Hensel's Lifting Theorem

Definition 6.5.1

Let $f(T) = c_n T^n + \cdots + c_1 T + c_0$ be an integer polynomial. Then its derivative is the integer polynomial

$$f'(T) = nc_n T^{n-1} + \cdots + c_1.$$

A root of $f(T)$ in R (either $\mathbb{Z}$ or $\mathbb{Z}/m$) is called a simple root if it is not a root of $f'(T)$ in R.

N.B. The derivative is formal, not necessarily related to what you learned in Calculus.

Theorem 6.5.2 (Hensel's lifting)

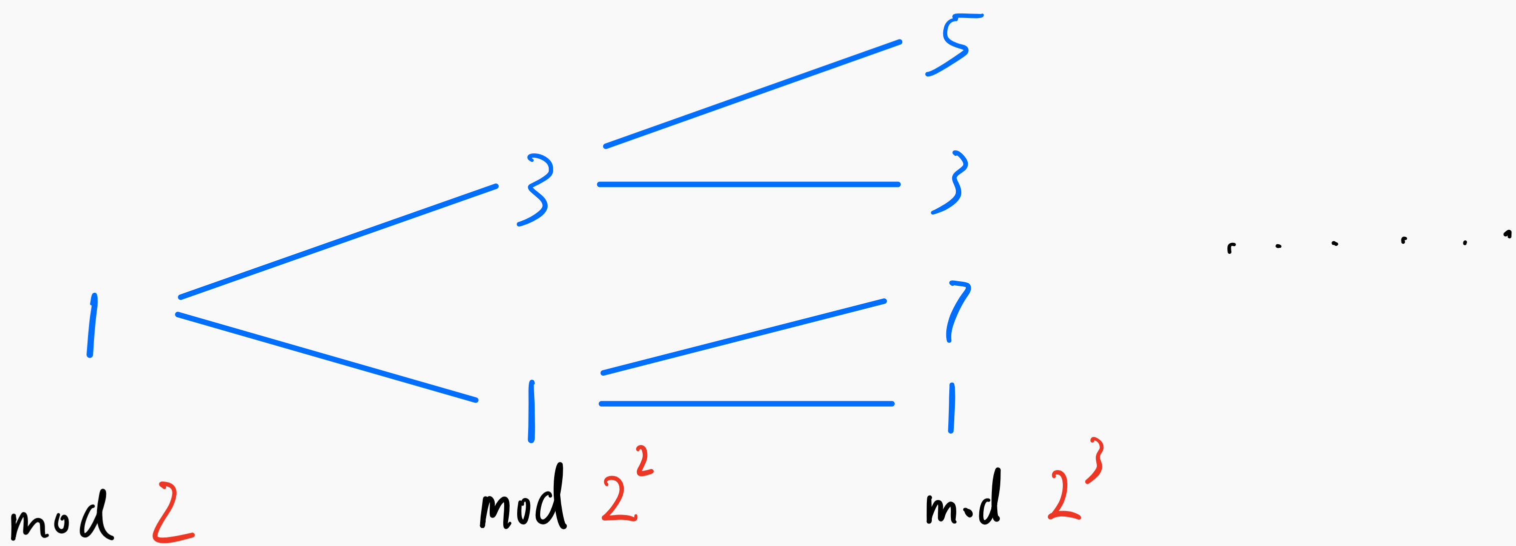
Let $f(T)$ be an integer polynomial, p be a prime, and e be a positive integer. If x is a root of $f(T) \mod p^e$ which descends to a simple root in $\mathbb{F}_p$, then x can be uniquely lifted to a root $\widetilde{x}$ of $f(T) \mod p^{2e}$.

Remark. One can replace $2e$ by any integer e' between e and $2e$: just reduce $\widetilde{x} \in \mathbb{Z}/p^{2e}$ to $\mathbb{Z}/p^{e'}$.

Hensel's Lifting Theorem

Example 6.5.3

The polynomial $T^2 - 1$ has no simple roots in $\mathbb{F}_2$ since its derivative $2T$ descends to the zero polynomial over $\mathbb{F}_2$. As a consequence, one cannot apply the Hensel's lifting. Indeed, The polynomial $T^2 - 1$ has multiple lifting of the duplicate root $\overline{1}$.



