Hensel引理、原根

李 辉

Table of Contents

Hensel引理

Hensel's Lemma Suppose that $f(x) \in Z(x)$,

$$f(a) \equiv 0 \, mod \, p^k,$$

and $f'(a) \neq 0 \, mod \, p$.

Then there is a unique t mod p such that

$$f(a + tp^k) \equiv 0 \, mod \, p^{k+1}.$$

That is, there is a unique solution $b \, mod \, p^{k+1}$ which is congruent to $a \, mod \, p^k$.

Proof.

We are looking for the solutions $b = a + tp^k$ where $t \in \{0,1,\cdots,p-1\}$ to the congruence mod p^{k+1}.

Use Taylor expansion around a:

$$f(a + tp^k)$$

$$= f(a) + f'(a)tp^k + \frac{f''(a)}{2!}[tp^k]^2 + \cdots + \frac{f^{(n)}(a)}{n!}[tp^k]^n$$

If f is a polynomial with integer coefficients, $\frac{f^{(n)}(a)}{n!} \, mod \, p^{k+1}$ is an integer.
So,

$$f(a + tp^k) \equiv f(a) + f'(a)tp^k \, mod \, p^{k+1} \qquad if \; j \geq 1$$

Let both sides to $\equiv 0 \, mod \, p^{k+1}$.

$$f(a) + tp^k f'(a) \equiv 0 \; mod \, p^{k+1}$$
$$tf'(a) + \frac{f(a)}{p^k} \equiv 0 \, mod \, p$$
$$t \equiv -(\frac{f(a)}{p^k}\frac{1}{f'(a)}) \, mod \, p$$

Example

Use Hensel's Lemma to find a solution to $x^3 - 2x \equiv 1(mod\ 125)$.

Let $f(x) = x^3 - 2x - 1$.

Find a solution to $f(x) \equiv 0(mod 5)$.

$$f(0) = -1 \equiv 4(mod\ 5)$$
$$f(1) = -2 \equiv 3(mod\ 5)$$
$$f(2) = 3 \equiv 3(mod\ 5)$$
$$f(3) = 20 \equiv 0(mod\ 5)$$
$$f(4) = 55 \equiv 0(mod\ 5)$$

So, $a_1 = 3,4$ are all solutions to $f(x) \equiv 0(mod 5)$.

We compute the derivative of f: $f'(x) = 3x^2 - 2$.

$$f'(3) = 27 - 2 = 25 \equiv 0(mod 5)$$
$$f'(4) = 48 - 2 = 46 \equiv 1(mod 5)$$

We cannot apply Hensel's

$$(f'(4))^{-1} \equiv 1(mod5).$$

So

$$\begin{aligned} a_2 &\equiv 4 - f(4)[f'(4)]^{-1}(mod25) \\ &\equiv 4 - 55 \times 1(mod25) \\ &\equiv -51(mod25) \\ &\equiv 24(mod25) \end{aligned}$$

$$\begin{aligned} a_3 &\equiv 24 - f(24)[f'(24)]^{-1}(mod125) \\ &\equiv 24 - 13775 \times 1(mod125) \\ &\equiv -13751(mod125) \\ &\equiv -1(mod125) \\ &\equiv 124(mod125) \end{aligned}$$

So, $x = 124$ is a solution to

$$x^3 - 2x \equiv 1(mod125).$$

Excise007

Solve the equation:

$$x^3 - x \equiv 139(mod\ 343)$$

模多项式

Theorem A congruence $f(x) \equiv 0$ mod p (p is a prime) of degree n has at most n solutions.

Example

- $3x - 2 \equiv 0\ mod\ 7$
- $x^2 \equiv 2\ mod\ 7$
- $x^3 \equiv 1\ mod\ 7$
- $x^2 \equiv 1\ mod\ 15$

Proof.

The statements hold for degree 0 or 1.

Assume it holds for degree $< n$ ($n \geq 2$).

If it has no root, then done.

Otherwise, suppose it have a root α.

Dividing $f(x)$ by $x - \alpha$, we obtain $g(x) \in Z[x]$ and a constant r such that

$$f(x) = g(x)(x - \alpha) + r.$$

Now if we plug in α we obtain

$$f(\alpha) = (\alpha - \alpha)g(\alpha) + r = r,$$

which means that $f(\alpha) = r$ and

$$f(x) = (x - \alpha)g(\alpha) + f(\alpha).$$

We know that $f(\alpha)\ mod\ p = 0$. If β is any other root of $f(x)$ then we plug β into the equation to obtain

$$f(\beta) = (\beta - \alpha)g(\beta) + f(\alpha)\ mod\ p,$$
$$f(\beta) \equiv (\beta - \alpha)g(\beta)\ mod\ p,$$

so

$$(\beta - \alpha)g(\beta) \equiv 0 \, mod \, p.$$

We also assume that $\beta \neq \alpha$, so

$$g(\beta) \equiv 0 \, mod \, p.$$

So, β is a root of $g(x)$ as a solution of

$$g(x) \equiv 0 \, mod \, p.$$

We know that $g(x)$ has degree $n - 1$, so by induction hypothesis

$$g(x) \equiv 0 \, mod \, p$$

has at most $n - 1$ solutions, which by including α gives $f(x)$ at most n solutions.

