Lecture Notes for International Mathematical Olympiad

PRIME POWER CONGRUENCE AND HENSEL'S LEMMA

1. Congruence lifting and Hensel's lemma

We begin with an introductory example. Note that for $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ a product of distinct prime powers, by Chinese remainder theorem, $f(x) \equiv 0 \bmod m$ has an integer solution x if and only if $f(x) \equiv 0 \bmod p_i^{\alpha_i}$ for each $i = 1, \ldots, k$.

Also, suppose $\alpha \in \mathbb{N}^*$ and $f(x) \equiv 0 \bmod p^\alpha$ has some integer solution with p prime, then so also does $f(x) \equiv 0 \bmod p$. Unluckily, the converse of this is not valid. For a counter example, $x = 2$ is a solution to $x^{10} - 1 \equiv 0 \bmod 11$ but can never be a solution to $x^{10} - 1 \equiv 0 \bmod 11^2$.

This phenomenon indicates us to ask for a condition to guarantee that the existence of solution to $f(x) \equiv 0 \bmod p$ implies that of $f(x) \equiv 0 \bmod p^\alpha$. This process is usually called "congruence lifting". To be precise, we are going to begin with a given solution to $f(x) \equiv 0 \bmod p$, and to construct a solution to $f(x) \equiv 0 \bmod p^\alpha$ inductively.

Theorem 1 (Existence of congruence lifting)**.** *Let p be a prime number and $a_i \in \mathbb{Z}$ for $i = 0, 1, \ldots, n$. Consider the following equation with $\alpha \in \mathbb{Z}_{\geqslant 1}$,*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \bmod p^\alpha, \quad p^\alpha \nmid a_n. \tag{1}$$

Assume that

$$f(x) \equiv 0 \bmod p, \quad p \nmid a_n. \tag{2}$$

Suppose also that $x \equiv x_0 \bmod p$ is a solution of (2), i.e.

$$x = x_0 + pt_1, \quad t_1 \in \mathbb{Z} \tag{3}$$

satisfies (2), and $p \nmid f'(x_0)$, where $f'(x)$ is the formal derivative of $f(x)$.

Then there exists a unique solution of (1) generated by (3), say $x \equiv x_\alpha \bmod p^\alpha$, i.e. $x = x_\alpha + p^\alpha t_\alpha$ for some $t_\alpha \in \mathbb{Z}$, such that $x_\alpha \equiv x_0 \bmod p$.

Proof. We apply the induction on α. The case where $\alpha = 1$ is trivial. Suppose $\alpha \geqslant 2$ and the result is valid for $p^{\alpha-1}$, i.e. $f(x) \equiv 0 \bmod p^{\alpha-1}$ admits a solution $x = x_{\alpha-1} + p^{\alpha-1} t_{\alpha-1}$ say, with $t_{\alpha-1} \in \mathbb{Z}$ and $x_{\alpha-1} \equiv x_0 \bmod p$. Then for each $k = 0, \ldots, n$,

$$a_k (x_{\alpha-1} + p^{\alpha-1} t_{\alpha-1})^k = a_k \left(x_{\alpha-1}^k + k x_{\alpha-1}^{k-1} p^{\alpha-1} t_{\alpha-1} + \frac{k(k-1)}{2} x_{\alpha-1}^{k-2} p^{2\alpha-2} t_{\alpha-1}^2 + \cdots \right).$$

Since $\alpha \geqslant 2$ we have $2\alpha - 2 \geqslant \alpha$, and hence $p^\alpha \mid p^{2\alpha-2}$. Consequently,

$$a_k (x_{\alpha-1} + p^{\alpha-1} t_{\alpha-1})^k \equiv a_k x_{\alpha-1}^k + k a_k x_{\alpha-1}^{k-1} p^{\alpha-1} t_{\alpha-1} \bmod p^\alpha.$$

So, by summing up these,

$$\begin{aligned} f(x_{\alpha-1} + p^{\alpha-1} t_{\alpha-1}) &\equiv \sum_{k=0}^{n} a_k x_{\alpha-1}^k + \sum_{k=0}^{n} (k a_k x_{\alpha-1}^{k-1}) p^{\alpha-1} t_{\alpha-1} \\ &\equiv f(x_{\alpha-1}) + f'(x_{\alpha-1}) p^{\alpha-1} t_{\alpha-1} \equiv 0 \bmod p^\alpha. \end{aligned}$$

Date: August 19, 2022.