Sketch of the proof

Let x be a representative of a root of $f(T)$ in $\mathbb{Z}/p^e$. Then a representative of a lifting of that root can be written as

$$\widetilde{x} = x + t,$$

where t is some integer divided by p^e.

So our requirement can be interpreted as

$$f(x+t) \equiv 0 \pmod{p^{2e}}.$$

Now, we need a formal* version of *Taylor's expansion*:

$$f(x+t) = f(x) + \frac{f'(x)}{1!}t + \frac{f''(x)}{2!}t^2 + \cdots + \frac{f^{(n)}(x)}{n!}t^n,$$

where $f^{(k)}(T)$ is the k-th derivative of $f(T)$ and n is the degree of $f(T)$. What we need in particular is that each fraction $\frac{f^{(k)}(x)}{k!}$ is actually an integer. Hence, we have (notice that $p^e \mid t$)

$$f(x+t) \equiv f(x) + f'(x)t \pmod{p^{2e}}.$$

*There is NO continuity or calculus stuff involved.

Since x descends to a simple root in $\mathbb{F}_p$, by theorem 6.4.1, $f'(x)$ is invertible modulo any power of p. Therefore, the linear congruence equation

$$f(x) + f'(x)t \equiv 0 \pmod{p^{2e}}$$

always has a unique solution (up to congruence $\pmod{p^{2e}}$). Substituting this solution back to $\widetilde{x} = x + t$, we get a desired lifting.

We may summarize above by the formula*:

$$(\star) \qquad [\widetilde{x}]_{p^{2e}} = [x]_{p^{2e}} + [-f(x)]_{p^{2e}}[f'(x)]^{-1}_{p^{2e}}.$$

*Note that those operations are taking in $\mathbb{Z}/p^{2e}$.

Example 6.5.4

Solve the congruence $x^2 \equiv 7 \pmod{27}$.

Example 6.5.4

Solve the congruence $x^2 \equiv 7 \pmod{27}$.

Let $f(T)$ be the polynomial $T^2 - 7$. Then its derivative is $f'(T) = 2T$.

Notice that $27 = 3^3$. We start with $\mathbb{F}_3$.

Example 6.5.4

Solve the congruence $x^2 \equiv 7 \pmod{27}$.

Let $f(T)$ be the polynomial $T^2 - 7$. Then its derivative is $f'(T) = 2T$.

Notice that $27 = 3^3$. We start with $\mathbb{F}_3$.

Since $T^2 - 7$ descends to $T^2 - \overline{1}$ over $\mathbb{F}_3$, we see that $[1]_3$ and $[2]_3$ are two roots of $f(T)$ in $\mathbb{F}_3$.

Since $f'(1) = 2 \not\equiv 0 \pmod{3}$ and $f'(2) = 4 \not\equiv 0 \pmod{3}$, both $[1]_3$ and $[2]_3$ are simple roots.

Example 6.5.4

Solve the congruence $x^2 \equiv 7 \pmod{27}$.

Let $f(T)$ be the polynomial $T^2 - 7$. Then its derivative is $f'(T) = 2T$.

Notice that $27 = 3^3$. We start with $\mathbb{F}_3$.

Since $T^2 - 7$ descends to $T^2 - \overline{1}$ over $\mathbb{F}_3$, we see that $[1]_3$ and $[2]_3$ are two roots of $f(T)$ in $\mathbb{F}_3$.

Since $f'(1) = 2 \not\equiv 0 \pmod{3}$ and $f'(2) = 4 \not\equiv 0 \pmod{3}$, both $[1]_3$ and $[2]_3$ are simple roots. Moreover, the multiplicative inverses of $f'(1)$ and $f'(2)$ modulo 3 are 2 and 1 respectively.

Applying theorem 6.4.1, we can lift these multiplicative inverses from modulo 3 world to modulo 3^2 world:

$$[f'(1)]_3^{-1} = [2]_3 \implies [f'(1)]_{3^2}^{-1} = [2 \cdot (2 - 2 \cdot 2)]_{3^2} = [5]_{3^2},$$
$$[f'(2)]_3^{-1} = [1]_3 \implies [f'(2)]_{3^2}^{-1} = [1 \cdot (2 - 1 \cdot 1)]_{3^2} = [1]_{3^2}.$$

