

Math 104A, Number Theory, Fall 2002.
Summary of Lecture 24.

All polynomials here have integer coefficients.

Example: Long Division of polynomials (for a linear divisor). The long division $x^4 - x^3 + 2x$ divided by $x - 3$,

$$x - 3 \overline{) x^4 - x^3 + 0x^2 + 2x + 0}$$

has a quotient $x^3 + 2x^2 + 6x + 20$ and a remainder 60.

Theorem For $f(x) = a_n x^n + \dots + a_0$ and an integer b , we can write $f(x) = (x-b)g(x) + c$ where g is a polynomial with degree $g = \text{degree } f - 1$ and c is an integer.

Proof. By induction on the degree of f . The result is clearly true when the degree of f is zero. Suppose that the assertion holds when the degree of f is less than n and now take $f(x) = a_n x^n + \dots + a_0$. Now the n th degree coefficient of f is a_n which is the same as the n th degree coefficient of $a_n x^n - b a_n x^{n-1} = (x-b)a_n x^{n-1}$. Hence $\tilde{f}(x) = f(x) - (x-b)a_n x^{n-1}$ has degree less than n . By induction, $\tilde{f}(x) = (x-b)\tilde{g}(x) + c$ where the degree of \tilde{g} is less than n . Then

$$f(x) = (x-b)(a_n x^{n-1} + \tilde{g}(x)) + c.$$

By induction, the result holds for all polynomials f .

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 $f(x) - g(x) = mh(x)$ where h is a polynomial with integer coefficients.

Example. $x^2 + x - 12 \equiv x^2 + x + 2 \pmod{7}$. However, although by Fermat's theorem we have $x^7 \equiv x \pmod{7}$ for every x , we do not have $x^7 \equiv x \pmod{7}$.

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.

Lemma If $f \equiv \tilde{f} \pmod{m}$ and $g \equiv \tilde{g} \pmod{m}$ then $f+g \equiv \tilde{f}+\tilde{g} \pmod{m}$ and $fg \equiv \tilde{f}\tilde{g} \pmod{m}$. Also $f(g(x)) \equiv \tilde{f}(\tilde{g}(x)) \pmod{m}$ as was noted by a member of the audience. If $m = p$ is prime then the degree of fg modulo p is the degree of f modulo p plus the degree of g modulo p .

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 .

Example. Consider $x^4 - 1$ modulo 5. By Fermat, the roots are 1, 2, 3, 4 modulo 5. By the Theorem

$$x^4 - 1 \equiv (x - 1)^{e_1}(x - 2)^{e_2}(x - 3)^{e_3}(x - 4)^{e_4}g(x) \pmod{5},$$

where the exponents $e_j > 0$. By comparing degrees and the coefficient of x^4 on both sides, $e_1 = \dots = e_4 = 1$ and $g(x) = 1$ and

$$x^4 - 1 \equiv (x - 1)(x - 2)(x - 3)(x - 4) \pmod{5}.$$

Proof of the Theorem. (a). We prove this by induction on the degree of f . Suppose it holds when the degree of f is less than n , and now take f whose degree is precisely n . If f has no root modulo p then we can take $g = f$ and no r s. If f has a root r modulo p . Then by long division we can write

$$f(x) = (x - r)\tilde{f}(x) + c$$

where the degree of \tilde{f} is $n - 1$. Then plugging in $x = r$ we get

$$0 \equiv f(r) \equiv c \pmod{p}$$

and so

$$f(x) \equiv (x - r)\tilde{f}(x) \pmod{p}.$$

By applying the inductive hypothesis to \tilde{f} we get (*) for f . By induction we are done.

(b). Clearly r_1, \dots, r_k are roots of f modulo p and if a is not one of the r_j s modulo p we have

$$f(a) \equiv (a - r_1) \cdots (a - r_k)g(a) \pmod{p}$$

which is a product of non-zero elements modulo p and hence non-zero modulo p . This shows that the roots modulo p are precisely r_1, \dots, r_k .