Lecture 13: Quadratic Reciprocity II

William Stein

Math 124 HARVARD UNIVERSITY **Fall 2001**

IN-CLASS MIDTERM THIS WEDNESDAY, OCTOBER 17!

Monday's lecture will be a review lecture; Grigor's review session is on Monday at 4pm; I will have an extra office hour in SC 515, Tuesday, 2:35–3:30.

1 Recall Gauss's Lemma

We proved the following lemma in the previous lecture.

Lemma 1.1. *Let p be an odd prime and a an integer with $p \nmid a$. Form the numbers $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ and reduce them modulo p to lie in the interval $(-\frac{p}{2}, \frac{p}{2})$. Let ν be the number of negative numbers in the resulting set. Then $\left(\frac{a}{p}\right) = (-1)^\nu$.*

2 Euler's Conjecture

Lemma 2.1. *Let $a, b \in \mathbb{Q}$. Then for any $n \in \mathbb{Z}$,*

$$\#\left((a,b)\cap\mathbb{Z}\right) \equiv \#\left((a,b+2n)\cap\mathbb{Z}\right) \equiv \#\left((a+2n,b)\cap\mathbb{Z}\right) \pmod{2}.$$

Proof. If $n > 0$, then

$$(a, b+2n) = (a,b) \cup [b, b+2n),$$

where the union is disjoint. Let $[x]$ denote the least integer $\geq x$. There are $2n$ integers,

$$[b], [b]+1, \ldots, [b]+2n-1,$$

in the interval $[b, b+2n)$, so the assertion of the lemma is true in this case. We also have

$$(a, b-2n) = (a,b) \backslash [b-2n, b)$$

and $[b-2n, b)$ also contains exactly $2n$ integers, so the lemma is also true when n is negative. The statement about $\#\left((a+2n,b)\cap\mathbb{Z}\right)$ is proved in a similar manner. □

The following proposition was first conjectured by Euler, based on extensive numerical evidence. Once we've proved this proposition, it will be easy to deduce the quadratic reciprocity law.

Proposition 2.2 (Euler's Conjecture). *Let p be an odd prime and $a \in \mathbb{N}$ a natural number with $p \nmid a$.*

1. *The symbol* $\left(\frac{a}{p}\right)$ *depends only on* p *modulo* $4a$.

2. *If* q *is a prime with* $q \equiv -p \pmod{4a}$, *then* $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

Proof. To apply Gauss's lemma, we have to compute the parity of the intersection of

$$S = \left\{a, 2a, 3a, \ldots \frac{p-1}{2}a\right\}$$

and

$$I = \left(\frac{1}{2}p, p\right) \cup \left(\frac{3}{2}p, 2p\right) \cup \cdots \cup \left(\left(b - \frac{1}{2}\right)p, bp\right),$$

where $b = \frac{1}{2}a$ or $\frac{1}{2}(a-1)$, whichever is an integer. (Why? We have to check that every element of S that reduces to something in the interval $(-\frac{p}{2}, 0)$ lies in I. This is clear if $b = \frac{1}{2}a < \frac{p-1}{2}a$. If $b = \frac{1}{2}(a-1)$, then $bp + \frac{p}{2} > \frac{p-1}{2}a$, so $((b-\frac{1}{2})p, bp)$ is the last interval that could contain an element of of S that reduces to $(-\frac{p}{2}, 0)$.) Also note that the integer endpoints of I are not in S, since those endpoints are divisible by p, but no element of S is divisible by p.

Dividing I through by a, we see that

$$\#(S \cap I) = \#\left(\mathbb{Z} \cap \frac{1}{a}I\right),$$

where

$$\frac{1}{a}I = \left(\left(\frac{p}{2a}, \frac{p}{a}\right) \cup \left(\frac{3p}{2a}, \frac{2p}{a}\right) \cup \cdots \cup \left(\frac{(2b-1)p}{2a}, \frac{bp}{a}\right)\right).$$

Write $p = 4ac + r$, and let

$$J = \left(\left(\frac{r}{2a}, \frac{r}{a}\right) \cup \left(\frac{3r}{2a}, \frac{2r}{a}\right) \cup \cdots \cup \left(\frac{(2b-1)r}{2a}, \frac{br}{a}\right)\right).$$

The only difference between I and J is that the endpoints of intervals are changed by addition of an even integer. By Lemma 2.1,

$$\nu = \#\left(\mathbb{Z} \cap \frac{1}{a}I\right) \equiv \#(\mathbb{Z} \cap J) \pmod{2}.$$

Thus $\left(\frac{a}{p}\right) = (-1)^\nu$ depends only on r, i.e., only on p modulo $4a$. WOW!

