Lecture 12: Quadratic Reciprocity I

William Stein

Math 124 HARVARD UNIVERSITY **Fall 2001**

Key Ideas:

- *Euler's Criterion:* When is a a square modulo p?
- Quadratic reciprocity
- Lemma of Gauss

1 Euler's Criterion

Proposition 1.1 (Euler's Criterion). *Let p be an odd prime and a an integer not divisible by p. Then $x^2 \equiv a \pmod{p}$ has a solution if and only if*

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Proof. By the theorem from Lecture 11, there is an integer g that has order $p-1$ modulo p. Every integer coprime to p is congruent to a power of g. First suppose that a is congruent to a perfect square modulo p, so

$$a \equiv (g^r)^2 \equiv g^{2r} \pmod{p}$$

for some r. Then

$$a^{(p-1)/2} \equiv g^{2r \cdot \frac{p-1}{2}} \equiv g^{r(p-1)} \equiv 1 \pmod{p}.$$

Conversely, suppose that $a^{(p-1)/2} \equiv 1 \pmod{p}$. We have $a \equiv g^r \pmod{p}$ for some integer r. Thus $g^{r(p-1)/2} \equiv 1 \pmod{p}$, so

$$p-1 \mid r(p-1)/2$$

which implies that r is even. Thus $a \equiv (g^{r/2})^2 \pmod{p}$, so a is congruent to a square modulo p. □

Corollary 1.2. *If $x^2 \equiv a \pmod{p}$ has no solutions if and only if $a^{(p-1)/2} \equiv -1 \pmod{p}$.*

Proof. This follows from Proposition 1.1 and that the polynomial x^2-1 has no roots besides $+1$ and -1. □

Example 1.3. Suppose $p = 11$. By squaring each element of $(\mathbb{Z}/11\mathbb{Z})^*$, we see exactly which numbers are squares modulo 11:

$$1^2 = 1,\ 2^2 = 4,\ 3^2 = 9,\ 4^2 = 5,\ 5^2 = 3,\ 6^2 = 3,\ 7^2 = 5,\ 8^2 = 9,\ 9^2 = 4,\ 10^2 = 1.$$

Thus the squares are $\{1, 3, 4, 5, 9\}$. Next, we compute $a^{(p-1)/2} = a^5$ for each $a \in (\mathbb{Z}/11\mathbb{Z})^*$.

$$1^5 = 1,\ 2^5 = -1,\ 3^5 = 1,\ 4^5 = 1,\ 5^5 = 1,\ 6^5 = -1,\ 7^5 = -1,\ 8^5 = -1,\ 9^5 = 1,\ 10^5 = -1.$$

The a with $a^5 = 1$ are $\{1, 3, 4, 5, 9\}$, which is exactly the same as the set of squares, just as Proposition 1.1 predicts.

Example 1.4. Determine whether or not 3 is a square modulo $p = 726377359$.
Answer: We compute $3^{(p-1)/2}$ modulo p using PARI:

```
? Mod(3,p)^((p-1)/2)
%5 = Mod(726377358, 726377359)   \\ class of -1 modulo 726377359.
```

Thus 3 is not a square modulo p. This computation wasn't too difficult, but it would have been very tedious to carry about by hand. The law of quadratic reciprocity, which we will state in the next section, is a vastly more powerful way to answer such questions. For example, you could easily answer the above question by hand using quadratic reciprocity.

Remark 1.5. Proposition 1.1 can be reformulated in more group-theoretic language as follows. The map

$$(\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}$$

that sends a to $a^{(p-1)/2} \pmod{p}$ is a homomorphism of groups, whose kernel is the subgroup of squares of elements of $(\mathbb{Z}/p\mathbb{Z})^*$.

Definition 1.6. An element $a \in \mathbb{Z}$ with $p \nmid a$ is called a *quadratic residue* modulo p if a is a square modulo p.

