CS681 **Computational Number Theory**

Lecture 18: Quadratic Reciprocity

Instructor: Piyush P Kurur *Scribe: Ramprasad Saptharishi*

Overview

Polynomial factorization and randomized primality testing were one of the first examples of the power of randomization. Two standard algorithms for primality testing (randomized) are the Miller-Rabin test and the Solovay-Strassen test.

We shall build some theory on quadratic reciprocity laws before we get into the Solovay Strassen test.

1 Quadratic Reciprocity

The reciprocity laws are closely related to how primes split over *number fields.* Let us first understand what these number fields are.

Definition 1. *An algebraic integer over $\mathbb{Q}$ is an element ζ such that it is a root of a monic polynomial in $\mathbb{Z}[X]$. For example, the number $\frac{1}{2} + i\frac{\sqrt{3}}{2}$ is an algebraic integer as it is a root of $x^2 - x + 1$.*

A number field is a finite extension of $\mathbb{Q}$. One could think of this as just adjoining an algebraic number to $\mathbb{Q}$.

Note that number fields are strange objects. They may not even be UFDs. We saw the example when we consider $\mathbb{Q}(\sqrt{-5})$, the number 6 factors as both 3×2 and $(1+\sqrt{-5})(1-\sqrt{-5})$. However, if one were to consider factorization over ideals, they form unique factorizations.

1.1 The Legendre Symbol

Fix an odd prime p. We want to study equations of the form $X^2 - a$ over $\mathbb{F}_p$. What does it mean to say that this has a solution in $\mathbb{F}_p$? It means that a has a square-root in $\mathbb{F}_p$ or a is a square in $\mathbb{F}_p$. The legendre symbol captures that.

Definition 2. *For $a \in \mathbb{F}_p$, the legendre symbol $\left(\frac{a}{p}\right)$ is defined as follows:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \textit{if } p \mid a \\ -1 & \textit{if } a \textit{ is not a square modulo } p \\ 1 & \textit{if } a \textit{ is a square modulo } p \end{cases}$$

Proposition 1.

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

The proof is fairly straight forward; just consider them case by case when they are $-1, 0, 1$.

Thus, the above proposition tells us that the $\left(\frac{\cdot}{p}\right)$ is a homomorphism from $\mathbb{Z}/p\mathbb{Z}$ to $\{-1, 0, 1\}$.

Another observation is that since $\mathbb{F}_p^\star$ is cyclic, there is a generator b. Then we can write $a = b^t$. We then have,

$$a = \begin{cases} 0 & \text{if } p \mid a \\ -1 & \text{if } a \text{ is not a square modulo } p \\ 1 & \text{if } a \text{ is a square modulo } p \end{cases}$$

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

Note that $x^2 = y^2 \implies x = y$ or $x = -y$ and therefore, the number of squares in $\mathbb{F}_p^\star$ is exactly $\frac{p-1}{2}$. And if the generator of the group is a quadratic non-residue (not a square), then any odd power of the generator is also a non-residue.

2 Quadratic Reciprocity Theorem

Theorem 2. *Let p and q be odd primes (not equal to each other). Then*

$$\begin{aligned} \left(\frac{2}{p}\right) &= (-1)^{\frac{p^2-1}{8}} \\ \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \end{aligned}$$

Proof. We shall prove the part of $\left(\frac{2}{p}\right)$ in this class and do the other in the next. The idea is to go to a field extension (if necessary) and evaluate certain elements in two ways to get what we want. In the case of $\left(\frac{2}{p}\right)$ we shall go to the extension $\mathbb{F}_p(i)$ where i is a square root of -1.

Firstly note that this needn't be a proper extension at all. For example, in $\mathbb{F}_5$, we already have a root of -1 which is 2. Infact, for every prime of the form $1 \bmod 4$, we have a square root of -1. So we will go to an extension if necessary.

Now set $\tau = 1 + i$. We know that $\tau^2 = 1 - 1 + 2i = 2i$ and $\tau^p = 1 + i^p$ in $\mathbb{F}_p$. We could also evaluate τ^p as $\tau \cdot (\tau^2)^{\frac{p-1}{2}}$. Also $(1+i)^{-1} = \frac{1-i}{2}$.

$$\begin{aligned}
1 + i^p &= \tau^p \\
&= \tau(2i)^{\frac{p-1}{2}} \\
&= (1+i)2^{\frac{p-1}{2}} i^{\frac{p-1}{2}} \\
\implies \frac{(1+i^p)(1-i)}{2} &= 2^{\frac{p-1}{2}} i^{\frac{p-1}{2}} \\
\implies \frac{1 + i^p - i - i^{p+1}}{2} &= \left(\frac{2}{p}\right) i^{\frac{p-1}{2}}
\end{aligned}$$

Case 1: When $p = 1 \bmod 4$

Then $i \in \mathbb{F}_p$ and the above equation reduces to

$$\begin{aligned}
\frac{1 + i - i + 1}{2} &= \left(\frac{2}{p}\right)(-1)^{\frac{p-1}{4}} \\
\implies \left(\frac{2}{p}\right) &= (-1)^{\frac{p-1}{4}}
\end{aligned}$$

Case 2: When $p = 3 \bmod 4$

$$\begin{aligned}
\frac{1 - i - i - 1}{2} &= \left(\frac{2}{p}\right) i^{\frac{p-1}{2}} \\
\implies i^3 &= \left(\frac{2}{p}\right) i^{\frac{p-1}{2}} \\
\implies \left(\frac{2}{p}\right) &= i^{\frac{1-p}{2}+3} = i^{\frac{8-(1+p)}{4}} \\
&= (-1)^{\frac{p+1}{4}}
\end{aligned}$$

Therefore,

$$\left(\frac{2}{p}\right) = \begin{cases} (-1)^{\frac{p-1}{4}} & p = 1 \bmod 4 \\ (-1)^{\frac{p+1}{4}} & p = 3 \bmod 4 \end{cases}$$

and combining the two, we get

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

$\square$

The proof of the other part is very similar. We consider a similar τ and evaluate τ^p in two different ways to get to our answer. We shall do this in the next class.