Corollary. If

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \equiv 0 \, mod \, p$$

has more than n solutions, then all

$$a_i \equiv 0 \, mod \, p.$$

Theorem Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

$f(x) \equiv 0 \bmod p$ has exactly n distinct solutions if and only if $f(x)$ divides

$$x^p - x \, mod \, p.$$

Namely, there exists $g(x) \in Z[x]$ such that

$$f(x)g(x) = x^p - x \, mod \, p$$

as polynomials.

Proof.

Part 1.

Suppose $f(x)$ has n solutions. Then $n \leq p$ because only p possible roots mod p.

Divide $x^p - x$ by $f(x)$ to obtain

$$x^p - x = f(x)g(x) + r(x),$$
$$deg(r) < deg(f) = n.$$

Now, if α is a root of $f(x)$ mod p then plug in to obtain

$$\alpha^p - \alpha = f(\alpha)g(\alpha) + r(\alpha) \equiv 0$$

So, α must be a solution to

$$r(x) \equiv 0 \, mod \, p.$$

Since $f(x)$ has distinct roots,

$$r(x) \equiv 0 \, mod \, p$$

has n distinct solutions. But $deg(r) < n$.

So,

$$x^p - x = f(x)g(x) \, mod \, p,$$

and $f(x)$ divides $x^p - x$.

Part2.

Suppose

$$f(x) | x^p - x \, mod \, p.$$

Write

$$x^p - x \equiv f(x)g(x) \, mod \, p,$$

where $f(x)$ is a monic of degree n and $g(x)$ is a monic of degree $p - n$. We shall show that $f(x)$ has n distinct solutions.

By previous theorem, $g(x)$ has at most $p - n$ roots mod p.

If $\alpha \in \{0,1,\cdots,p-1\}$ is not a root of $g(x)$ mod p then
$\alpha^p - \alpha \equiv f(\alpha)g(\alpha)\, mod\, p \equiv 0(Fermat)$.

Since $g(\alpha) \neq 0$ mod p,
$f(\alpha) \equiv 0\, mod\, p$.

So, since there are at least $p - (p - n)$ such α, we see that $f(x)$ has at least n distinct roots mod p.

By the theorem, $f(x)$ has at most n roots mod $p \Rightarrow f(x)$ has exactly n distinct roots mod p. ■

Corollary If $d|p-1$ then

$$x^d \equiv 1 \, mod \, p$$

has exactly d distinct solutions mod p.

Example

$$x^3 \equiv 1 \, mod \, 7$$
$$x^3 \equiv 1 \, mod \, 5$$

Proof.

$d|p-1$, so $x^d - 1 | x^{p-1} - 1$ as polynomials.

$p - 1 = kd$, so

$$x^{kd} - 1 = (x^d - 1)(x^{(k-1)d} + \cdots + 1).$$

So,

$$x^d - 1 | x(x^{p-1} - 1) = x^p - x.$$

So has d solutions.

Another proof of **Wilson's Theorem**.

Suppose p is an odd prime.

Let

$$f(x) = x(x-1)\cdots(x-p+1).$$

This has deg p and p solutions mod p, so it must divide $x^p - x$ mod p.

Both polynomials are monic of the same degree (p), so must be equal mod p.

$$x(x-1)\cdots(x-p+1) \equiv x^p - x \, mod \, p$$

Coefficient of x on the left side is just

$$(-1)(-2)\cdots(-(p-1))$$
$$= (-1)^{p-1}(p-1)! = (p-1)!$$

since p is odd.

So

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

元素的阶

Question:

We know

$$gcd(22,35) = 1,$$

so

$$22^{\phi(35)} = 22^{24} \equiv 1 \, mod \, 35.$$

Is there a smallest positive integer N such that

$$22^N \equiv 1 mod 35?$$

Definition **Order**

If $gcd(a, m) = 1$ and h is the smallest positive integer such that $a^h \equiv 1$ mod m then say h is the **order** of a mod m.
Notation: $h = ord_m(a)$.

Example

$$ord_7(2) = 3$$
$$ord_{11}(2) = 10$$
$$ord_{11}(5) = 5$$

Lemma. Let $h = ord_m(a)$. The set of integers k such that $a^k \equiv 1 \bmod m$ is exactly the set of multiples of h.

Example

$$ord_{11}(5) = 5$$

If $5^k \equiv 1 \, mod \, 11$, then

$$k = 5,10.$$

Proof. $a^{rh} \equiv (a^h)^r \equiv 1^r \equiv 1 \bmod m$.

Suppose we have k such that

$$a^k \equiv 1 \, mod \, m.$$

We shall show $h|k$.

Let $k = hq + r$ where $0 \leq r < h$.

$$1 \equiv a^k = a^{hq+} = a^{hq} a^r \equiv 1a^r$$
$$\equiv a^r \, mod \, m,$$

so

$$a^r \equiv 1 \, mod \, m.$$

But $r < h$, so $r = 0$, and k is multiple of h.

