CLASS 13, GIVEN ON 10/20/2010, FOR MATH 25

1. Polynomial congruences mod p

Let's think about polynomial congruences mod p, where p is a prime. The previous proposition, which considered $x^2 \equiv 1 \mod n$, showed that this equation can have many more than 2 solutions, at least when n has multiple prime divisors. In contrast, $ax \equiv b \mod n$ has at most one solution.

If we think about the number of solutions to $f(x) = 0$ when considered as an equation over integers, real numbers, or complex numbers, a fundamental result is that $f(x) = 0$ has at most d solutions, where d is the degree of $f(x)$. As a matter of fact, the fundamental theorem of algebra (first proved by Gauss...) says that $f(x) = 0$ has exactly d complex solutions, when those solutions are appropriately counted with multiplicity.

So in general, $f(x) \equiv 0 \mod n$ violates what we expect to be true from thinking about polynomials over real or complex numbers. Is there a situation where $f(x) \equiv 0 \mod n$ has at most d solutions? The answer is yes, as the following theorem shows:

Theorem 1 (Theorem 4.1)**.** *Let $f(x) = a_d x^d + \ldots + a_0$ be a polynomial with integer coefficients, with $a_d \neq 0$ and some $a_i \not\equiv 0 \mod p$. Let p be a prime number. Then $f(x) \equiv 0 \mod p$ has at most d solutions mod p.*

Proof. We will prove this result using induction. When $d = 0, 1$, the result is clear; for instance, when $d = 0$, then $f(x) = a_0$, and $p \nmid a_0$, so $a_0 \equiv 0 \mod p$ has no solutions. When $d = 1$, the fact that $a_1 x + a_0 \equiv 0 \mod p$ has at most one solution mod p is a consequence of the fact that $\gcd(a_1, p) = 1$ if $p \nmid a_1$.

Let us assume that the result is true for polynomials of degree $d - 1$. Let $f(x) = a_d x^d + \ldots + a_0$ be a polynomial of degree d we are trying to prove the result for. Suppose that $a \mod p$ solves $f(x) \equiv 0 \mod p$. Then $f(a) = a_d a^d + \ldots + a_0 \equiv 0 \mod p$. Now consider the polynomial $f(x) - f(a)$. This is equal to

$$f(x) - f(a) = a_d(x^d - a^d) + \ldots + a_1(x - a).$$

Notice that we can factor $(x - a)$ from every term on the right hand side. This gives

$$f(x) - f(a) = (x - a)((a_d(x^{d-1} + x^{d-2}a + \ldots + a^{d-1}) + \ldots + a_1).$$

The remaining term we get when we factor $x - a$ out is very complicated, but it is a polynomial of degree $d - 1$. Let us call it $g(x)$. Then $f(x) - f(a) = (x - a)g(x)$.

How many solutions mod p does $f(x) \equiv 0 \mod p$ have? Since $f(a) \equiv 0 \mod p$, this has the same number of solutions as $f(x) - f(a) = (x - a)g(x) \equiv 0 \mod p$ has. And this has a solution precisely when $p | (x - a)g(x)$. Let's count how many solutions this has. We either have $p | (x - a)$ or $p | g(x)$. In the former case, $x \equiv a \mod p$. In the latter case, $g(x) \equiv 0 \mod p$. We now use the inductive hypothesis on $g(x)$, which is a polynomial of degree d.

However, to be sure we can use the inductive hypothesis, we need to check that there is a coefficient of $g(x)$ not divisible by p. Suppose every coefficient of $g(x)$ were divisible by p. Then expanding out $(x - a)(g(x)) = f(x) - f(a)$, we find that every coefficient of $f(x) - f(a)$, and hence $f(x)$, is divisible by p, contradicting our original assumption on $f(x)$.

So the inductive hypothesis on $g(x)$ tells us $g(x)$ has at most $d-1$ roots mod p. Since $f(x) \equiv 0 \mod p$ if and only if $x \equiv a \mod p$ or $g(x) \equiv 0 \mod p$, there are at most d possible roots for $f(x) \equiv 0 \mod p$, as desired. □

This is a really important theorem. It is the first hint that moduli which are prime numbers preserve some of the familiar properties we know from real or complex numbers. This theorem is also instrumental in proving some important later results on $\mathbb{Z}/p\mathbb{Z}$.

