MEM204-Number Theory

7th virtual lecture

Giorgos Kapetanakis

Spring semester 2019-20 - 24/04/2020

University of Crete

Computing the Legendre Symbol

Number of quadratic residues

Lemma

Let p be an odd prime. Then exactly half of the elements of $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{\bar{0}\}$ *are quadratic residues modulo p and the other half are non-quadratic residues modulo p.*

Proof.

Take the map $f : \mathbb{Z}_p^* \to \mathbb{Z}_p^*,\ x \mapsto x^2$. Then, since p is prime, we get that $f(x) = f(y) \iff x = \pm y$. Additionally, since p is odd, we get that (for $x \neq \bar{0}$), $x \neq -x$. It follows that f is 2-1 and the result follows. □

Euler's Criterion

Theorem (Euler's Criterion)

Let p be an odd prime and $p \nmid n$. Then

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

Proof

First, assume that $\left(\frac{n}{p}\right) = 1$. Then there exists some a, such that $a^2 \equiv n \pmod{p}$. Now, Fermat's theorem implies

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

Next, assume that $\left(\frac{n}{p}\right) = -1$. Take the polynomial congruence

$$x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}.$$

From the first part of the proof, we see that all the quadratic residues modulo p are solutions of this congruence. Moreover, since this congruence's degree is $(p-1)/2$, then it has at most $(p-1)/2$ solutions. However this is exactly the number of quadratic residues modulo p. It follows that if n is a non-quadratic residue modulo p, $n^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. This combined with the fact that $n^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ (Fermat's theorem) yields the desired result.

A reduction

Lemma

Let p be a prime and a, b be such that $p \nmid a, b$. Then

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

Proof.

The result follows immediately from Euler's criterion. □

The Legendre Symbol of -1

Proposition

Let p be an odd prime. Then

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

In other words,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \textit{if } p \equiv 1 \pmod{4}, \\ -1, & \textit{if } p \equiv 3 \pmod{4}. \end{cases}$$

Proof.

The result follows immediately from Euler's criterion. □

The Legendre Symbol of 2

Proposition

Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

In other words,

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

Proof

Take the following $(p-1)/2$ congruences:

$$\begin{aligned}
p-1 &\equiv 1(-1)^1 \pmod{p} \\
2 &\equiv 2(-1)^2 \pmod{p} \\
p-3 &\equiv 3(-1)^3 \pmod{p} \\
4 &\equiv 4(-1)^4 \pmod{p} \\
&\vdots \\
r &\equiv \frac{p-1}{2}(-1)^{(p-1)/2} \pmod{p},
\end{aligned}$$

where $r = (p-1)/2$ or $r = p - (p-1)/2$. Note that the left hand sides of these congruences are always even and, in fact, all positive even numbers up to $p-1$ appear exactly once.

Proof

Now, we multiply these congruences and get:

$$2\cdot 4\cdots(p-1)\equiv\left(\frac{p-1}{2}\right)!(-1)^{1+2+\cdots+(p-1)/2}\pmod{p},$$

that is,

$$2^{(p-1)/2}\left(\frac{p-1}{2}\right)!\equiv\left(\frac{p-1}{2}\right)!\cdot(-1)^{\frac{p^2-1}{8}}\pmod{p}.$$

Further, $\left(\frac{p-1}{2}\right)!\not\equiv 0\pmod{p}$. Hence, Euler's criterion yields

$$\left(\frac{2}{p}\right)\equiv 2^{(p-1)/2}\equiv(-1)^{\frac{p^2-1}{8}}\pmod{p}$$

and the result follows.

The Quadratic Reciprocity Law

The final supplement in our arsenal for computing the Jacobi symbol is the following theorem.

Theorem (Quadratic reciprocity law - Νόμος τετραγωνικής αντιστροφής)

Let p, q be distinct odd primes. Then

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

Proof.

