Lecture 12
Cyclotomic Polynomials, Primes Congruent to 1 mod n

Cyclotomic Polynomials - just as we have primitive roots mod p, we can have primitive n^{th} roots of unity in the complex numbers. Recall that there are n distinct nth roots of unity - ie., solutions of $z^n = 1$, in the complex numbers. We can write them as $e^{2\pi ij/n}$ for $j = 0, 1, \dots n-1$. They form a regular n-gon on the unit circle.

We say that z is a primitive nth root of unity if $z^d \neq 1$ for any d smaller than n. If we write $z = e^{2\pi ij/n}$, this is equivalent to saying $(j, n) = 1$. So there are $\phi(n)$ primitive nth roots of unity.

Eg. 4th roots of 1 are solutions of $z^4 - 1 = 0$, or $(z-1)(z+1)(z^2+1) = 0 \Rightarrow z = 1, -1 \pm i$

Now 1 is a primitive first root of unity, -1 is a primitive second root of unity, and $\pm i$ are primtiive fourth roots of unity. Notice that $\pm i$ are roots of the polynomial $z^2 + 1$. In general, define

$$\Phi_n(x) = \prod_{\substack{(j,n)=1 \\ 1 \leq j \leq n}} (x - e^{2\pi ij/n})$$

This is the nth **cyclotomic polynomial**.

We'll prove soon that $\Phi_n(x)$ is a polynomial with integer coefficients. Another fact is that it is **irreducible**, ie., cannot be factored into polynomials of smaller degree with integer coefficients (we won't prove this, however).

Anyway, here is how to compute $\Phi_n(x)$: take $x^n - 1$ and factor it. Remove all factors which divide $x^d - 1$ for some $d|n$ and less than n.

Eg. $\Phi_6(x)$. Start with $x^6 - 1 = (x^3-1)(x^3+1)$. Throw out $x^3 - 1$ since $3|6$ and $3 < 6$. $x^3 + 1 = (x+1)(x^2 - x + 1)$. Throw out $x + 1$ which divides $x^2 - 1$, since $2|6, 2 < 6$. We're left with $x^2 - x + 1$ and it must be $\Phi_6(x)$ since it has the right degree $2 = \varphi(6)$ (the nth cyclotomic polynomial has degree $\varphi(n)$, by definition).

If you write down the first few cyclotomic polynomials you'll notice that the coefficient seems to be 0 or ± 1. But in fact, $\Phi_{105}(x)$ has -2 as a coefficient, and the coefficients can be arbitrarily large if n is large enough.

These polynomials are very interesting and useful in number theory. For instance, we're going to use them to prove that given any n, there are infinitely many primes congruent to $1 \mod n$.

Eg. $\Phi_4(x) = x^2 + 1$ and the proof for primes $\equiv 1 \mod 4$ used $(2p_1 \dots p_n)^2 + 1$

Proposition 45. *1.* $x^n - 1 = \prod \Phi_n(x)$

2. $\Phi_n(x)$ *has integer coefficients*

3. For $n \geq 2$, $\Phi_n(x)$ *is reciprocal; ie.,* $\Phi_n(\frac{1}{x}) \cdot x^{\varphi(n)} = \Phi_n(x)$ *(ie., coefficients are palindromic)*

Proof. **1.** is easy - we have

$$x^n - 1 = \prod_{1 \leq j \leq n} (x - e^{2\pi i j/n})$$

If $(j,n) = d$ then $e^{2\pi i j/n} = e^{2\pi i j'/n'}$ where $j' = \frac{j}{d}, n' = \frac{n}{d}$, and $(j', n') = 1$. $(x - e^{2\pi i j'/n'})$ is one of the factors of $\Phi_{n'}(x)$ and $n'|n$. Looking at all possible j, we recover all the factors of $\Phi_{n'}(x)$, for every n' dividing n, exactly once. So

$$x^n - 1 = \prod_{n'|n} \Phi_{n'}(x)$$

2. By induction. $\Phi_1(x) = x - 1$. Suppose true for $n < m$. Then

$$x^m - 1 = \prod_{d|m} \Phi_d(x) = \underbrace{\left(\prod_{\substack{d|m \\ d<m}} \Phi_d(x) \right)}_{\substack{\text{monic (by defn), integer} \\ \text{coefficients (by ind. hypothesis)}}} \cdot \Phi_m(x)$$

So $\Phi_m(x)$, obtained by dividing a polynomial with integer coefficients, by a monic polynomial with integer coefficients, also has integer coefficients. This completes the induction.

