a) \in f(Y)$. So $f(a) \in f(X) \cap f(Y)$. This proves $f(X \cap Y) \subset f(X) \cap f(Y)$.

On the other hand, if $b \in f(X) \cap f(Y)$, then there exist $x \in X$ and $y \in Y$ such that $b = f(x) = f(y)$. Because f is injective, $x = y$, so $x \in X \cap Y$. This shows $f(X \cap Y) \supset f(X) \cap f(Y)$. □