2 The Quadratic Reciprocity Law

Let p be an odd prime and let a be an integer with $p \nmid a$. Set

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \text{ is a quadratic residue, and} \\ -1 & \text{otherwise.} \end{cases}$$

Proposition 1.1 implies that

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

Also, notice that

$$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right),$$

because $\left(\frac{\cdot}{p}\right)$ is a homomorphism (see Remark 1.5).

The symbol $\left(\frac{a}{p}\right)$ only depends on the residue class of a modulo p. Thus tabulating the value of $\left(\frac{a}{5}\right)$ for hundreds of a would be silly. *Would it be equally silly to make a table of $\left(\frac{5}{p}\right)$ for hundreds of primes p?* Let's begin making such a table and see whether or not there is an obvious pattern. (To compute $\left(\frac{a}{p}\right)$ in PARI, use the command `kronecker(a,b)`.)

p	$\left(\frac{5}{p}\right)$	$p \bmod 5$
7	-1	2
11	1	1
13	-1	3
17	-1	2
19	1	4
23	-1	3
29	1	4
31	1	1
37	-1	2
41	1	1
43	-1	3
47	-1	2

The evidence suggests that $\left(\frac{5}{p}\right)$ depends only on the congruence class of p; more precisely, $\left(\frac{5}{p}\right) = 1$ if and only if $p \equiv 1, 4 \pmod 5$, i.e., p is a square modulo 5. However, when I think directly about the equation

$$5^{(p-1)/2} \pmod p,$$

I see no way that knowing that $p \equiv 1, 4 \pmod 5$ helps us to evaluate that strange expression! And yet, the numerical evidence is so *compelling*! Argh!

Based on such computations, various mathematicians found a conjectural explanation for this mystery in the 18th century. Finally, on April 8, 1796, at your age (age 19), Gauss proved their conjecture.

Theorem 2.1 (The Law of Quadratic Reciprocity). *Suppose that p and q are odd primes. Then*

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

We will prove this theorem in the next lecture.

In the case considered above, this theorem implies that

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

Thus the quadratic reciprocity law "explains" why knowing p modulo 5 helps in computing $5^{\frac{p-1}{2}} \pmod{p}$.

Here is a list of almost 200 proofs of Theorem 2.1:

`http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html`

3 A Lemma of Gauss

The proof we will give of Theorem 2.1 was first discovered by Gauss, though not when he was 19. This proof is given in many elementary number theory texts (including Davenport). It depends on the following lemma of Gauss:

Lemma 3.1. *Let p be an odd prime and let a be an integer $\not\equiv 0 \pmod{p}$. 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

$$\left(\frac{a}{p}\right) = (-1)^{\nu}.$$

Proof. In defining ν, we expressed each number in

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

as congruent to a number in the set

$$\left\{1, -1, 2, -2, \ldots, \frac{p-1}{2}, -\frac{p-1}{2}\right\}.$$

No number $1, 2, \ldots \frac{p-1}{2}$ appears more than once, with either choice of sign, because if it did then either two elements of S are congruent modulo p or 0 is the sum of two elements of S, and both events are impossible. Thus the resulting set must be of the form

$$T = \left\{\varepsilon_1 \cdot 1, \varepsilon_2 \cdot 2, \ldots, \varepsilon_{(p-1)/2} \cdot \frac{p-1}{2}\right\},$$

where each ε_i is either $+1$ or -1. Multiplying together the elements of S and of T, we see that

$$(1a) \cdot (2a) \cdot (3a) \cdot \cdots \cdot \left(\frac{p-1}{2}a\right) \equiv (\varepsilon_1 \cdot 1) \cdot (\varepsilon_2 \cdot 2) \cdots \left(\varepsilon_{(p-1)/2} \cdot \frac{p-1}{2}\right) \pmod{p},$$

so

$$a^{(p-1)/2} \equiv \varepsilon_1 \cdot \varepsilon_2 \cdot \cdots \cdot \varepsilon_{(p-1)/2} \pmod{p}.$$

The lemma then follows from Proposition 1.1. $\square$