3. By induction. True for $n = 2$, since $\Phi_2(x) = x + 1$.

$$\Phi_2\left(\frac{1}{x}\right) x^{\varphi(2)} = \left(\frac{1}{x} + 1\right) x = x + 1 = \Phi_2(x)$$

Suppose true for $n < m$. If we plug in $\frac{1}{x}$ into

$$\begin{aligned} x^m - 1 &= \prod_{d|m} \Phi_d(x) \\ \left(\frac{1}{x}\right)^m - 1 &= \prod_{d|m} \Phi_d\left(\frac{1}{x}\right) \\ &= \left(\prod_{\substack{1<d<m \\ d|m}} \Phi_d\left(\frac{1}{x}\right) \right) \cdot \Phi_m\left(\frac{1}{x}\right) \cdot \left(\frac{1}{x} - 1\right) \end{aligned}$$

Multiply by $x^m = \sum_{x^d|m} \varphi(d) = \prod_{d|m} x^{\varphi(d)}$ - proved before - to get

$$
\begin{aligned}
1 - x^m &= \left(\prod_{\substack{1<d<m \\ d|m}} \Phi_d\left(\frac{1}{x}\right) x^{\varphi(d)} \right) \cdot \Phi_m\left(\frac{1}{x}\right) x^{\varphi(m)} \cdot \left(\frac{1}{x} - 1\right) x \\
-(x^m - 1) &= \left(\prod_{\substack{1<d<m \\ d|m}} \underbrace{\Phi_d(x)}_{\text{by ind hyp}} \right) \cdot \Phi_m\left(\frac{1}{x}\right) x^{\varphi(m)} \cdot (1 - x) \\
-\prod_{d|m} \Phi_d(x) &= \left(\prod_{\substack{1<d<m \\ d|m}} \Phi_d(x) \right) \cdot \Phi_m\left(\frac{1}{x}\right) x^{\varphi(m)} \cdot (-\Phi_1(x))
\end{aligned}
$$

Cancelling almost all the factors we get

$$\Phi_m(x) = \Phi_m\left(\frac{1}{x}\right) x^{\varphi(m)}$$

completing the induction. ∎

Lemma 46. *Let $p \nmid n$ and $m|n$ be a proper divisor of n (ie., $m \neq n$). Then $\Phi_n(x)$ and $x^m - 1$ cannot have a common root mod p.*

Proof. By contradiction. Suppose a is a common root mod p. Then $a^m \equiv 1 \mod p$ forces $(a, p) = 1$. Next,

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x) \prod_{\substack{d|n \\ d<n}} \Phi_d(x)$$

Notice that $x^m - 1 = \prod_{d|n} \Phi_d(x)$ has all its factors in the last product. So this shows $x^n - 1$ has a double root at a, ie., $(x^n - 1) \equiv (x - a)^2 f(x) \mod p$ for some $f(x)$. Then the derivative must also vanish at $a \mod p$, so $na^{n-1} \equiv 0 \mod p$.

But $p \nmid n$ and $p \nmid a$, a contradiction. ($\lightning$) ∎

Now, we're ready to prove the main theorem.

Theorem 47. *Let n be a positive integer. There are infinitely many primes congruent to $1 \mod n$.*

Proof. Suppose not, and let $p_1, p_2, \ldots p_N$ be all the primes congruent to $1 \mod n$. Choose some large number l and let $M = \Phi_n(lnp_1 \ldots p_N)$. Since $\Phi_n(x)$ is monic, if l is large enough, M will be > 1 and so divisible by some prime p.

First, note that p cannot equal p_i for any i, since $\Phi_n(x)$ has constant term 1, and so p_i divides every term except the last of $\Phi_n(lnp_1 \ldots p_n) \Rightarrow$ it doesn't divide M. For the same reason we have $p \nmid n$. In fact, $(p, a) = 1$ where $a = lnp_1 \ldots p_N$.

Now $\Phi_n(a) \equiv 0 \mod p$ by definition, which means $a^n \equiv 1 \mod p$. By the lemma, we cannot have $a^m \equiv 1 \mod p$ for any $m|n, m < n$. So the order of $a \mod p$ is exactly n, which means that $n|p-1$ since $a^{p-1} \equiv 1 \mod p \Rightarrow p \equiv 1 \mod n$, exhibiting another prime which is $\equiv 1 \mod n$. Contradiction. ($\lightning$) ■

Note - we did not even need to assume that there's a single prime $\equiv 1 \mod n$; if $N = q$ take the empty product, ie., 1, and we end up looking at $\Phi_n(ln)$ for large l.

18.781 Theory of Numbers
Spring 2012