Examples.

- The fact that p does not divide at least one coefficient of $f(x)$ is clearly necessary for this theorem to be true. If every coefficient of $f(x)$ were divisible by p, then $f(x) \equiv 0 \mod p$ regardless of the value of p, and then there would be p roots mod p. This is analogous to the situation where the constant polynomial $f(x) = 0$ has infinitely many roots over real or complex numbers.
- In contrast, the proposition does not require that the leading coefficient of $f(x)$ be not divisible by p. And if $p|a_d$, then for all intents and purposes we can replace $f(x)$ with a lower-degree polynomial if we are interested only in its values mod p. For instance, $3x^2 + 1 \equiv 1 \mod 3$ for any value of x.
- The fact that the modulus is prime is essential. We already saw that $x^2 \equiv 1 \mod n$ can have more than n solutions if n is not prime. Of course, there are some situations where $f(x) \equiv 0 \mod n$ will have d or fewer solutions, even if n is composite, but in general this will not happen.

We now prove another important theorem. This is a favorite in high school math competitions, but it also expresses a deep truth about numbers mod p.

Theorem 2 (Fermat's Little Theorem, Theorem 4.3)**.** *Let p be a prime, and let $p \nmid a$. Then $a^{p-1} \equiv 1 \mod p$.*

Proof. The book gives two proofs, but one of them uses a little bit of group theory, so we give the other. (If you know algebra, you should read the group theory proof. And even if you don't know algebra, you should know enough in a few weeks to go back and read this proof.)

Consider the numbers $1, 2, \dots, p-1$. These form what is known as a *complete set of (nonzero) residues* mod p: that is, this list of $p-1$ numbers consists of numbers which represent each of the $p-1$ nonzero congruence classes mod p exactly once. Another way of saying this is that $1, 2, \dots, p-1 \mod p$ are all the nonzero congruence classes mod p.

Consider the list of numbers $a, 2a, 3a, \dots, (p-1)a$. We claim that this is still a complete set of nonzero residues mod p. To do this, it is enough to show that any two numbers from this list are not congruent mod p, because then we have a list of $p-1$ integers which are all in distinct nonzero congruence classes mod p, and there are only $p-1$ of these, so that $a, 2a, \dots, (p-1)a \mod p$ are all of the distinct congruence classes mod p.

So consider ia, ja, where $1 \le i, j, \le p-1$. Suppose $ia \equiv ja \mod p$. Then $p \mid (ia - ja) = a(i-j)$. Since $p \nmid a$, we must have $p \mid (i-j)$. But since $1 \le i, j \le (p-1)$, we must have $i = j$. Therefore the ia are all inequivalent mod p as we let i vary from 1 to $p-1$.

One consequence of this is that $1 \cdot 2 \cdot \ldots (p-1) \equiv (a) \cdot (2a) \cdot \ldots \cdot (p-1)a \mod p$, or, in other words, $(p-1)! \equiv (p-1)!a^{p-1} \mod p$. Indeed, notice that each product is just the product of representatives from each of the $p-1$ nonzero congruence classes mod p. In particular, the right hand side is just a reordering of the terms on the left hand side, if we think of two numbers which are congruent mod p as the same.

But we also know that $\gcd(p, (p-1)!) = 1$. So we can cancel $(p-1)!$ from both sides of the above congruence to get $a^{p-1} \equiv 1 \mod p$, as desired. □

Examples.

- Here is a concrete example of the main idea behind the proof of Fermat's Little Theorem. Suppose we wish to prove the statement true for $a = 2, p = 5$. Then the list of numbers $1, 2, 3, 4$ form a complete set of representatives of nonzero congruence classes mod 5. Multiplying every number on this list by 2 gives $2, 4, 6, 8$, and one checks these still are a complete set of representatives of nonzero congruence classes mod 5, because $2, 4, 6, 8 \equiv 2, 4, 1, 3 \mod 5$, respectively. If you want, you can work out what happens with $a = 3, 4$ as well.
- A favorite type of calculation involving Fermat's Little Theorem (now abbreviated FLT, not to be confused with Fermat's Last Theorem) is something of the following type: compute $27^{3212363} \mod 11$ say. (In this problem, we really mean to find the remainder of $27^{3212363}$ when divided by 11.