If $q \equiv -p \pmod{4a}$, then the only change in the above computation is that r is replaced by $4a - r$. This changes $\frac{1}{a}I$ into

$$K = \left(\left(2 - \frac{r}{2a}, 4 - \frac{r}{a}\right) \cup \left(6 - \frac{3r}{2a}, 8 - \frac{2r}{a}\right) \cup \cdots \cup \left(4b - 2 - \frac{(2b-1)r}{2a}, 4b - \frac{br}{a}\right)\right).$$

Thus K is the same as $-\frac{1}{a}I$, except even integers have been added to the endpoints. By Lemma 2.1,

$$\#(K \cap \mathbb{Z}) \equiv \#\left(\left(\frac{1}{a}I\right) \cap \mathbb{Z}\right) \pmod{2},$$

so $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$, which completes the proof. $\square$

The following more careful analysis in the special case when $a = 2$ helps illustrate the proof of the above lemma, and is frequently useful in computations.

Proposition 2.3. *Let p be an odd prime. Then*

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

Proof. When $a = 2$, the set $S = \{a, 2a, \ldots, 2 \cdot \frac{p-1}{2}\}$ is

$$\{2, 4, 6, \ldots, p-1\}.$$

We must count the parity of the number of elements of S that lie in the interval $I = (\frac{p}{2}, p)$. Writing $p = 8c + r$, we have

$$\begin{aligned} \#\,(I \cap S) &= \#\left(\frac{1}{2} I \cap \mathbb{Z}\right) = \#\left(\left(\frac{p}{4}, \frac{p}{2}\right) \cap \mathbb{Z}\right) \\ &= \#\left(\left(2c + \frac{r}{4}, 4c + \frac{r}{2}\right) \cap \mathbb{Z}\right) \equiv \#\left(\left(\frac{r}{4}, \frac{r}{2}\right) \cap \mathbb{Z}\right) \pmod 2, \end{aligned}$$

where the last equality comes from Lemma 2.1. The possibilities for r are $1, 3, 5, 7$. When $r = 1$, the cardinality is 0, when $r = 3, 5$ it is 1, and when $r = 7$ it is 2. □

3 The Quadratic Reciprocity Law

With the lemma in hand, it is straightforward to deduce the quadratic reciprocity law.

Theorem 3.1 (Gauss). *Suppose that p and q are distinct odd primes. Then*

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

Proof. First suppose that $p \equiv q \pmod 4$. By swapping p and q if necessary, we may assume that $p > q$, and write $p - q = 4a$. Since $p = 4a + q$,

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

and

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

Proposition 2.2 implies that $\left(\frac{a}{q}\right) = \left(\frac{a}{p}\right)$, since $p \equiv q \pmod{4a}$. Thus

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

where the last equality is because $\frac{p-1}{2}$ is even if and only if $\frac{q-1}{2}$ is even.

Next suppose that $p \not\equiv q \pmod 4$, so $p \equiv -q \pmod 4$. Write $p + q = 4a$. We have

$$\left(\frac{p}{q}\right) = \left(\frac{4a-q}{q}\right) = \left(\frac{a}{q}\right), \quad \text{and} \quad \left(\frac{q}{p}\right) = \left(\frac{4a-p}{p}\right) = \left(\frac{a}{p}\right).$$

Since $p \equiv -q \pmod{4a}$, Proposition 2.2 implies that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Since $(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = 1$, the proof is complete. □

3.1 Examples

Example 3.2. Is 6 a square modulo 389? We have

$$\left(\frac{6}{389}\right) = \left(\frac{2\cdot 3}{389}\right) = \left(\frac{2}{389}\right)\cdot\left(\frac{3}{389}\right) = (-1)\cdot(-1) = 1.$$

Here, we found that $\left(\frac{2}{389}\right) = -1$ using Proposition 2.3 and that $389 \equiv 3 \pmod 8$. We found $\left(\frac{3}{389}\right)$ as follows:

$$\left(\frac{3}{389}\right) = \left(\frac{389}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Thus 6 is a square modulo 389.

Annoyingly, though we know that 6 is a square modulo 389, we still don't know an x such that $x^2 \equiv 6 \pmod{389}$!

```
? for(a=1,388,if(Mod(a,389)^2==6,print1(a, " ")))
28 361
```

Example 3.3. Is 3 a square modulo $p = 726377359$? We proved that the answer is "no" in the previous lecture by computing $3^{p-1} \pmod p$. It's easier to prove that the answer is no using Theorem 3.1:

$$\left(\frac{3}{726377359}\right) = (-1)^{1\cdot\frac{726377358}{2}}\cdot\left(\frac{726377359}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

4 Some Homework Hints

Spend time studying for the midterm in addition to doing the homework. To point you in the right direction on the homework problems, here are some hints.

(1) Use the quadratic reciprocity law, just like in the above examples.

(2) Use the quadratic reciprocity law.

(3) Relate the statement for $n = 3$ to the statement for $n > 3$.

(4) Write down an element of $(\mathbb{Z}/p^2\mathbb{Z})^*$ that looks like it might have order p, and prove that it does. Recall that if a, b have orders n, m, with $\gcd(n, m) = 1$, then ab has order nm.

(5)

(6)

(7) Replace $\sum\left(\frac{a}{p}\right)$ by $\sum\left(\frac{ab}{p}\right)$ and use that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$.

(8) Write a little program.