CS681 **Computational Number Theory**

Lecture 23 and 24 : The Cyclotomic Polynomial

Instructor: Piyush P Kurur *Scribe: Ramprasad Saptharishi*

Overview

We started looking at the AKS primality test in the last class. The idea was to check if $(X+a)^n - X^n - a = 0 \pmod{n, X^r - 1}$ for many values for a. We first need to understand the polynomial $X^r - 1$ and extensions associated with it.

1 The polynomial $X^r - 1 = 0$

The roots of this polynomial are the r-th roots of unity. Over $\mathbb{Q}$ these are the complex numbers $e^{\frac{2\pi i}{r}}$ where $0 \leq i \leq r-1$.

Note that the roots of unity form a group under multiplication. If ζ_1 and ζ_2 are roots, then so is $\zeta_1\zeta_2$. Infact, it forms a cyclic group. And therefore, we can talk about a generator of this group.

Definition 1. *An r-th root of unity ζ is called a primitive r-th root of unity if ζ is a generator of the group of roots.*

Or in other words, ζ is a number such that $\zeta^r = 1$ and $\zeta^t \neq 1$ for any $t < r$.

Now, let ζ be a primitive r-th root of unity. What are the other primitive roots? Any other root ζ' can be written as ζ^t. Suppose the $\gcd(r,t) = d$ then look at $\zeta'^{r/d}$. Since d divides r, the exponent is an integer.

$$\zeta'^{r/d} = \zeta^{tr/d} = (\zeta^r)^{t/d} = 1$$

Therefore, the primitive r-th roots of unity are ζ^t where t is coprime with r. And therefore, there are $\varphi(r)$ of them. Let us consider the following polynomial:

$$\Phi_r(X) = \prod_{\zeta \text{ primitive}} (X - \zeta)$$

This is called the r-th cyclotomic polynomial. Clearly, the degree of $\Phi_r(X)$ is $\varphi(r)$.

1.1 Cyclotomic Polynomials over $\mathbb{Q}$

Let us restrict our attention to the field of rational numbers. We want to study $\prod(X - \zeta)$. The first important property is the following:

Proposition 1. *The coefficients of $\Phi_r(X)$ are rational numbers.*

Proof. The idea is quite simple. The equation $X^r - 1$ has all the r-th roots of unity as roots and certainly includes the primitive roots as well. Therefore, $\Phi_r(X)$ divides $X^r - 1$. So the idea is to eliminate all the non-primitive roots of unity.

Note that since the roots of unity form a group under multiplication, for any root of unity ζ the order of ζ divides r. So the order could either be r or some proper factor of r. We are interested in only the ζs whose order is equal to r.

For every ζ, if the order of ζ is t, then $t \mid r$ and ζ is a root of $\Phi_t(X)$ by definition. And running over all the roots of unity, we have

$$X^r - 1 = \prod_{d|r} \Phi_d(X)$$

And therefore,

$$\Phi_r(X) = \frac{X^r - 1}{\prod_{d|r, d \neq r} \Phi_d(X)}$$

By induction, if we assume that $\Phi_d(X)$ has rational coefficients, for all $d < r$, it follows that $\Phi_r(X)$ has rational coefficients too. □

To see a few examples,

1. $\Phi_1(X) = X - 1$
2. $\Phi_2(X) = \frac{X^2-1}{X-1} = X + 1$
3. $\Phi_3(X) = \frac{X^3-1}{X-1} = X^2 + X + 1$
4. $\Phi_4(X) = \frac{X^4-1}{(X+1)(X-1)} = X^2 + 1$

And if you notice, the coefficients are not only rationals but infact integers. This can be got from the earlier proof using the following very useful lemma.

