Lecture 6 - Fermat's Little Theorem & Euler's Formula

In this lecture we will study powers of congruences and prove two important results, Fermat's little theorem and Euler's formula, which can be very useful in solving congruence equations.

First we prove an easy lemma which will be helpful in the proofs to come.

Theorem

Let p be a prime, and a any number which is not a multiple of p. Then

$$\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\} = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$$

where $\overline{x}$ denotes the congruence class of x modulo p. That is, multiplying by a, $\overline{a} \neq 0 \pmod{p}$, simply re-orders congruence classes modulo a prime p.

pf

We first show that no two elements of $\{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$ are the same — i.e., none of them are congruent to one another. We'll proceed by contradiction. Suppose $\overline{ia} = \overline{ja}$ with $i \neq j$ and $1 \leq j, i, \leq p-1$. That is $ia \equiv ja \pmod{p}$. But this means $p \mid (ia - ja)$, so $p \mid (i-j)a$. Recall that we're assuming $p \nmid a$, and so $p \mid (i-j)$ — b/c p is prime.

Since $1 \leq i, j \leq p-1$, $\quad i-j < p-1$ and $i-j > -(p-1)$.

That is, $|i-j| < p-1$. But what numbers between $-(p-1)$ and $p-1$ are divisible by p? Only 0! Thus $i-j=0$, so $i=j$. However, we've explicitly chosen i and j so that they are not equal, and so it must be that ia and ja are in different congruence classes.

So, $\{\bar{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$ contains $p-1$ distinct congruence classes, and there are only $p-1$ non-zero distinct congruence classes. Hence

$$\{\bar{a}, \overline{2a}, \ldots, \overline{(p-1)a}\} = \{\bar{1}, \bar{2}, \ldots, \overline{(p-1)}\}. \qquad \square$$

Corollary

Recall that $n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$.

The result above implies that

$$(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$$

Pf

$$\overline{(p-1)a} \cdot \overline{(p-2)a} \cdot \ldots \cdot \overline{2a} \cdot \overline{a}$$
$$= \overline{(p-1)} \cdot \overline{(p-2)} \cdot \ldots \cdot \bar{2} \cdot \bar{1} = \overline{(p-1)!}$$

(We're multiplying the same congruence classes, but possibly in a different order.)

But

$$\overline{(p-1)a} \cdot \overline{(p-2)a} \cdot \ldots \cdot \overline{2a} \cdot \overline{a}$$
$$= \overline{(p-1)} \cdot \overline{(p-2)} \cdot \ldots \cdot \bar{2} \cdot \bar{1} \cdot \underbrace{\bar{a} \cdot \bar{a} \cdots \bar{a}}_{p-1 \text{ times}}$$
$$= \overline{a^{p-1} \cdot (p-1)!}$$

$\square$

Now we can easily prove Fermat's little theorem:

Theorem (Fermat's Little Theorem)

If p is any prime and a any number which is not a multiple of p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Pf

By the corollary above,

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}.$$

Notice that $(p-1)!$ and p are relatively prime: if $p \mid (p-1)!$, then p would have to divide one of $p-1, p-2, \ldots, 3, 2,$ or 1 — but it does not divide any of these. The gcd of p and any number x will be either 1 or p, but if it's p, then $p \mid x$. As $p \nmid (p-1)!$, $\gcd(p, (p-1)!) = 1$, so p and $(p-1)!$ are relatively prime.

Thus

$$a^{p-1} \cdot (p-1)! \equiv 1 \cdot (p-1)! \pmod{p}$$
$$\Longrightarrow a^{p-1} \equiv 1 \pmod{p}.$$

□

One neat application of Fermat's ~~test~~ little theorem is that it gives a litmus test for determining that a number is not prime.

Suppose we're given a number q which we may believe to be prime. If we could also find an a, $q \nmid a$, such that $a^{q-1} \not\equiv 1 \pmod{q}$, then there's no way that q can be prime. Thus we determine q is composite, without knowing any of its factors!

*

Fermat's little theorem only applies when we're looking at congruences modulo a prime, so we may ask what happens for congruences modulo a composite number: is there any sort of generalization to Fermat's little theorem for these congruences? Let's first consider some examples.

First an example to show Fermat's ~~last~~ little theorem does not work for composite numbers: if it did, then we'd have $3^{29} \equiv 1 \pmod{30}$. However, this would mean $30 \mid 3^{29}-1$, which would mean for some z, $30z = 3^{29}-1$, but this would mean $3^{29} - 30z = 1$. We could then set $x = 3^{28}$, $y = -z$ and we'd have a solution to

$$3x + 30y = 1$$

However, we know this equation has no solutions! Hence $3^{29} \not\equiv 1 \pmod{30}$, so Fermat's little theorem does not apply for

composite numbers.