Applying theorem 6.4.1, we can lift these multiplicative inverses from modulo 3 world to modulo 3^2 world:

$$[f'(1)]_3^{-1} = [2]_3 \implies [f'(1)]_{3^2}^{-1} = [2 \cdot (2 - 2 \cdot 2)]_{3^2} = [5]_{3^2},$$
$$[f'(2)]_3^{-1} = [1]_3 \implies [f'(2)]_{3^2}^{-1} = [1 \cdot (2 - 1 \cdot 1)]_{3^2} = [1]_{3^2}.$$

Applying the Hensel's lemma (theorem 6.5.2, but more precisely, the formula ($\star$)), we get

$$[1]_3 \overset{\text{Hensel}}{\rightsquigarrow} [1]_{3^2} + [-f(1)]_{3^2}[f'(1)]_{3^2}^{-1} = [1 + 6 \cdot 5]_{3^2} = [4]_{3^2},$$
$$[2]_3 \overset{\text{Hensel}}{\rightsquigarrow} [2]_{3^2} + [-f(2)]_{3^2}[f'(2)]_{3^2}^{-1} = [2 + 3 \cdot 1]_{3^2} = [5]_{3^2}.$$

Next, we use theorem 6.4.1 again to lift the multiplicative inverses of $f'(4) = 8$ and $f'(5) = 10$ from $\mathbb{Z}/3^2$ to $\mathbb{Z}/3^3$:

$$[f'(4)]_{3^2}^{-1} = [8]_{3^2} \implies [f'(4)]_{3^3}^{-1} = [8 \cdot (2 - 8 \cdot 8)]_{3^3} = [17]_{3^3},$$
$$[f'(5)]_{3^2}^{-1} = [1]_{3^2} \implies [f'(5)]_{3^3}^{-1} = [1 \cdot (2 - 10 \cdot 1)]_{3^3} = [19]_{3^3}.$$

Next, we use theorem 6.4.1 again to lift the multiplicative inverses of $f'(4) = 8$ and $f'(5) = 10$ from $\mathbb{Z}/3^2$ to $\mathbb{Z}/3^3$:

$$[f'(4)]_{3^2}^{-1} = [8]_{3^2} \implies [f'(4)]_{3^3}^{-1} = [8 \cdot (2 - 8 \cdot 8)]_{3^3} = [17]_{3^3},$$
$$[f'(5)]_{3^2}^{-1} = [1]_{3^2} \implies [f'(5)]_{3^3}^{-1} = [1 \cdot (2 - 10 \cdot 1)]_{3^3} = [19]_{3^3}.$$

Applying the Hensel's lemma again, we get

$$[4]_{3^2} \overset{\text{Hensel}}{\rightsquigarrow} [4]_{3^3} + [-f(4)]_{3^3}[f'(4)]_{3^3}^{-1} = [4 + (-9) \cdot 17]_{3^3} = [13]_{3^3},$$
$$[5]_{3^2} \overset{\text{Hensel}}{\rightsquigarrow} [5]_{3^3} + [-f(5)]_{3^3}[f'(5)]_{3^3}^{-1} = [5 + (-18) \cdot 19]_{3^3} = [14]_{3^3}$$

Next, we use theorem 6.4.1 again to lift the multiplicative inverses of $f'(4) = 8$ and $f'(5) = 10$ from $\mathbb{Z}/3^2$ to $\mathbb{Z}/3^3$:

$$[f'(4)]_{3^2}^{-1} = [8]_{3^2} \implies [f'(4)]_{3^3}^{-1} = [8 \cdot (2 - 8 \cdot 8)]_{3^3} = [17]_{3^3},$$
$$[f'(5)]_{3^2}^{-1} = [1]_{3^2} \implies [f'(5)]_{3^3}^{-1} = [1 \cdot (2 - 10 \cdot 1)]_{3^3} = [19]_{3^3}.$$

Applying the Hensel's lemma again, we get

$$[4]_{3^2} \xrightarrow{\text{Hensel}} [4]_{3^3} + [-f(4)]_{3^3}[f'(4)]_{3^3}^{-1} = [4 + (-9) \cdot 17]_{3^3} = [13]_{3^3},$$
$$[5]_{3^2} \xrightarrow{\text{Hensel}} [5]_{3^3} + [-f(5)]_{3^3}[f'(5)]_{3^3}^{-1} = [5 + (-18) \cdot 19]_{3^3} = [14]_{3^3}$$

Therefore, the solution of $x^2 \equiv 7 \pmod{27}$ is $x \equiv 13$ or $14 \pmod{27}$.