  First, notice $27 \equiv 5 \mod 11$, so we can replace the base 27 with 5. Since $11 \nmid 5$, we have $5^{10} \equiv 1 \mod 11$. But this means that $5^{10k} \equiv 1 \mod 11$, for any positive integer k. Since the exponent 3212363 can be written as $3212363 = 10(321236) + 3$, this tells us that

$$5^{3212363} = 5^{10(321236)+3} = 5^{10(321236)} \cdot 5^3 \equiv 1 \cdot 5^3 \equiv 4 \mod 11.$$

- A corollary (corollary 4.4) is that $a^p \equiv a \mod p$, regardless of the value of the integer a. Indeed, if $p \nmid a$, just multiply both sides of the statement of FLT by a, and if $p|a$, then $a \equiv 0 \mod p$, and the statement is obviously true. Notice that we can only go from $a^p \equiv a \mod p$, which is true for all a, to $a^{p-1} \equiv 1 \mod p$, if a has a multiplicative inverse mod p; ie, if $\gcd(a, p) = 1$, which is the same as saying $p \nmid a$.

Using many of the same ideas as in the proof of Fermat's Little Theorem, we can prove the following interesting theorem:

Theorem 3 (Wilson's Theorem, Corollary 4.5)**.** *Let $n > 1$ be a positive integer. Then $(n-1)! \equiv -1 \mod n$ if and only if n is a prime.*

Proof. Suppose n is not prime; say $n = ab$, for $1 < a, b$. Then a appears in $(n-1)!$, so $a|(n-1)!$. Since $(n-1)! \equiv 0 \mod a$, this implies that $(n-1)! \equiv b, 2b, \ldots, (a-1)b \mod n$. Since $n > 1$ and $b > 1$, it is impossible for any of these numbers to be congruent to -1 mod n.

Now suppose $n = p$ is prime. Consider the set of numbers $1, 2, \ldots, p-1$. Let a be some number from this set not equal to 1 or $p-1$. We claim that there is exactly one other number b in this set such that $ab \equiv 1 \mod p$, and also that $b \neq a$. Indeed, since $\gcd(a, p) = 1$, we already know that a has a multiplicative inverse $a^{-1} \mod p$. So we take b to be the number on this list which belongs to the congruence class of $a^{-1} \mod p$, and this b is unique since $1, 2, \ldots, p-1$ represents each nonzero congruence class exactly once. If $a = b$, then $a^2 \equiv 1 \mod p$, or $a \equiv \pm 1 \mod p$, which says that $a = 1, p-1$, contradicting our original assumption on a.

In this way, we can pair off each of the $p-3$ numbers $2, 3, \ldots, p-2$ in such a way so that the product of the numbers in each pair is $1 \mod p$. In particular, this tells us that $(p-1)! \equiv 1(p-1) \equiv -1 \mod p$. □

Wilson's Theorem provides an alternate characterization of prime numbers, so perhaps one might think that Wilson's Theorem could be used as a primality test. Given an integer n, we compute $(n-1)!$, and then check if it is $\equiv -1 \mod n$. Indeed, this works, but the problem is that it apparently takes a lot of effort to compute $(n-1)! \mod n$; after all, to do this naively would require $n-2$ multiplications.

However, Fermat's Little Theorem does give us a way to possibly test for primality. Suppose we are given a number n, which we wish to test for primality. Suppose we compute $a^n \mod n$. If we find that $a^n \not\equiv a \mod n$, then we know that n must be composite, since if n were prime, $a^n \equiv a \mod n$ must be true.

To really check whether this is a good test for primality, we need to know a few things. First, is it possible to compute $a^n \mod n$ quickly? If so, is it the case that for every composite integer n, is there some a such that $a^n \not\equiv a \mod n$? These are the questions we will discuss in the next class.