By assumption, $x_{\alpha-1}$ is a solution to $f(x) \equiv 0 \bmod p^{\alpha-1}$, and hence $p^{\alpha-1} \mid f(x_{\alpha-1})$. Note that the above equation is divisible by $p^{\alpha-1}$, so we obtain

$$\frac{f(x_{\alpha-1})}{p^{\alpha-1}} + f'(x_{\alpha-1})t_{\alpha-1} \equiv 0 \bmod p.$$

On the other hand, as $x_{\alpha-1} \equiv x_0 \bmod p$, we see $f'(x_{\alpha-1}) \equiv f'(x_0) \bmod p$. For this, the equation above turns out to be

$$\frac{f(x_{\alpha-1})}{p^{\alpha-1}} + f'(x_0)t_{\alpha-1} \equiv 0 \bmod p,$$

which is a congruence equation of degree 1 with respect to $t_{\alpha-1}$. Now we apply the technical condition $p \nmid f'(x_0)$ to see $(p, f'(x_0)) = 1$, which indicates that the above equation admits a unique solution (up to modulo p), say

$$t_{\alpha-1} = pt_\alpha + t'_{\alpha-1}, \quad 0 \leqslant t'_{\alpha-1} \leqslant p-1.$$

Plugging this back to $x = x_{\alpha-1} + p^{\alpha-1}t_{\alpha-1}$, we get

$$\begin{aligned} x &= x_{\alpha-1} + p^{\alpha-1}(pt_\alpha + t'_{\alpha-1}) \\ &= x_{\alpha-1} + p^{\alpha-1}t'_{\alpha-1} + p^\alpha t_\alpha \\ &= x_\alpha + p^\alpha t_\alpha \end{aligned}$$

for $t_\alpha \in \mathbb{Z}$, in which

$$x_\alpha = x_{\alpha-1} + p^{\alpha-1}t'_{\alpha-1} \equiv x_{\alpha-1} \equiv x_0 \bmod p.$$

This completes the proof of existence, and the uniqueness is obvious modulo p^α. □

By applying Theorem 1 inductively for $\alpha = 2, 3, \ldots$ respectively, we get the following result.

Corollary 2 (The first lemma of Hensel)**.** *If $x_0 \in \mathbb{Z}$ is a solution to $f(x_0) \equiv 0 \bmod p$ with $p \nmid f'(x_0)$, then there is a unique integer sequence $t_1, t_2, \ldots$ with $0 \leqslant t_i \leqslant p-1$, such that for any integer $\alpha > 1$, the equation*

$$f(x) \equiv 0 \bmod p^\alpha, \quad x \equiv x_0 \bmod p$$

admits a unique solution generated by x_0 up to modulo p^α; that is,

$$x \equiv x_0 + pt_1 + p^2t_2 + \cdots + p^{\alpha-1}t_{\alpha-1}.$$

Remark 3. We are to consider the solution to

$$\frac{f(x_{\alpha-1})}{p^{\alpha-1}} + f'(x_{\alpha-1})t_{\alpha-1} \equiv 0 \bmod p.$$

If $p \nmid f'(x_{\alpha-1})$, then, by Corollary 2, there is a unique $t_{\alpha-1} = p^\alpha t_\alpha + t'_{\alpha-1}$ such that $x_{\alpha-1} + p^{\alpha-1}t_{\alpha-1}$ lifts uniquely to $x_\alpha + p^\alpha t_\alpha$. It suffices to consider the case where $p \mid f'(x_{\alpha-1})$. For this, we have $(p, f'(x_{\alpha-1})) = p$.

