F9

Rep. $a \equiv b \pmod n$ eq. rel. on $\mathbb{Z}$.

Prop. $a \equiv b \iff a, b$ have same remainder $\rightsquigarrow$ eq. classes are $[0], \dots, [n-1]$.

• Reduce mod $n$.

Thm. $\equiv$ respects $\cdot, +, -$ $\quad (\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}_n)$

Ex. Reduce $2^{40} \cdot 5^{16} - 3^{14} \cdot 13^{9} \pmod 7$.

• Warning! Only $\cdot, +, -$. Not e.g. exponents.

• Inverse mod $n$; unique $\pmod n$ if $\exists$

Thm. $a$ invertible mod $n \iff \gcd(a, n) = 1$ (coprime)

Ex. Invert 9 mod 52.

Ex. Solve $9x \equiv 3 \pmod{52}$.

if time [Ex. Prove $a_n \cdots a_1 a_0$ (base 10) is div. by 3 iff $a_n + \cdots + a_1 + a_0$ is.]

CRT. $n_1, \dots, n_m$ pairwise coprime

$$\Rightarrow \begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_m \pmod{n_m} \end{cases} \quad \text{has unique sol.} \pmod{n_1 \cdots n_m}.$$

The sol. is $x \equiv \sum_{i=1}^{m} a_i d_i N_i$,

with $N_i = \dfrac{n_1 \cdots n_m}{n_i}$ and $d_i N_i \equiv 1 \pmod{n_i}$.

Ex. Solve $\begin{cases} x \equiv 2 \pmod 4, \\ x \equiv 3 \pmod 5, \\ x \equiv 6 \pmod 9. \end{cases}$

sketch may be enough [Pf of CRT]

Ex. Solve $x^3 + 4x + 1 \equiv 0 \pmod{30}$
[or $\pmod{60}$ if time]