Lemma 2 (Gauss Lemma)**.** *Let f be a monic polynomial with integer coefficients. If f is irreducible in $\mathbb{Z}$, that is there are no polynomials g, h with integer coefficients such that $f(X) = g(X)h(X)$, then f is irreducible over $\mathbb{Q}$ as well.*

Therefore if f and g are integer monic polynomials such that there g divides f over $\mathbb{Q}$, that is there exists a polynomial h with rational coefficients such that $f(X) = g(X)h(X)$, the g infact divides f over $\mathbb{Z}$ or h infact has only integer coefficients. Thus all the above divisions will only yeild integer polynomials and hence $\Phi_r(X)$ is an integer polynomial.

Another important property of cyclotomic polynomials is that they are irreducible over $\mathbb{Q}$. We shall prove this soon. But what's important is that it needn't be so in the case of finite fields. For example, if $r = p - 1$ and we looked at $\Phi_r(X)$ in $\mathbb{F}_p$. Note that $\Phi_r(X)$ is a factor of $X^r - 1 = X^{p-1} - 1$ which inturn is a factor of $X^p - X$ and this completely splits.

However, if we can show that $\Phi_r(X)$ was irreducible over some prime p, then it has to be irreducible over $\mathbb{Q}$. Because if it were reducible as $f(X) \cdot g(X)$ over $\mathbb{Q}$, then we can reduce the equation $\Phi_r(X) = f(X)g(X) \bmod p$ and get a factorization in $\mathbb{F}_p$.

1.2 Cyclotomic polynomials over $\mathbb{F}_p$

Let ζ be a primitive r-th root of unity over $\mathbb{F}_p$. Note that ζ could very well be in $\mathbb{F}_p$ itself; when $r = p - 1$ for example. In any case, consider the field extensio $\mathbb{F}_p(\zeta)$ over $\mathbb{F}_p$ by just adjoining ζ to $\mathbb{F}_p$. Let us say the degree of this extension $[\mathbb{F}_p(\zeta) : \mathbb{F}_p] = d$.

Recall that the degree of a field extension $[K(\alpha) : K]$ is the degree of the $K(\alpha)$ as vector space over K and therefore is equal to the degree of the minimum polynomial of α over K.

Therefore, if $\mu(X)$ is the minimum polynomial of ζ over $\mathbb{F}_p$, $\mu(\zeta) = a_0 + a_1\zeta + \cdots a_d\zeta^d = 0$ and therefore the set $1, \zeta, \zeta^2, \cdots, \zeta^{d-1}$ is the largest linearly independent subset. Therefore, $[\mathbb{F}_p(\zeta) : \mathbb{F}_p] = \deg \mu(X) = d$.

Now, ζ is a root. What about the other roots of this polynomial? Recall our old friend Fröbenius. The automorphism $a \mapsto a^p$ fixes every element in $\mathbb{F}_p$.

$$\begin{aligned}
\mu(\zeta) &= a_0 + a_1\zeta + \cdots + a_d\zeta^d = 0 \\
\implies (\mu(X))^p &= 0 \\
&= \left(a_0 + a_1\zeta + \cdots + a_d\zeta^d\right) \\
&= a_0^p + a_1^p\zeta^p + \cdots + a_d^p\zeta^{dp} \\
&= a_0 + a_1\zeta^p + \cdots + a_d(\zeta^p)^d \\
&= \mu(\zeta^p)
\end{aligned}$$

and hence, ζ^p is also a root. Applying the map again, we can show $\zeta, \zeta^p, \zeta^{p^2}, \cdots, \zeta^{p^{d-1}}$ are all roots of $\mu(X)$.

One can't go up to more than d such applications because the degree of μ is bounded by d and therefore can have only d roots. And if we were to apply the Fröbenius map again, then we would end up in ζ again. Or in other words,

$$\zeta^{p^d} = \zeta \implies \zeta^{p^d-1} = 1 \implies r \mid p^d - 1 \implies p^d = 1 \bmod r$$

Since d was the first place where this sort of wraparound happened, d is the least such number such that $p^d = 1 \bmod r$ which implies that d is the order of p modulo r. This is denoted by $d = ord_r(p)$.

