Example: Solve the systems of linear congruences

(a) $x \equiv 1 \pmod{\underbrace{30}_{2\cdot 3\cdot 5}}$; $x \equiv 13 \pmod{\overbrace{36}^{4\cdot 9}}$; $x \equiv 11 \pmod{\overbrace{40}^{8\cdot 5}}$

(b) $x \equiv 11 \pmod{\underbrace{36}_{4\cdot 9}}$; $x \equiv 7 \pmod{\underbrace{40}_{8\cdot 5}}$; $x \equiv 32 \pmod{\underbrace{75}_{3\cdot 25}}$

(a) $x \equiv 1 \pmod 2$ $\quad$ $x \equiv 13 \pmod 4$ $\quad$ $x \equiv 11 \pmod 8$

$x \equiv 1 \pmod 3$ $\quad$ $x \equiv 13 \pmod 9$

$x \equiv 1 \pmod 5$ $\quad$ $x \equiv 11 \pmod 5$

$p=5$: $x \equiv 1 \pmod 5$ and $x \equiv 11 \pmod 5$

$\Rightarrow x \equiv 1 \pmod 5$

$p=3$: $x \equiv 1 \pmod 3$ and $x \equiv 13 \pmod 9$

$\Rightarrow x \equiv 4 \pmod 9$

$p=2$: $x \equiv 1 \pmod 2$ and $x \equiv 13 \pmod 4$ and $x \equiv 11 \pmod 8$

$x \equiv 11 \pmod 8 \Rightarrow x \equiv 11 \pmod 4$ not compatible with $x \equiv 13 \pmod 4$

incompatible

No solution.

(b) $x \equiv 11 \pmod{4}$; $x \equiv 7 \pmod{8}$

$x \equiv 11 \pmod{9}$

11

$x \equiv 32 \pmod{3}$

32

$x \equiv 7 \pmod{5}$

$x \equiv 32 \pmod{25}$

$p=2$: $x \equiv 7 \pmod{8}$ ✓

$p=3$: $x \equiv 11 \pmod{9}$ ✓

$p=5$: $x \equiv 32 \pmod{25}$ ✓

We are solving

(1) $x \equiv 7 \pmod{8}$

(2) $x \equiv 2 \pmod{9}$

(3) $x \equiv 7 \pmod{25}$

(1) and (3) : $x \equiv 7 \pmod{8}$

$x \equiv 7 \pmod{25}$ $\Rightarrow$ $x \equiv 7 \pmod{200}$

Now we solve

$$x \equiv 7 \pmod{200}$$

$$x \equiv 2 \pmod{9}$$

$$\overset{x}{\overset{\shortparallel}{200k+7}} \equiv 2 \pmod 9$$

$$\Rightarrow 200k \equiv -5 \pmod 9$$

$$\Rightarrow 2k \equiv 4 \pmod 9$$

$$\Rightarrow k \equiv 2 \pmod 9$$

$$x = 200k+7 = 200(9\ell+2)+7 = 1800\ell + 407$$

$$x \equiv 407 \pmod{1800}.$$

<u>Theorem:</u> (CRT) The congruences $x \equiv a_1 \pmod{m_1}$, $\dots$, $x \equiv a_k \pmod{m_k}$ has 0 or 1 solution in $\mathbb{Z}_m$, where $m = [m_1, m_2, \dots, m_k]$.

Exercise: read Theorem 3.12 and its proof from the textbook. It says

solution exists $\iff \gcd(m_i, m_j) \mid a_i - a_j$ for all $i \neq j$.

Some non-linear congruences

Solve $x^2 \equiv 1 \pmod{16}$.

$0^2 \equiv 0 \pmod{16}$, $1^2 \equiv 1 \pmod{16}$ no need to check
$3^2 \equiv 9 \pmod{16}$, $5^2 \equiv 25 \equiv 9 \pmod{16}$ even numbers
$7^2 \equiv 1 \pmod{16}$, $9^2 \equiv 1 \pmod{16}$, $11^2 \equiv 9 \pmod 5$
$13^2 \equiv 9 \pmod{16}$, $15^2 \equiv 1 \pmod{16}$

$\Rightarrow \quad x \equiv 1, 7, 9, \text{ or } 15 \pmod{16}$

Solve $\quad x^2 \equiv 1 \pmod{17}$

$17 \mid x^2 - 1 \quad \Rightarrow \quad 17 \mid (x-1)\cdot(x+1)$

$\Rightarrow \quad 17 \mid x-1 \quad \text{or} \quad 17 \mid x+1$

$\Rightarrow \quad x \equiv 1 \text{ or } 16 \pmod{17}$

Solve $\quad x^2 \equiv -1 \pmod{35}$

$5 \quad 7$

$x^2 \equiv -1 \pmod 5$ and $x^2 \equiv -1 \pmod 7$

$x \equiv 2, 3 \pmod 5$ no solution

$\Rightarrow$ no solution

Theorem: (CRT) If x has n_i possible values modulo m_i, for $i = 1, 2, \dots, k$ and $(m_i, m_j) = 1$ for all $i \neq j$, then x has $n_1 n_2 \dots n_k$ possible values modulo $m_1 m_2 \dots m_k$.

- How many solutions $x^2 \equiv 1 \pmod{p^\alpha}$ has?

Case - I : p is odd.

$p^\alpha \mid x^2 - 1 \Rightarrow p^\alpha \mid (x-1)\cdot(x+1)$ p cannot divide both

$\Rightarrow p^\alpha \mid x-1$ or $p^\alpha \mid x+1$

$\Rightarrow x \equiv 1$ or $-1 \pmod{p^\alpha}$

$\Rightarrow$ Two solutions

Case - II : $p = 2$

both of them even

one of them $4k+2$

$2^\alpha \mid x^2 - 1 \Rightarrow 2^\alpha \mid (x-1)\cdot(x+1)$

$\Rightarrow 2^{\alpha-1} \mid x-1$ and $2 \mid x+1$

or

$2 \mid x-1$ and $2^{\alpha-1} \mid x+1$

$\Rightarrow x \equiv 1$ or $-1 \pmod{2^{\alpha-1}}$

$\Rightarrow x \equiv 1, 2^{\alpha-1}-1, 2^{\alpha-1}+1, 2^\alpha - 1 \pmod{2^\alpha}$

$\Rightarrow$ Four solutions

However, $\alpha = 1$ and $\alpha = 2$ are exceptional cases (why?) For $\alpha = 1$: one sol. $\alpha = 2$: two sol

Question: How many solutions does the congruence $x^2 \equiv 1 \pmod{n}$ have in $\mathbb{Z}_n$?
(Example 3.18)