Omitted. □

A few comments

- Euler and Legendre conjectured this theorem and Gauss was the first to provide a proof.
- There are numerous (more than 150) proofs of the quadratic reciprocity law. Gauss himself gave 8 proofs. However, these proofs are either technical, complicated or advanced.
- Its importance was recognized by Gauss, who called it the “fundamental theorem” in his *Disquisitiones Arithmeticae* and his papers.

Putting everything together

Let p, q be distinct odd primes and a, b be such that $p \nmid a, b$.

1. $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. $\left(\frac{1}{p}\right) = \left(\frac{a^2}{p}\right) = 1$.
3. (Euler's criterion) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
5. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.
6. $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.
7. (Quadratic reciprocity law) $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}$.

A few examples

Example 1

Remark

In the remaining slides, the numbers on top of the equality symbols indicate the corresponding property of the last slide.

Example

We will compute $\left(\frac{-14}{71}\right)$. We have that

$$\begin{aligned}\left(\frac{-14}{71}\right) &\overset{4}{=} \left(\frac{-1}{71}\right)\left(\frac{2}{71}\right)\left(\frac{7}{71}\right) \overset{5,6}{=} (-1)^{\frac{70}{2}+\frac{71^2-1}{8}}\left(\frac{7}{71}\right)\\ &= (-1)\left(\frac{7}{71}\right) \overset{7}{=} (-1)\cdot(-1)^{\frac{70\cdot 6}{4}}\left(\frac{71}{7}\right) = \left(\frac{71}{7}\right)\\ &\overset{1}{=} \left(\frac{1}{7}\right) \overset{2}{=} 1.\end{aligned}$$

Example 2

We will determine whether 219 is a quadratic residue modulo 383. We easily verify that 383 is a prime. It follows that the question is equivalent to computing $\left(\frac{219}{383}\right)$. Thus, we have that:

$$\begin{aligned}\left(\frac{219}{383}\right) &\overset{4}{=} \left(\frac{3}{383}\right)\left(\frac{73}{383}\right) \overset{7}{=} (-1)^{2\cdot 382/4}\left(\frac{383}{3}\right)(-1)^{72\cdot 382/4}\left(\frac{383}{73}\right)\\ &= (-1)\left(\frac{383}{3}\right)\left(\frac{383}{73}\right) \overset{1}{=} (-1)\left(\frac{2}{3}\right)\left(\frac{18}{73}\right) = \left(\frac{18}{73}\right)\\ &\overset{4}{=} \left(\frac{2}{73}\right)\left(\frac{3^2}{73}\right) \overset{6,2}{=} (-1)^{(73^2-1)/8}\cdot 1 = 1.\end{aligned}$$

It follows that 219 is a quadratic residue modulo 383.

Example 3

We will check whether

$$x^2 - 6x - 13 \equiv 0 \pmod{127}$$

is solvable. The above is equivalent to $y^2 \equiv 22 \pmod{127}$, where $y = x - 3$. In other words, the original congruence is solvable iff 22 is a quadratic residue modulo 127. Also, since 127 is prime, this means that if suffices to compute $\left(\frac{22}{127}\right)$. So, we have that

$$\begin{aligned}\left(\frac{22}{127}\right) &\stackrel{4}{=} \left(\frac{2}{127}\right)\left(\frac{11}{127}\right) \stackrel{6}{=} \left(\frac{11}{127}\right) \stackrel{7}{=} -\left(\frac{127}{11}\right) \stackrel{1}{=} -\left(\frac{6}{11}\right) \\ &\stackrel{4}{=} -\left(\frac{2}{11}\right)\left(\frac{3}{11}\right) \stackrel{6}{=} \left(\frac{3}{11}\right) \stackrel{7}{=} -\left(\frac{11}{3}\right) \stackrel{1}{=} -\left(\frac{2}{3}\right) = 1.\end{aligned}$$

It follows that the original congruence is solvable.

Stay home, stay safe!