Thus, the degree of the the minimum polynomial of ζ over $\mathbb{F}_p$ for any primitive r-th root is $ord_r(p)$. And since we just specified ζ as any primitive root, it follows that every primitive root has the degree of its minimum polynomial as $ord_r(p)$.

But with a little thought, this will tell us that the approach that $\Phi_r(X)$ is irreducible in $\mathbb{F}_p$ for some p may not work. Suppose this was true, then the minimum polynomial of ζ must infact be $\Phi_r(X)$. And from what we have proved above, the degree of this polynomial must be $ord_r(p)$ and therefore $\varphi(r) = ord_r(p)$. Now notice that if we consider $(\mathbb{Z}/r\mathbb{Z})^\star$, then the size of this group is $\varphi(r)$ and if $ord_r(p) = \varphi(r)$, then p generates the group $(\mathbb{Z}/r\mathbb{Z})^\star$. But not all $(\mathbb{Z}/n\mathbb{Z})^\star$s are cyclic and therefore such a p may not exist at all.

But let us just take it on faith that the cyclotomic polynomial is irreducible. The proof is not hard but would be a significant digression. The interested reader can look it up online or on any abstract algebra text. But what is important that any primitive r-th root has a minimum polynomial of degree $ord_r(p)$ in $\mathbb{F}_p$.

2 AKS Primality Test: A sketch

Now we have enough machinary to go ahead with the primality test. The algorithm would be the following:

1. Find two numbers r and l based on some requirements
2. Do some small preprocessing
3. For all $1 \leq a \leq r$, check if the following identity holds

$$(X + a)^n = X^n + a \pmod{n, X^r - 1}$$

Use repeated squaring to evaluate the LHS and RHS and check.

If any of the test failed, output COMPOSITE.

4. If all the above tests succeeded, output PRIME

Our preprocessing steps would be the following:

- Check if n is a perfect power of some number. If it is some non-trivial power, output COMPOSITE. This will rule out the case that $n = p^k$ for $k \geq 2$.
- For each $2 \leq d \leq r$, check if $\gcd(n, d) = 1$. If you find a factor, output COMPOSITE.

And the parameters will be fixed soon and we shall see that both r and l are less than $(\log n)^c$ for some constant c. Therefore, the preprocessing steps take only polylog time, checking if the identity holds for each a in that range also takes polylog time and therefore the entire algorithm runs in time polynomial in $\log n$.

Further, if n was indeed a prime, the algorithm would definitely output PRIME. The tricky part is to show that if n had atleast 2 distinct prime factors, the algorithm will catch it.

To prove the correctness of this algorithm, we would be studying 2 rings:

- $R = \frac{\mathbb{Z}[X]}{(n, X^r - 1)} = (\mathbb{Z}/n\mathbb{Z}[X]) / (X^r - 1)$
- $R = \frac{\mathbb{Z}[X]}{(p, h(X))} = (\mathbb{Z}/p\mathbb{Z}[X]) / (h(X))$ where p is a prime factor of n and $h(X)$ is an irreducible factor of $\Phi_r(X)$ over $\mathbb{F}_p$. Note that we have shown that $t = \deg(h(X)) = ord_r(p)$.

Suppose the algorithm said n was a prime even when it had p as a prime factor of n. What we would do is construct a group $\mathcal{G}$ and get bounds on the size of $\mathcal{G}$ in two different ways. We will show that $|\mathcal{G}| \geq \binom{t+l}{t-1}$. And also, if n had at least 2 distinct prime factors, then $|\mathcal{G}| \leq n^{\sqrt{t}}$. Thus, unifying the two, we have

$$\binom{t+l}{t-1} \leq \mathcal{G} \leq n^{\sqrt{t}}$$

And then, with suitable choice of r and l, we shall show that the lower bound is larger than the upper bound which would give the required contradiction. That is the general idea.

We shall see this in detail in the next class.