

Math 104A, Number Theory, Fall 2002.
Summary of Lecture 25.

All polynomials here have integer coefficients.

Definition. The polynomials $f(x) = a_n x^n + \dots + a_0$ and $g(x) = b_n x^n + \dots + b_0$ are *congruent as polynomials modulo m* (written $f \equiv g \pmod{m}$) if $a_j \equiv b_j \pmod{m}$ for each j with $0 \leq j \leq n$. Another way of saying this is $f(x) - g(x) = ph(x)$ where h is a polynomial with integer coefficients.

Definition. For f as above, the degree of f modulo m is the largest j such that $m \nmid a_j$. If f is congruent to zero modulo m then the degree is undefined.

Theorem. Let p be prime and let $f(x)$ be a polynomial which is not congruent to zero as a polynomial modulo p .

(a). There exist integers r_1, \dots, r_k and a polynomial $g(x)$, such that g has no roots modulo p and

$$(*) \quad f(x) \equiv (x - r_1) \cdots (x - r_k) g(x) \pmod{p}.$$

(b). Moreover r_1, \dots, r_k are precisely the roots of f (possibly repeated more than once), and so by comparing the degree modulo p of both sides, the number of roots of f is at most n .

The fact that the number of roots of f is at most the degree of f is *Lagrange's Theorem*. The number of times the factor $(x - r)$ is repeated on the right hand side of (*) is called the *multiplicity* of the root r . The proof given above shows a bit more than Lagrange's Theorem. It shows that if r_1, \dots, r_k are the distinct roots of f and they have multiplicities m_1, \dots, m_k then the sum of the multiplicities $m_1 + \dots + m_k$ is bounded by the degree of f . We'll call this the *extended Lagrange Theorem*. We remark that if the multiplicity of the root r is 1 then the root is called *simple*.

Example. Consider $x^2 + x + c$ modulo 7.

x	0	1	2	3	4	5	6
$x(x + 1)$	0	2	6	5	6	2	0

We see that $x^2 + x$ has the two roots 0 and 6 modulo 7, while $x^2 + x - 5$ has the single root 3 modulo 7. This is actually a repeated root, $x^2 + x - 5 \equiv (x - 3)^2 \pmod{7}$. Furthermore, $x^2 + x - 4$ has no roots modulo 7. Note that if the quadratic polynomial $f(x)$ has just one root r modulo a prime p then that root must actually be repeated. (When you factor out the root r by writing $f(x) = (x - r)g(x)$ you are left with a linear factor $g(x)$ whose only root can be r .) This is only true for quadratic polynomials.

Example. For any prime p ,

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod{p}.$$

To see this, by Fermat, the roots of $x^{p-1} - 1$ modulo p are $1, 2, \dots, (p-1)$. By the Theorem,

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-(p-1))g(x) \pmod{p},$$

For some polynomial $g(x)$. By comparing degrees modulo p , we see that $g(x)$ is congruent as a polynomial to a constant, but comparing the coefficient of x^{p-1} on both sides, $g \equiv 1 \pmod{p}$ and we get the result.

Corollary 1. Let p be a prime and let $d|p-1$. Then $x^d - 1$ has d distinct roots modulo p and these are all simple.

Proof.

$$y^q - 1 = (y-1)(y^{q-1} + y^{q-2} + \cdots + 1)$$

Setting $y = x^d$ we have

$$x^{dq} - 1 = (x^d - 1)(x^{d(q-1)} + x^{d(q-2)} + \cdots + 1).$$

But now choose $q = (p-1)/d$. We have

$$x^{p-1} - 1 = (x^d - 1)(x^{p-1-d} + x^{p-1-2d} + \cdots + 1).$$

Define $h(x)$ to be the second factor on the right, $h(x) = x^{p-1-d} + x^{p-1-2d} + \cdots + 1$. By Fermat's Theorem, the left hand side has $p-1$ distinct roots modulo p and by Lagrange's Theorem, $h(x)$ has at most $p-1-d$ roots, so $x^d - 1$ has at least $p-1 - (p-1-d) = d$ distinct roots. Since this is the same as the degree, using Lagrange's Theorem again, $x^d - 1$ must have exactly d roots modulo p , and by the extended Lagrange Theorem these roots must all be simple.

Corollary 2. Let p be prime and suppose $d > 0$. Then $x^d - 1$ has $(d, p-1)$ distinct roots modulo p . (These may not be simple.)

Proof. We will show that

$$(**) \quad r^d \equiv 1 \pmod{p} \quad \Leftrightarrow \quad r^{(d, p-1)} \equiv 1 \pmod{p},$$

Hence the roots of $x^d - 1$ modulo p are precisely the roots of $x^{(d, p-1)-1}$ modulo p , and by the previous lemma there are exactly $(d, p-1)$ of these. To prove (**), first to show \Leftarrow , let $q = d/(d, p-1)$. Then

$$r^{(d, p-1)} \equiv 1 \pmod{p} \Rightarrow r^d \equiv \left(r^{(d, p-1)}\right)^q \equiv 1 \pmod{p}.$$

Conversely, if $r^d \equiv 1 \pmod{p}$ then by Proposition 4.1.5, $r^{(d, p-1)} \equiv 1 \pmod{p}$.