**Bharathidasan University**
Tiruchirappalli - 620 024
Tamil Nadu, India

**Programme: M.Sc., Mathematics**

Course Title :Theory of Numbers
COurse Code : 21M04CC

# Hensel's Lemma

**Dr. V. Piramanantham**
Professor
Department of Mathematics

congruence (modulo prime power)

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$,
where $a_0, a_1, \ldots, a_n$ are integers.

Discuss the problem of finding solution of

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

where $p$ is prime and $\alpha \geq 0$.

If we know the solutions of $f(x) \equiv 0 \pmod{p^\alpha}$ then we can find solutions of $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ from them

If $f(a) \equiv 0 \pmod{p^\alpha}$ find $t$ such that

$$f(a + tp^\alpha) \equiv 0 \pmod{p^{\alpha+1}}$$

A solution $a \pmod{p^\alpha}$ of $f(x) \equiv 0 \pmod{p^\alpha}$ is called nonsingular if

$$f'(a) \not\equiv 0 \pmod{p};$$

otherwise it is singular.

**Definition:** If $f(a) \equiv 0 \pmod{p^\alpha}$, $f(b) \equiv 0 \pmod{p^\beta}$, $\alpha < \beta$ and $a \equiv b \pmod{p^\alpha}$, then we say that b lies above a or a lifts to b

**Objective:** If $f(a) \equiv 0 \pmod{p^\alpha}$ then a lifts to a solution of

$$f(x) \equiv 0 \pmod{p^{\alpha+1}}.$$

Hensel's Lemma:

If $a$ is a nonsingular solution $f(x) \equiv 0 \pmod{p^\alpha}$, then $a$ lifts to a unique solution in the form $a + t p^\alpha$ of $f(x) \equiv 0 \pmod{p^{\alpha+1}}$.

(or)

If $f(a) \equiv 0 \pmod{p^\alpha}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there is a unique $t \pmod{p}$ such that $f(a + t p^\alpha) \equiv 0 \pmod{p^{\alpha+1}}$

Proof By use of Taylor's expansion for any $t$,

$$f(a+tp^{\alpha}) = f(a) + tp^{\alpha} f'(a) + \frac{t^2 p^{2\alpha}}{2!} f''(a) + \cdots + \frac{t^n p^{n\alpha}}{n!} f^{(n)}(a). \quad \text{--- (1)}$$

where $n$ is the degree of $f$. $f^{(k)}(a) = 0 \ \forall k > n$.

Now w.r.t the modulus $p^{\alpha+1}$, (1) yields

$$f(a+tp^{\alpha}) \equiv f(a) + tp^{\alpha} f'(a) \pmod{p^{\alpha+1}} \quad \text{--- (2)}$$

For this,

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

$1 \leq k \leq n$

$$f^{(k)}(x) = \sum_{i=k}^{n} a_i\, i(i-1)\cdots(i-k+1)\, x^{i-k}.$$

Except the first two terms, we consider each term, $2 \leq k \leq n$

$$\frac{t^k p^{k\alpha}}{k!} f^{(k)}(a)$$

$$= t^{k} p^{(k-1)\alpha - 1} \frac{f^{(k)}(a)}{k!} p^{\alpha+1}$$

$$= t^{k} p^{(k-1)\alpha - 1} \sum_{i=k}^{n} a_i \frac{i(i-1)\cdots(i-k+1)}{k!} x^{i-k} p^{\alpha+1}$$

since ${}^{i}C_k$ is int

$$\frac{t^{k} p^{k\alpha} f^{(k)}(a)}{k!} \text{ is an integer}$$

for $2 \le k \le n$.

$$\therefore \frac{t^{k} p^{k\alpha} f^{(k)}(a)}{k!} \equiv 0 \pmod{p^{\alpha+1}}$$

② is true.

$$f(a+tp^{\alpha}) \equiv f(a) + tp^{\alpha} f'(a) \pmod{p^{\alpha+1}}$$

we look for an integer $t$ such that

$$③ \quad — \quad f(a+tp^{\alpha}) \equiv 0 \pmod{p^{\alpha+1}}$$

Since $f(a) \equiv 0 \pmod{p^{\alpha}}$

$f(a)$ is divisible by $p^{\alpha}$.

From ② and ③,

$$f(a) + t p^{\alpha} f'(a) \equiv 0 \pmod{p^{\alpha+1}}$$

$$\Rightarrow \quad t f'(a) \equiv -\frac{f(a)}{p^{\alpha}} \pmod{p} \quad \text{— ④}$$

we have a linear congruence in $t$

③ & ④ are equivalent

given $f'(a) \not\equiv 0 \pmod{p}$

since $(f'(a), p) = 1$,

(4) has only one solution $t \pmod p$.