Generalizing, it's not difficult to show that $3^\alpha \not\equiv 1 \pmod{30}$ for <u>any</u> α: if it did, then $30z = 3^\alpha - 1$ for some z, and $x = 3^{\alpha-1}$, $y = (-z)$ would be a solution to

$$3x + 30y = 1$$

but this equation has no solutions. Hence for every α, $3^\alpha \not\equiv 1 \pmod{30}$.

The issue here is that $\gcd(3, 30) \neq 1$. So let's pick a number which is relatively prime to 30 — say 7. Even here $7^{29} \not\equiv 1 \pmod{30}$, but justifying this obviously can't rely on rewriting the congruence as a linear Diophantine equation, since there <u>are</u> solutions to

$$7x + 30y = 1.$$

It turns out that $7^{29} \equiv 7 \pmod{30}$.

So is there any number we can raise to the 29th power and get something congruent to 1 mod 30? If so, we know that number must be relatively prime to 30. The numbers < 30 which are relatively prime to 30 are

1, 7, 11, 13, 17, 19, 23, and 29.

What happens when we raise these to 29?

$$7^{29} \equiv 7 \pmod{30}$$
$$11^{29} \equiv 11 \pmod{30}$$
$$13^{29} \equiv 13 \pmod{30}$$
$$17^{29} \equiv 17 \pmod{30}$$
$$19^{29} \equiv 19 \pmod{30}$$
$$23^{29} \equiv 23 \pmod{30}$$
$$29^{29} \equiv 29 \pmod{30}$$

So, Fermat's little theorem seems to completely fail for congruences modulo 30—at least if we're raising everything to the 29^{th} power. But could there be another power that works?

To show there is another power making $7^y \equiv 1 \pmod{30}$, as well as $11^y \equiv 1 \pmod{30}$, $13^y \equiv 1 \pmod{30}$, and so on, we need to discuss Euler's totient function.

Euler's totient function, φ, is a function $\varphi: \mathbb{N} \to \mathbb{N}$ which is defined to give the number of values, $\varphi(n)$, between 1 and n which are relatively prime to n.

$$\varphi(n) = \#\{a \mid 1 \le a \le n, \ \gcd(a,n) = 1\}.$$

For example, $\varphi(30)=8$ because there are eight numbers between 1 and 30 which are relatively prime to 30. $\varphi(6)=2$ as there are only 2 numbers between 1 and 6 which are relatively prime to 6 (1 and 5). (Notice if p is prime, $\varphi(p)=p-1$.)

Theorem (Euler's Formula)

If $\gcd(a,m)=1$, then

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Pf

The proof of Euler's formula is almost exactly like the proof for Fermat's ~~last~~ little theorem, so I'll leave it to you to modify the proof of Fermat's little theorem to get Euler's formula. (Try it on your own, but read the proof in the book — pg. 72-73 — if you get stuck. □

A very reasonable question to ask at this point is how do we compute $\varphi(n)$ in an efficient way, other than computing $\gcd(a,n)$ for each $1 \le a \le n$. As we'll see, assuming we can determine the prime factorization of n, $\varphi(n)$ is actually very easy to compute.

Lemma

If p is prime, then

$$\varphi(p) = p-1$$

Pf

Very easy exercise.

Lemma

If p is prime, then

$$\varphi(p^k) = p^k - p^{k-1}$$

Pf

We need to count the numbers $1 \le a \le p^k$ which are relatively prime to p^k. Notice that the divisors of p^k are just powers of p: $p, p^2, p^3, \dots, p^{k-2}, p^{k-1}, p^k$. Thus, the only way $\gcd(a, p^k) \neq 1$ is if $\gcd(a, p^k) = p^j$. In particular, a number $1 \le a \le p^k$ will be relatively prime to p^k iff $p \nmid a$. So we need to remove all the multiples of p from $1 \le a \le p^k$. These multiples are

$$p, 2p, 3p, \dots, (p-1)p, p^2, (p+1)p, \dots, (p^{k-1}-1)p, p^k$$

These multiples all have the form $j \cdot p$ with $1 \le j \le p^{k-1}$, hence there are p^{k-1} multiples of p in $1, 2, \dots, p^k$. Removing these multiples, there are $p^k - p^{k-1}$ numbers in $1, 2, \dots, p^k$ which are relatively prime to p^k. □

Now if we can compute $\varphi(pq)$ for distinct primes p and q, we'll basically be done. We will postpone this calculation until after we've discussed the Chinese remainder theorem in the next lecture.