11. Polynomial congruences

We now want to look at the problem of solving polynomial equations modulo a natural number m. First note that the natural homomorphism

$$\mathbb{Z} \longrightarrow \mathbb{Z}_m \qquad \text{which sends} \qquad a \longrightarrow \bar{a}$$

extends naturally to a homomorphism

$$\mathbb{Z}[x] \longrightarrow \mathbb{Z}_m[x] \qquad \text{which sends} \qquad f(x) \longrightarrow \bar{f}(x).$$

If

$$f(x) = a_0 + a_1 x + \dots + a_n x^n \qquad \text{then} \qquad \bar{f}(x) = \bar{a}_0 + \bar{a}_1 x + \bar{a}_2 x^2 + \dots + \bar{a}_n x^n.$$

Note also that it makes sense to evaluate $\bar{f}(x)$ as $\bar{a} \in \mathbb{Z}_m$. In particular it makes sense to look for zeroes of polynomials in $\mathbb{Z}_m$.

Note that if p is a prime then $\mathbb{Z}_p$ is a field so that $\mathbb{Z}_p[x]$ is a UFD; every polynomial factors into prime polynomials, uniquely up to order and units. On the other hand, if m is composite then $\mathbb{Z}_m$ is not even an integral domain.

Proposition 11.1. *Let $f(x) \in \mathbb{Z}[x]$ and let p be a prime.*

If a is a root of the congruence $f(x) \equiv 0 \mod p$ then $x - \bar{a}$ divides $\bar{f}(x)$ in the ring $\mathbb{Z}_p[x]$.

Proof. Since $\mathbb{Z}_p$ is a field, the ring $\mathbb{Z}_p[x]$ is a Euclidean domain. Therefore we can divide $(x - \bar{a})$ into $\bar{f}(x)$ to get a quotient and a remainder,

$$\bar{f}(x) = q(x)(x - \bar{a}) + r(x),$$

where $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $x - \bar{a}$. As the degree of $x - \bar{a}$ is one, it follows that $r(x) = r$ is a constant. If we plug in a then we get

$$\begin{aligned} 0 &= \bar{f}(\bar{a}) \\ &= q(\bar{a})(\bar{a} - \bar{a}) + r \\ &= r. \end{aligned}$$

Thus $r(x) = 0$ and so $x - \bar{a}$ divides $\bar{f}(x)$. □

Theorem 11.2 (Lagrange's Theorem)**.** *If p is a prime and $f(x) \in \mathbb{Z}[x]$ has degree n then the equation $f(x) \equiv 0 \mod p$ has at most n roots.*

Proof. If $\bar{a}$ is a root of $\bar{f}(x) = 0$ then $(x - a)$ is a linear factor of $\bar{f}(x)$. As $\mathbb{Z}_p[x]$ is a UFD, $\bar{f}(x)$ can have at most n different linear factors. □

Note that this fails in general if m is composite. For example,

$$(x-2)(x-3) = x^2 - 5x = x(x-5) \mod 6,$$

so that 0, 2, 3 and 5 are all roots of the polynomial $x^2 - 5x$, modulo 6.

Theorem 11.3. *Let p be a prime and let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree n.*

The number of distinct roots of $f(x)$ is the degree of the polynomial $(f(x), x^p - x)$. In particular $f(x)$ has exactly n roots if and only if $f(x)$ divides $x^p - x$.

Proof. Fermat's theorem implies that if $a \in \mathbb{Z}_p$ then

$$a^p = a \in \mathbb{Z}_p.$$

Thus a is a root of $x^p - x \in \mathbb{Z}_p[x]$. It follows that x, $x-1$, $x-2$, ..., $x+1-p$ are all linear factors of $x^p - x$. As the product

$$x(x-1)(x-2)\dots(x-p+1)$$

has degree p and it is monic, it follows that

$$x^p - x = x(x-1)(x-2)\dots(x-p+1) \in \mathbb{Z}_p[x].$$

Suppose that r is a root of $f(x)$. Then we can write

$$f(x) = (x-r)^e g(x),$$

for some natural number e, which we will call the multiplicity. So if $f(x)$ has roots $r_1, r_2, \dots, r_k$ with multiplicities $e_1, e_2, \dots, e_k$ then we may write

$$f(x) = (x-r_1)^{e_1}(x-r_2)^{e_2}\dots(x-r_k)^{e_k} g(x),$$

where $g(x) \in \mathbb{Z}_p[x]$ has no roots. It follows that

$$(f(x), x^p - x) = (x-r_1)(x-r_2)\dots(x-r_k).$$

Clearly this is a polynomial of degree k, the number of roots of $f(x)$.

If $f(x)$ has n distinct roots, then $r_1 = r_2 = \dots = r_k$ and $k = n$ so that $f(x)$ divides $x^p - x$. $\square$

Corollary 11.4. *Let d be a natural number and let p be a prime.*

If d divides $p-1$ then the congruence $x^d \equiv 1 \mod p$ has d solutions.

Proof. Note that

$$y^k - 1 = (y-1)(y^{k-1} + y^{k-2} + \dots + 1).$$

By assumption there is an integer k such that $p - 1 = dk$. Therefore

$$\begin{aligned} x^p - x &= x(x^{p-1} - 1) \\ &= x(x^{dk} - 1) \\ &= x((x^d)^k - 1) \\ &= x(x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \dots + x^d + 1). \end{aligned}$$

Thus $x^d - 1$ divides $x^p - x$ so that $x^d - 1$ has d distinct roots by (11.3). $\square$

Theorem 11.5 (Wilson's Theorem). *If p is a prime number then*

$$(p-1)! \equiv -1 \mod p.$$

Proof. If $p = 2$ then the result is clear. Otherwise p is odd. We have already seen that

$$x^p - x = x(x-1)(x-2)\dots(x-(p+1)) \mod p.$$

Cancelling a factor of x from both sides, we get

$$x^{p-1} - 1 = (x-1)(x-2)\dots(x-(p+1)) \mod p.$$

The constant term on the LHS is -1 and the constant term on the RHS is

$$(p-1)!.$$

□