$\therefore \quad f(a + tp^{\alpha}) \equiv 0 \pmod{p^{\alpha+1}}$

for only one $t \pmod p$.

Hence the theorem.

Note The solution $t \pmod p$ of (3)

$$t = -\frac{\overline{f'(a)}\, f(a)}{p^{\alpha}}.$$

Note ②

If $f(a) \equiv 0 \pmod{p^\alpha}$ &

$f'(a) \not\equiv 0 \pmod{p}$,

then

$$\boxed{b = a - \overline{f'(a)}\, f(a)}$$

is a solution of $f(x) \equiv 0 \pmod{p^{\alpha+1}}$

$$b \overset{?}{\equiv} a \pmod{p^\alpha} \qquad \text{Yes}$$

Known $\quad f(x) \equiv 0 \pmod{p}$ — $a$

$$f'(a) \not\equiv 0 \pmod{p} \qquad a_0 = a$$

$$f(x) \equiv 0 \pmod{p^2} \qquad \text{has soln}$$

$$a_1 = a - \overline{f'(a)}\, f(a)$$

$$a_1 \equiv a \pmod{p}$$

$$f'(a_1) \equiv f'(a) \pmod{p}$$
$$\not\equiv 0 \pmod{p}$$

$$\overline{f'(a_1)} = \overline{f'(a)}$$

$$a_2 = a_1 - \overline{f'(a)}\, f(a_1)$$

is a soln of $f(x) \equiv 0 \pmod{p^2}$

$f'(a_2) \not\equiv 0 \pmod{p}$ $\quad \overline{f'(a_2)} = \overline{f'(a)}$

$$a_3 = a_2 - \overline{f'(a)}\, f(a_2)$$

$$f(x) \equiv 0 \pmod{p^3}$$

If $a$ is a nonsingular solution of $f(x) \equiv 0 \pmod{p}$, then for any $k \geq 0$

$$a_{k+1} = a_k - \overline{f'(a)}\, f(a_k)$$

is a solution of $f(x) \equiv 0 \pmod{p^{k+1}}$

where $a_0 = a$ & $\overline{f'(a)}$ is a multiplicative inverse (modulo $p$).

Hensel's lemma

$f(a) \equiv 0 \pmod{p^\alpha}$, $f'(a) \not\equiv 0 \pmod{p^\alpha}$

for only one $t$ from $1, 2, \ldots, p$

$$f(a + tp^\alpha) \equiv 0 \pmod{p^\alpha}$$

for other $s \not\equiv t$, $f(a+sp^{\alpha}) \not\equiv 0 \pmod{p^{\alpha}}$

If $a$ is singular solution of

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

then

$$f'(a) \equiv 0 \pmod{p}$$

$f(a) \equiv 0 \pmod{p^{\alpha}}$.

from proof of Hensel's lemma

$$② \Rightarrow \quad f(a+tp^{\alpha}) \equiv f(a) + tp^{\alpha} f'(a) \pmod{p^{\alpha+1}}$$

$$\Rightarrow \boxed{f(a+tp^{\alpha}) \equiv f(a) \pmod{p^{\alpha+1}}}$$

for any $t$.

If $\underline{f(a) \equiv 0 \pmod{p^{\alpha+1}}}$,

$$f(a+tp^{\alpha}) \equiv 0 \pmod{p^{\alpha+1}},$$

otherwise,

$$f(a+tp^{\alpha}) \not\equiv 0 \pmod{p^{\alpha+1}}$$

$$f(a) \equiv 0 \pmod{p^\alpha}$$

Nonsingular

$f'(a) \not\equiv 0 \pmod{p}$

Hensel lemma

$$f(a+tp^\alpha) \equiv 0 \pmod{p^{\alpha+1}}$$

for unique $t$

$$t = -\overline{f'(a)}\,\frac{f(a)}{p^\alpha}$$

singular

$f'(a) \equiv 0 \pmod{p}$

$f(a) \equiv 0 \pmod{p^{\alpha+1}}$

$$f(a+tp^\alpha) \equiv 0 \pmod{p^{\alpha+1}}$$

$f(a) \not\equiv 0 \pmod{p^{\alpha+1}}$

$$f(a+tp^\alpha) \not\equiv 0 \pmod{p}$$