- Suppose $p \mid \frac{f(x_{\alpha-1})}{p^{\alpha-1}}$, or equivalently, $p^\alpha \mid f(x_{\alpha-1})$. In this case the equation admits exactly p solutions (c.f. Lecture 10, *Linear congruence equation, congruence inverse, and Wilson's theorem*).
- Suppose $p \nmid \frac{f(x_{\alpha-1})}{p^{\alpha-1}}$, or equivalently, $p^\alpha \nmid f(x_{\alpha-1})$. In this case the equation admits no solution.

Theorem 4 (The second lemma of Hensel)**.** *Let $f(x)$ be a polynomial with integer coefficients, p a prime number, and $\alpha \in \mathbb{Z}$ such that $\alpha > 1$. Suppose a is a solution to $f(x) \equiv 0 \bmod p^{\alpha-1}$. Denote δ the number of solutions $x \equiv a \bmod p^{\alpha-1}$ to $f(x) \equiv 0 \bmod p^{\alpha}$. Then*

$$\delta = \begin{cases} 1, & p \nmid f'(a), \\ p, & p \mid f'(a),\ p^{\alpha} \mid f(a), \\ 0, & p \mid f'(a),\ p^{\alpha} \nmid f(a). \end{cases}$$

2. An example of application of Hensel's lemma

Problem 5. *Solve the following congruence equation*

$$x^3 + x^2 + 2x + 26 \equiv 0 \bmod 343.$$

Solution. Note that $343 = 7^3$. So we first consider $f(x) \equiv 0 \bmod 7$. For this, we have

x	-3	-2	-1	0	1	2	3
$f(x) \bmod 7$	2	4	3	5	2	0	5

So the solution to $f(x) \equiv 0 \bmod 7$ is read as $x = 7t_1 + 2$ with $t_1 \in \mathbb{Z}$. Next we consider $f(x) \equiv 0 \bmod 7^2$. This can be computed explicitly as

$$(7t_1 + 2)^3 + (7t_1 + 2)^2 + 2(7t_1 + 2) + 26 \equiv 28t_1 + 42 \equiv 0 \bmod 49,$$

so we have

$$4t_1 + 6 \equiv 0 \bmod 7 \implies 2t_1 \equiv -3 \equiv 4 \bmod 7 \implies t_1 \equiv 2 \bmod 7.$$

By taking $t_1 = 7t_2 + 2$ for $t_2 \in \mathbb{Z}$, the solution becomes $x = 7(7t_2 + 2) + 2 = 49t_2 + 16$ for $t_2 \in \mathbb{Z}$. Repeat this argument, we see the solution to $f(x) \equiv 0 \bmod 7^3$ looks like

$$x = 49(7t_3 + 2) + 2 = 343t_3 + 114, \quad t_3 \in \mathbb{Z}.$$

Thus, $f(x) \equiv 0 \bmod 343$ have a unique solution $x \equiv 114 \bmod 343$. □

Alternative Solution. We still work with

$$\frac{f(x_{\alpha-1})}{p^{\alpha-1}} + f'(x_{\alpha-1})t_{\alpha-1} \equiv 0 \bmod p.$$

Also, $f'(x) = 3x^2 + 2x + 2$. Using the same argument before, we have $x = 7t_1 + 2$ for $t_1 \in \mathbb{Z}$ being the candidate solution. So

$$\frac{f(2)}{7} + f'(2)t_1 \equiv 0 \bmod 7 \implies 6 + 18t_1 \equiv 0 \bmod 7,$$

which also implies $t_1 \equiv 2 \bmod 7$. Again, take $t_1 = 7t_2 + 2$ for $t_2 \in \mathbb{Z}$. So $x = 49t_2 + 16$ with $t_2 \in \mathbb{Z}$ is the solution of $f(x) \equiv 0 \bmod 7^2$.

