We continue with a few more examples on counting the solutions to polynomial congruences modulo p^k using Hensel's lemma.

② $f(x) = x^2 + x + 7$. $\quad f(x) \equiv 0 \pmod{27}$

$f(0) = 7 \not\equiv 0 \pmod 3$ $\quad f(1) = 9 \equiv 0 \pmod 3$ $\quad f(2) = 13 \not\equiv 0 \pmod 3$

$f'(x) = 2x + 1$ and $f'(1) = 3 \equiv 0 \pmod 3$

In mod 9 either

- 1, 4, 7 are all solutions, or
- none of them is a solution.

$f(1) = 9 \equiv 0 \pmod 9 \Rightarrow 1$ is a solution mod 9

$\Rightarrow 1, 4, 7$ are solutions mod 9.

$f(1) = 9 \not\equiv 0 \pmod{27} \Rightarrow 1, 10, 19$ are not solutions in mod 27.

$f(4) = 27 \equiv 0 \pmod{27} \Rightarrow 4, 13, 22$ are solutions mod 27.

$f(7) = 63 \not\equiv 0 \pmod{27} \Rightarrow 7, 16, 25$ are not solutions in mod 27.

$\Rightarrow x \equiv 4, 13, 22 \pmod{27}$

③ $f(x) = x^3 + 4x^2 + 19x + 1$ $\qquad f(x) \equiv 0 \pmod{25}$

$f(0) \equiv 1$, $f(1) \equiv 0$, $f(2) \equiv 3$, $f(3) \equiv 1$, $f(4) \equiv 0 \pmod{5}$

$f'(x) = 3x^2 + 8x + 19$ $\qquad f'(1) \equiv 0 \pmod{5}$, $f'(4) \not\equiv 0 \pmod{5}$

- 4 can be lifted uniquely to mod 25.
- $f(1) = 25 \equiv 0 \pmod{25}$

$\Rightarrow$ 1, 6, 11, 16, 21 are solutions mod 25

So, $1 + 5 = 6$ solutions in mod 25.

Recall Fermat's Theorem

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{when } (a, p) = 1$$

Is it true when p is replaced with a composite number?

Not in general. For example,

$$3^3 \not\equiv 1 \pmod{4}$$

$$5^5 \not\equiv 1 \pmod{6}$$

Goal: To modify the proof of Fermat's Theorem to have a result mod n.

Is this true: $(a, n) = 1$. $\{1, 2, \ldots, n-1\}$ and $\{a, 2a, \ldots, (n-1)\cdot a\}$ are the same mod n?

- For example $\{1, 2, 3\} \equiv \{3, 6, 9\}$ mod 4.
- This will be true, but let's not prove it.

$$\Rightarrow 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1) \equiv a \cdot 2a \cdot 3a \cdot \ldots (n-1)\, a \pmod{n}$$

$$\Rightarrow 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1) \equiv a^{n-1} \cdot 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1) \pmod{n}$$

However, we cannot do the cancellations here because

$$ux \equiv uy \pmod{n} \Rightarrow x \equiv y \left(\bmod \frac{n}{(n,u)}\right)$$

To have the analog of Fermat's Theorem, we should work with

$$\{u : 1 \leqslant u \leqslant n-1 \text{ and } (n, u) = 1\}$$

instead of $\{1, 2, \ldots, n-1\}$.

Definition: We'll say u is a **unit** modulo n if it has an inverse (or equivalently $(u,n)=1$).

$u^{-1} \pmod{n}$: $uu^{-1} \equiv 1 \pmod{n}$

- Definition doesn't depend on the representative u of a congruence class.

e.g. $5 \pmod{6}$, $11 \pmod{6}$, $17 \pmod{6}$

Units of $\mathbb{Z}_8$: $1, 3, 5, 7$

Units of $\mathbb{Z}_9$: $1, 2, 4, 5, 7, 8$

Units of $\mathbb{Z}_{10}$: $1, 3, 7, 9$

Units of $\mathbb{Z}_p$: $1, 2, 3, \ldots, p-1$.

Theorem: Let u and v be units in $\mathbb{Z}_n$. Then,

- u^{-1}, v^{-1}
- $-u$, $-v$
- uv

are also units in $\mathbb{Z}_n$.

<u>Proof:</u> • u^{-1} and v^{-1} are units by definition

• $(-u)\cdot(-u^{-1}) \equiv 1 \equiv (-v)\cdot(-v^{-1}) \pmod{n}$

$\Rightarrow$ $-u$ and $-v$ are units

• $(uv)\cdot(u^{-1}v^{-1}) = uu^{-1}\cdot vv^{-1} \equiv 1 \pmod{n}$

$\Rightarrow$ uv is a unit.