

## LECTURE 6: POLYNOMIAL CONGRUENCES MODULO PRIMES

### 1. LAGRANGE THEOREM

At this point we know that the number of solutions of a polynomial congruence modulo  $m$  is a multiplicative function of  $m$ , and thus it suffices to consider congruences modulo prime powers. We begin by investigating congruences modulo  $p$ , for prime numbers  $p$ .

**Definition 1.1.** Let  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$  be a polynomial with integral coefficients. Let  $j$  be the largest integer with  $m \nmid a_j$ . Then we say that the **degree** of  $f$  modulo  $m$  is  $j$ . If  $m \mid a_j$  for every  $j$ , then the degree of  $f$  is undefined.

**Theorem 1.2** (Lagrange). *Let a polynomial  $f \in \mathbb{Z}[x]$  have degree  $n$  (modulo  $p$ ), with  $n \geq 1$ . Then the congruence  $f(x) \equiv 0 \pmod{p}$  has at most  $n$  solutions.*

*Proof.* The situation when  $n = 1$  is clear, since we then have a linear equation to solve. Suppose then that  $n \geq 2$ , and that the conclusion of the theorem holds for all degrees smaller than  $n$ . Let  $f \in \mathbb{Z}[x]$  have degree  $n$  modulo  $p$ . Either  $f(x)$  has no zeros modulo  $p$ , or else there exists at least one zero, say  $x = a$ . Let  $g(x)$  be defined by means of the relation  $f(x) - f(a) = (x - a)g(x)$ . Since, for each natural number  $m$ ,  $(x^m - a^m)/(x - a)$  is a monic polynomial of degree  $m - 1$  with integer coefficients, it is apparent that  $g \in \mathbb{Z}[x]$  and that  $g$  has degree  $n - 1$  modulo  $p$ . Note that

$$f(x) = (x - a)g(x) + f(a) \equiv (x - a)g(x) \pmod{p},$$

and since  $p$  is a prime number it follows that whenever  $f(x) \equiv 0 \pmod{p}$ , one has either  $x \equiv a \pmod{p}$  or  $g(x) \equiv 0 \pmod{p}$ . But by our inductive hypothesis, the number of zeros of  $g(x) \pmod{p}$  is at most  $\deg g = n - 1$ , and hence the number of zeros of  $f(x) \pmod{p}$  is at most  $1 + (n - 1) = n$ . The desired conclusion therefore follows by induction.  $\square$

**Example 1.3.** It follows from Lagrange's Theorem that the congruence

$$x^2 + 1 \equiv 0 \pmod{p}$$

has at most 2 solutions for any prime  $p$ . We have shown that this congruence has precisely 2 solutions when  $p \equiv 1 \pmod{4}$ , and 0 solutions when  $p \equiv 3 \pmod{4}$ .

**Example 1.4.** It follows from Lagrange's Theorem that the congruence

$$x^p - x + 1 \equiv 0 \pmod{p}$$

has at most  $p$  solutions modulo  $p$ . In fact this congruence has no solutions for any prime  $p$ , because Fermat's Little Theorem shows that  $x^p \equiv x \pmod{p}$  for all  $x$ , whence  $x^p - x + 1 \not\equiv 1 \pmod{p}$  for every residue  $x$ .

**Example 1.5.** By Lagrange's Theorem, the congruence

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

has at most  $p - 1$  solutions modulo  $p$ , and it follows from Fermat's Little Theorem that these are  $x = 1, 2, \dots, p - 1$ . It follows from the proof of Lagrange's Theorem that we have the relation

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

Comparing coefficients of powers of  $x$ , we find from the constant coefficient in this relation that  $(p - 1)! \equiv -1 \pmod{p}$ , which we have already proved by different means.

**Example 1.6.** There is no analogue of Lagrange's Theorem for composite moduli. Consider for example the congruence  $x^2 \equiv 1 \pmod{8}$ . This is a congruence of degree 2, yet has 4 distinct solutions 1, 3, 5 and 7 modulo 8.