Lemma. If $h = ord_m(a)$ then a^k has order $\frac{h}{gcd(k,h)}$ mod m.

Example

$$ord_{11}(5) = 5$$
$$ord_{11}(2) = 10$$

- $5^3 \equiv 4$ has order $\frac{5}{gcd(3,5)} = 5\, mod\ 11$.
- $2^8 \equiv 3$ has order $\frac{10}{gcd(8,10)} = 5\, mod\ 11$.

Proof.

$$a^{kj} \equiv 1\, mod\, m \Leftrightarrow h|kj$$
$$\Leftrightarrow \frac{h}{gcd(h,k)} | \frac{k}{gcd(h,k)} j \Leftrightarrow \frac{h}{gcd(h,k)} | j$$

So, the smallest positive $j = \frac{h}{gcd(h,k)}$.

Lemma. If a has order h mod m and b has order k mod m, and $gcd(h,k) = 1$, then ab has order hk mod m.

Example

$$ord_{11}(4) = 5$$
$$ord_{11}(10) = 2$$
$$\Rightarrow ord_{11}(4 \times 10 \equiv 7) = 10$$

Proof.

$$(ab)^{hk} \equiv (a^h)^k (b^k)^h \equiv 1^k 1^h \equiv 1 \, mod \, m$$

Conversely, suppose that $r = ord_m(ab)$.

$$(ab)^r \equiv 1 \, mod \, m$$
$$(ab)^{rh} \equiv 1 \, mod \, m$$
$$(a^h)^r b^{rh} \equiv 1 \, mod \, m$$
$$b^{rh} \equiv 1 \, mod \, m$$

So, $k|rh \Rightarrow k|r$ (because $gcd(k, h) = 1$), and similarly $h|r$. So, $hk|r$, and so $hk = ord_m(ab)$.

原根

Definition **Primitive Root**

If a has order $\phi(m)$ mod m, we say that a is a **primitive root** mod m.

Example

3 is the primitive root of mod 7.

2,7 are the primitive roots of mod 11.

Lemma. Let p be prime and suppose $q^e | p-1$ for some other prime q. Then there's an element mod p of order q^e.

Let

$$p - 1 = q_1^{e_1} q_2^{e_2} \cdot q_r^{e_r}.$$

The lemma means that $\exists g_1$ with $ord_p(g_1) = q_1^{e_1}$, g_2 with $ord_p(g_2) = q_2^{e_2}$, etc.

Example

$$p = 101,\ q = 5,\ e = 2$$
$$Ord_{101}31 = 25$$

Set $g = g_1 g_2 \cdots g_r$.

By the previous lemma, g has order

$$q_1^{e_1} q_2^{e_2} \cdot q_r^{e_r} = p - 1 = \phi(p).$$

because all q_i are coprime in pairs.

So, g is a primitive root mod p.

Proof.

Consider solution of $x^{q^e} \equiv 1 \bmod p$.

Because $q^e | p-1$, $x^{q^e} - 1$ has exactly q^e roots mod p

If α is any such root, then $ord_p(\alpha)$ must divide q^e.

So, if it is not equal to q^e, it must divide q^{e-1}.

Then α would have to be root of $x^{q^{e-1}} - 1 \equiv 0 \bmod p$, which has exactly q^{e-1} solutions.

Since $q^e - q^{e-1} > 0$, there exists α such that $ord_p(\alpha) = q^e$.

Number of primitive roots

The number of primitive roots mod m is $\phi(\phi(m))$, if there is at least one.

Particularly, if m is a prime, then number of primitive roots is $\phi(m-1)$.

Example

$$\phi(\phi(31)) = 8$$

Indeed, $\{3,11,12,13,17,21,22,24\}$ are the primitive roots of 31.

Proof. Suppose there is a primitive root g mod m.

If we look at the integers $1, g, \cdots, g^{\phi(m)-1}$, they are all coprime to m and **distinct** mod m.

If we had $g^i \equiv g^j \bmod m$ $(0 \leq i < j \leq \phi(m)-1)$,then we have $g^{j-i} \equiv 1 \bmod m$, contradicting the fact that g is a primitive root.

Since there are $\phi(m)$ of these integers, They are the reduced residue classes.

Suppose a is a primitive root mod m, then $a \equiv g^k \bmod m$

$$\frac{ord(g)}{gcd(k, ord(g))} = \frac{\phi(m)}{gcd(k, \phi(m))}$$

So the only way for the order to be exactly $\phi(m)$ is for k to be coprime to $\phi(m)$.

The number of numbers which are coprime to $\phi(m)$ is $\phi(\phi(m))$.

Excise008

Try to find a primitive root of mod 211.

Theorem*** There is a primitive root mod m if and only of $m = 1,2,4, p^e, or\ 2p^e$.

The proof*** is **NOT** provided here.

Other relative concepts

- Discrete Log

Example

$$2^x \equiv 5\ mod\ 11$$
$$x = log_2 5\ mod\ 11$$

It is a NPC-hard problem.