MAT 115B Number Theory	**Winter 2025**
	January 29, 2025

Lecture 10

Lecturer: Martin Luu *Scribe: Avery Li*

Lecture 8 Review

General process for computing Legendre symbol

Jacobi Symbol

The Jacobi Symbol gives up on the direct connection of being a quadratic residue, generalizing it instead. It also retains nice Legendre-like properties, including multiplcativity and a Quadratic-reciprocity like statement. Note that this means that Jacobi symbols are as easy to compute as Legendre symbols.

Definition 10.1. The *Jacobi symbol* is defined as follows: for $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}.$$

Remark 10.2. hi

Solovay-Stressen Primality Test

Note that in general, the Euler criterion does *not* hold for Jacobi symbol mod composite n. For example, $\left(\frac{5}{21}\right) \not\equiv 5^{\frac{21-1}{2}} \equiv 16 \pmod{21}$, 16 is not even ± 1. To check if N is prime, compute $\left(\frac{a}{N}\right)$ and $a^{\frac{N-1}{2}} \pmod{N}$ for some random values a. If we find a value a for which $\left(\frac{a}{N}\right) \not\equiv a^{\frac{N-1}{2}} \pmod{n}$, we know that N is not prime.

Fact 10.3. *If N is composite, then at least half of all $a \pmod{n}$ that are coprime to N will give a failure of the Euler Criterion.*

This gives us a probabilistic test, and the probability of error is at most $\frac{1}{2}$. However, calculating $\left(\frac{a}{N}\right)$ requires factoring N, which would then already give us whether or not N is prime. We can use the "Quadratic-reciprocity" like property of Jacobi symbols to get around this and calculate it directly without ever factoring N.

Definition 10.4. The *primitive roots* $\pmod{m}$ are the numbers a such that $\gcd(a, m) = 1$ and $a^{\phi(m)} \equiv 1 \pmod{m}$. In other words, it is coprime to m.

Definition 10.5. Let $(a, m) = 1$. The *order* of a modulo m denoted $\mathrm{ord}_m(a)$ is the smallest k such that $a^k \equiv 1 \pmod{m}$. Note that $\mathrm{ord}_m(a) \leq \varphi(m)$.