

# Chapter 8

## Congruences

**Material to be Appended to Chapter 8**

Nonlinear congruences are also very important in number theory. For example, solutions to the congruence

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

are square roots of  $-1$  modulo  $m$ . For some values of  $m$  such as  $m = 5$  and  $m = 13$ , there are solutions,

$$2^2 + 1 \equiv 0 \pmod{5} \quad \text{and} \quad 5^2 + 1 \equiv 0 \pmod{13},$$

while for other values such as  $m = 3$  and  $m = 7$ , there are no solutions.

You probably already know that a polynomial of degree  $d$  with real coefficients has no more than  $d$  real roots.<sup>1</sup> This well-known “fact” is not true for congruences, since for example the congruence

$$x^2 + x \equiv 0 \pmod{6}$$

has four distinct roots modulo 6, namely 0, 2, 3, and 5. However, if we look at congruences modulo primes, then order and harmony are restored to the world.

**Theorem 8.2 (Polynomial Roots Mod  $p$  Theorem).** *Let  $p$  be a prime number and let  $f(x) = x^d + a_1x^{d-1} + \cdots + a_d$  be a polynomial of degree  $d \geq 1$  with integer coefficients. Then the congruence*

$$f(x) \equiv 0 \pmod{p}$$

*has at most  $d$  incongruent solutions.*

---

<sup>1</sup>In fact, the Fundamental Theorem of Algebra (cf. Theorem 33.1 on page 240) says that a polynomial of degree  $d$  with complex coefficients always has exactly  $d$  roots, provided that you count multiple roots appropriately.

The proof is based on the idea of canceling solutions one-by-one until none are left. We use the fact that for any value of  $r$ , the difference  $f(x) - f(r)$  can be factored. To see this, we write

$$f(x) - f(r) = (x^d - r^d) + a_1(x^{d-1} - r^{d-1}) + \cdots + a_{d-1}(x - r).$$

Each term  $x^i - r^i$  has a factor of  $x - r$ , since

$$x^i - r^i = (x - r)(x^{i-1} + x^{i-2}r + x^{i-3}r^2 + \cdots + xr^{i-2} + r^{i-1}).$$

Pulling an  $x - r$  out of each term, we find that

$$f(x) - f(r) = (x - r)(\text{some messy polynomial of degree } d - 1).$$

More precisely,

$$f(x) = f(r) + (x - r)g(x)$$

for some polynomial

$$g(x) = x^{d-1} + b_1x^{d-2} + \cdots + b_{d-2}x + b_{d-1}.$$

Now let  $x = r_1, r_2, \dots, r_n$  be the distinct incongruent solutions to  $f(x) \equiv 0 \pmod{p}$ . Looking at the first solution, we find

$$f(x) = f(r_1) + (x - r_1)g(x) \equiv (x - r_1)g(x) \pmod{p}.$$

If we evaluate this formula at any of the other solutions  $x = r_k$ , we obtain

$$0 \equiv f(r_k) \equiv (r_k - r_1)g(r_k) \pmod{p}.$$

We have assumed that  $r_1 \not\equiv r_k \pmod{p}$ , so the prime divisibility property (Theorem 7.2) tells us that  $g(r_k) \equiv 0 \pmod{p}$ . [Note that this is where we use the assumption that the modulus  $p$  is prime. Do you see why the argument would fall apart if the modulus were composite?]

We now know that  $r_2, r_3, \dots, r_n$  are solutions to  $g(x) \equiv 0 \pmod{p}$ . Applying the exact same argument to  $g(x)$  and its root  $r_2$ , we find that

$$g(x) = g(r_2) + (x - r_2)h(x) \equiv (x - r_2)h(x) \pmod{p}$$

for some polynomial  $h(x)$  of degree  $d - 2$ . Evaluating at  $x = r_k$  for any  $k \geq 3$  yields

$$0 \equiv g(r_k) \equiv (r_k - r_2)h(r_k) \pmod{p},$$

and using the fact that  $r_k \not\equiv r_2 \pmod{p}$ , we see that  $r_3, r_4, \dots, r_n$  are solutions to  $h(x) \equiv 0 \pmod{p}$ . We have thus factored  $f(x)$  as

$$f(x) \equiv (x - r_1)g(x) \equiv (x - r_1)(x - r_2)h(x) \pmod{p}.$$

Repeating this argument  $n$  times, we eventually find that

$$f(x) \equiv (x - r_1)(x - r_2) \cdots (x - r_n)u(x) \pmod{p}$$

for some polynomial  $u(x)$ . The polynomial  $f(x)$  has degree  $d$ , while the product  $(x - r_1) \cdots (x - r_n)u(x)$  has degree at least  $n$ . Hence

$$(\text{degree of } f(x)) = d \geq n = (\text{number of roots of } f(x) \equiv 0 \pmod{p}).$$

This completes the proof that a degree  $d$  polynomial has at most  $d$  incongruent roots modulo a prime  $p$ . Although this statement may seem innocuous, it provides a crucial tool in the proofs of many important results.

## Exercises

**8.8.** (a) How many solutions are there to the congruence

$$X^4 + 5X^3 + 4X^2 - 6X - 4 \equiv 0 \pmod{11} \quad \text{with } 0 \leq X < 11?$$

Are there four solutions, or are there fewer than four solutions?

(b) Consider the congruence  $X^2 - 1 \equiv 0 \pmod{8}$ . How many solutions does it have with  $0 \leq X < 8$ ? Notice that there are more than two solutions. Why doesn't this contradict the Polynomial Roots Mod  $p$  Theorem (Theorem 8.2).

**8.9.** Let  $p$  and  $q$  be distinct primes. What is the maximum number of possible solutions to a congruence of the form

$$x^2 - a \equiv 0 \pmod{pq},$$

where as usual we are only interested in solutions that are distinct modulo  $pq$ ?