Now it remains to consider

$$\frac{f(16)}{49} + f'(16)t_2 \equiv 0 \bmod 7 \implies 90 + 802t_2 \equiv 0 \bmod 7 \implies t_2 \equiv 2 \bmod 7.$$

Therefore, $t_2 \equiv 7t_3 + 2$ with $t_3 \in \mathbb{Z}$, and $f(x) \equiv 0 \bmod 343$ have a unique solution $x \equiv 114 \bmod 343$. □

3. A more difficult congruence problem

Problem 6. *Let $f(x) = x^2 + x + 34$. Solve the following congruence equations.*

(1) $f(x) \equiv 0 \bmod 27$,
(2) $f(x) \equiv 0 \bmod 81$.

Solution. First, we have $f'(x) = 2x + 1$.

(1) Note that

$$f(x) \equiv 0 \bmod 3 \implies x \equiv 1 \bmod 3 \implies x = 3t_1 + 1$$

for some $t_1 \in \mathbb{Z}$. Consider modulo 9: there is a equation

$$\frac{f(1)}{3} + f'(1)t_1 \equiv 0 \bmod 3$$

where $f(1) = 36$ and $f'(1) = 3$. Since $3 \mid f'(1)$ and $9 \mid f(1)$, by Hensel's second lemma (c.f. Theorem 4), there are 3 solutions to the equation above. Alternatively, this can also be computed directly as follows. The equation is written as $12 + 3t_1 \equiv 0 \bmod 3$, and hence $t_1 \equiv 0, 1, 2 \bmod 3$. For these three cases, one may take $t_1 = 3t_2$, $t_1 = 3t_2 + 1$, or $t_1 = 3t_2 + 2$, respectively. Then x equals either of $9t_2 + 1$, $9t_2 + 4$, or $9t_2 + 7$. Hence

$$x \equiv 1, 4, 7 \bmod 9$$

are the three solutions. Again, we consider modulo 27. If the solution that is to be lifted is $x \equiv 1 \bmod 9$, then the equation is read as

$$\frac{f(1)}{9} + f'(1)t_2 \equiv 0 \bmod 3$$

with $3 \mid f'(1) = 3$ and $27 \nmid f(1) = 36$. However, this admits no solution by Theorem 4. (Note that $4 + 3t_2 \equiv 3k$ for some k.) So we turn to consider $x \equiv 4 \bmod 9$. One obtains

$$\frac{f(4)}{9} + f'(4)t_2 \equiv 0 \bmod 3$$

with $3 \mid f'(4) = 9$ and $27 \mid f(4) = 54$. Hence there exist 3 solutions, say $t_2 \equiv 0, 1, 2 \bmod 3$. Consequently,

$$f(x) \equiv 0 \bmod 27 \implies x \equiv 4, 13, 22 \bmod 27.$$

(2) Resuming on (1), we consider the equation with $x \equiv 4 \bmod 27$; that is,

$$\frac{f(4)}{27} + f'(4)t_3 \equiv 0 \bmod 3$$

with $3 \mid f'(4) = 9$ and $3^4 = 81 \nmid f(4) = 54$. So this admits no solution by Theorem 4. Similarly, $x \equiv 13 \bmod 27$ cannot be lifted, as $3 \mid f'(13) = 216$ and $81 \nmid f(13) = 27$. Hence it remains to consider lifting $x \equiv 22 \bmod 27$. However, $3 \mid f'(22) = 45$ and $81 \nmid f(22) = 540$. To conclude, $f(x) \equiv 0 \bmod 81$ has no solution.

□

Exercise 7. Solve the congruence equation

$$f(x) = x^3 + 2x + 36 \equiv 0 \bmod (5^4 \times 7).$$

For this, first solve $f(x) \equiv 0 \bmod 5^4$ and $f(x) \equiv 0 \bmod 7$ respectively, and then apply Chinese remainder theorem to get a composite solution.

(Hint: the result may have a form $x \equiv b_1 M_1 M_1^{-1} + b_2 M_2 M_2^{-1} \bmod 4375$, where $M_1 = 7$, $M_2 = 625$, and $x \equiv b_1 \bmod 625$, $x \equiv b_2 \bmod 7$.)

School of Mathematical Sciences, Peking University, 100871, Beijing, China
Email address: daiwenhan@pku.edu.cn