Reduction and lifting

Reduction and lifting

Recall that whenever $n \mid m$, we have a reduction map

$$\mathbb{Z}/m \longrightarrow \mathbb{Z}/n.$$

When the congruence class $\alpha \in \mathbb{Z}/m$ is mapped to $\beta \in \mathbb{Z}/n$, we say "α descends to β", "β is a reduction of α", and "α is a lifting of β".

Reduction and lifting

Recall that whenever $n \mid m$, we have a reduction map

$$\mathbb{Z}/m \longrightarrow \mathbb{Z}/n.$$

When the congruence class $\alpha \in \mathbb{Z}/m$ is mapped to $\beta \in \mathbb{Z}/n$, we say "α descends to β", "β is a reduction of α", and "α is a lifting of β".

Question

Let $f(T)$ be an integer polynomial. Given a root β of $f(T)$ in $\mathbb{Z}/n$, how to lift it to a root α in $\mathbb{Z}/m$?

Note that: although we can always reduce a root in $\mathbb{Z}/m$ to a root in $\mathbb{Z}/n$, but the converse is not true. E.g. $[0]_2$ is a root of $T+2$ in $\mathbb{Z}/2$ but its natural lifting $[0]_4$ in $\mathbb{Z}/4$ is not a root.

Reduction and lifting

Theorem 6.4.1 (Lifting multiplicative inverse)

Let p be a prime and e be a positive integer. Then a multiplicative inverse x of a modulo p^e can always be lifted to a multiplicative inverse $\widetilde{x}$ of a modulo p^{2e}.

$$
\begin{tikzcd}
\cdots \arrow[r, dash] & a \arrow[r, dash] \arrow[d, phantom, "\cdot"] & a \arrow[r, dash] \arrow[d, phantom, "\cdot"] & \cdots \\
\cdots \arrow[r, rightsquigarrow] & x \arrow[r, rightsquigarrow] & \widetilde{x} \arrow[r, rightsquigarrow] & \cdots \\
\cdots & \bmod p^e \arrow[l] & \bmod p^{2e} \arrow[l] & \cdots \arrow[l]
\end{tikzcd}
$$

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

Proof. The requirement of $\widetilde{x}$ is

$$\widetilde{x} \equiv x \pmod{p^e} \qquad \text{and} \qquad a\widetilde{x} \equiv 1 \pmod{p^{2e}}.$$

The first tells us that $\widetilde{x}$ can be written as $x + up^e$. Plug it in the second, we get

$$ax + aup^e \equiv 1 \pmod{p^{2e}}.$$

Proof. The requirement of $\widetilde{x}$ is

$$\widetilde{x} \equiv x \pmod{p^e} \qquad \text{and} \qquad a\widetilde{x} \equiv 1 \pmod{p^{2e}}.$$

The first tells us that $\widetilde{x}$ can be written as $x + up^e$. Plug it in the second, we get

$$ax + aup^e \equiv 1 \pmod{p^{2e}}.$$

$ax \equiv 1 \mod p^e$

We know $ax = 1 + vp^e$ for some v. Hence, we get

$$aup^e \equiv 1 - ax = -vp^e \pmod{p^{2e}}.$$

$$\begin{aligned} aup^{e} &\equiv -vp^{e} \pmod{p^{2e}} \\ \Rightarrow au &\equiv -v \pmod{p^{e}} \\ \Rightarrow u &\equiv -xv \pmod{p^{e}}. \end{aligned}$$

$ax \equiv 1 \bmod p^e$

$$\begin{aligned} aup^e &\equiv -vp^e \pmod{p^{2e}} \\ \Longrightarrow au &\equiv -v \pmod{p^e} \\ \Longrightarrow u &\equiv -xv \pmod{p^e}. \end{aligned}$$

Therefore, we have

$$\begin{aligned} \widetilde{x} &= x + up^e \\ &\equiv x - xvp^e \pmod{p^{2e}} \\ &= x(1 - vp^e) = x(2 - ax). \end{aligned}$$

This finishes the proof. $\square$

Example 6.4.2

Find the multiplicative inverse of 2 modulo 27.

Example 6.4.2

Find the multiplicative inverse of 2 modulo 27.

First note that $27 = 3^3$. Hence, we start with modulo 3. The multiplicative inverse of 2 in $\mathbb{Z}/3$ is 2. Therefore, by Theorem 6.4.1, the multiplicative inverse of 2 modulo 3^2 is

$$[2]_{3^2}^{-1} = [2 \cdot (2 - 2 \cdot 2)]_{3^2} = [5]_{3^2}$$

Then, apply Theorem 6.4.1 again, the multiplicative inverse of 2 modulo 3^3 is

$$[2]_{3^3}^{-1} = [5 \cdot (2 - 2 \cdot 5)]_{3^3} = [13]_{3^3}.$$