**Corollary 1.7.** *Whenever  $d \mid (p - 1)$ , the congruence  $x^d \equiv 1 \pmod{p}$  has precisely  $d$  solutions modulo  $p$ .*

*Proof.* Suppose that  $d \mid (p - 1)$ . Then there exists a polynomial  $g \in \mathbb{Z}[x]$  with  $x^{p-1} - 1 = (x^d)^{(p-1)/d} - 1 = (x^d - 1)g(x)$ . But the degree of  $g$  is  $p - 1 - d$ , and so by Lagrange's Theorem the congruence  $g(x) \equiv 0 \pmod{p}$  has at most  $p - 1 - d$  solutions modulo  $p$ . Then since  $x^{p-1} - 1$  has precisely  $p - 1$  zeros modulo  $p$ , we see from the above relation that  $x^d - 1$  has at least  $d$  zeros modulo  $p$ . But Lagrange's Theorem shows that the latter polynomial has at most  $d$  zeros modulo  $p$ , and thus we see that it has precisely  $d$  zeros modulo  $p$ . This completes the proof of the theorem.  $\square$

## 2. CHEVALLEY THEOREM

Now we consider congruences in more than one variables. In 1935 Artin conjectured that a polynomial congruence with prime modulus always has a non-trivial solution provided that the number of variables is greater than its degree. For example,  $x^2 + 2y^2 - 3z^2 \equiv 0 \pmod{p}$  always has at least one non-zero solution. We discuss a proof of this conjecture, which was given by Chevalley a year later.

**Definition 2.1.** Let  $f$  and  $g$  be polynomial in  $n$  variables.

(i)  $f$  is *equivalent* to  $g$  modulo  $p$ ,  $f \equiv g$ , if for all  $(a_1, \dots, a_n) \in \mathbb{Z}^n$ ,

$$f(a_1, \dots, a_n) \equiv g(a_1, \dots, a_n) \pmod{p}$$

(ii)  $f$  is *congruent* to  $g$ ,  $f \sim g$ , if all the coefficients of corresponding monomials of  $f$  and  $g$  are congruent modulo  $p$ .

(iii)  $f$  is *reduced* if it has degree less than  $p$  in each of the variables.

It is clear that if  $f \sim g$ , then  $f \equiv g$ . It follows from Fermat's theorem that every polynomial  $f$  is equivalent to a reduced polynomial  $\tilde{f}$  such that  $\deg(\tilde{f}) \leq \deg(f)$ .

The following theorem is an extension of Lagrange's theorem.

**Theorem 2.2.** *If  $f$  and  $g$  are reduced polynomials and  $f \equiv g$ , then  $f \sim g$ .*

*Proof.* Without loss of generality, we may assume that  $g$  is zero polynomial. Let  $n$  be the number of variables in  $f$ . The proof goes by induction on  $n$ . The case  $n = 1$  follows immediately from Lagrange's theorem because  $\deg(f) \leq p - 1$ . In the general case, we write

$$f(x_1, \dots, x_n) = f_{p-1}(x_1, \dots, x_{n-1})x_n^{p-1} + \dots + f_0(x_1, \dots, x_{n-1}).$$

Given  $a_1, \dots, a_{n-1} \in \mathbb{Z}$ , the equation

$$f_{p-1}(a_1, \dots, a_{n-1})x^{p-1} + \dots + f_0(a_1, \dots, a_{n-1}) \equiv 0 \pmod{p}$$

has  $p$  solutions. Hence, by Lagrange's theorem again,  $f_i(a_1, \dots, a_{n-1}) \equiv 0 \pmod{p}$ . This shows that  $g_i \equiv 0$ , and by induction,  $g_i \sim 0$ . This completes the proof.  $\square$

We say that a polynomial  $f(x_1, \dots, x_n)$  is *homogeneous* if all of its monomials have the same degree.

**Theorem 2.3.** *Let  $f$  be a homogeneous polynomial in  $n$  variables and  $1 \leq \deg(f) < n$ . Then the congruence*

$$f(x_1, \dots, x_n) \equiv 0 \pmod{p}$$

*has at least one non-zero solution.*

*Proof.* Suppose that in contrary this congruence has only zero solution. We consider the polynomial

$$h(x_1, \dots, x_n) = 1 - f(x_1, \dots, x_n)^{p-1}.$$

We have  $h(x_1, \dots, x_n) \equiv 1 \pmod{p}$  if  $x_1 \equiv \dots \equiv x_n \equiv 0 \pmod{p}$ , and By Fermat's theorem,  $h(x_1, \dots, x_n) \equiv 1 \pmod{p}$  for all the other residues. Let  $\tilde{h}$  be a reduced polynomial equivalent to  $h$  with  $\deg(\tilde{h}) \leq \deg(h)$ . We also consider the reduced polynomial

$$g(x_1, \dots, x_n) = \prod_{i=1}^n (1 - x_i^{p-1}).$$

It takes exactly the same values as  $h$  and  $\tilde{h}$ . So  $g \equiv \tilde{h}$ , and by the previous theorem,  $g \sim h$ . However,  $\deg(g) = n(p - 1)$ , but  $\deg(\tilde{h}) < n(p - 1)$ . This gives a contradiction.  $\square$