

Think about the solution. Want $x \in \mathbb{Z}$.

Such a solution might have 4 components.

$$x = \underbrace{5 \cdot 7 x_1 + 3 \cdot 7 \cdot x_2 + 3 \cdot 5 x_3}_{x_0} + \boxed{3 \cdot 5 \cdot 7 \cdot n} \quad n \in \mathbb{Z}.$$

Find suitable x_1, x_2, x_3 .

Plug in x into first congruence:

$$35x_1 \equiv 2 \pmod{3}$$

Plug in x into second:

$$21x_2 \equiv 3 \pmod{5}$$

$$15x_3 \equiv 2 \pmod{7}$$

(61)

Thm. (Chinese Remainder Thm)

Let $m_1, m_2, m_3 \in \mathbb{N}$ be pairwise coprime!

$$\gcd(m_1, m_2) = \gcd(m_1, m_3) = \gcd(m_2, m_3) = 1$$

For $a_1, a_2, a_3 \in \mathbb{Z}$, the system

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$x \equiv a_3 \pmod{m_3}$$

has a solution, which is unique in $\mathbb{Z}_N$

$$N = m_1 \cdot m_2 \cdot m_3.$$

(62)

$$\cdot 35x_1 \equiv 2 \pmod{3}$$

$$2x_1 \equiv 2 \pmod{3}$$

$$x_1 = 1$$

$$\cdot 15x_3 \equiv 2 \pmod{7}$$

$$x_3 \equiv 2 \pmod{7}$$

$$x_3 = 2.$$

$$\cdot 21x_2 \equiv 3 \pmod{5}$$

$$x_2 \equiv 3 \pmod{5}$$

$$x_2 = 3$$

$$x = 128 + 105n$$

$$n \in \mathbb{Z}$$

$$x_0 = 35 \cdot 1 + 21 \cdot 3 + 15 \cdot 2$$

$$= 35 + 63 + 30 = 128$$

$$\equiv 23 \pmod{105}$$

(63)

$$x = 23 + 105n$$

$$n \in \mathbb{Z}.$$

Ex: 3 comets orbital periods 3, 8, and 13.

Their most recent perihelion was 2020, 2021, and 2021. What year will all 3 appear?

Ans: 2125.

Composite ^{integers} numbers are not prime numbers.

Euclid's lemma. Let $a, b \in \mathbb{Z}$.

If p is prime and $p \mid a \cdot b$, then

$p \mid a$ or $p \mid b$.

Ex: $p=6$, $a=2$, $b=3$.

$6 \nmid 2$ $6 \nmid 3$

Fundamental Theorem of Arithmetic

Every integer $n > 1$, can be written as a product of powers of primes:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_r^{e_r}, =: \prod_{i=1}^r p_i^{e_i}$$

where p_i (for $i \in \{1, \dots, r\}$) are pairwise distinct primes and $e_i \geq 1$.

Ex: $360 = 2^3 \cdot 3^2 \cdot 5$.

Using this can get gcd & lcm.

$$a = \prod_{i=1}^r p_i^{e_i},$$

$$b = \prod_{j=1}^s q_j^{f_j}$$

$$\begin{array}{l} \min \\ \max \end{array} \left\{ \begin{array}{l} \gcd(a, b) = \prod_{k=1}^t p_k^{\min(e_k, f_k)} \\ \text{lcm}(a, b): \text{ similar but with max.} \end{array} \right. \quad (p_k = q_k).$$

Thm. (Fermat's little theorem)

Let p be a prime, and assume

$$a \not\equiv 0 \pmod{p}.$$

Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

$$a^p \equiv a \pmod{p}$$

Use? Can use to reduce very large exponents in $\mathbb{Z}_p$.

Fermat's Last Thm '94

$$x^n + y^n = z^n$$

$n > 2$ has no solutions.

Modern
crypt.

Ex: $x^2 \equiv 68 \pmod{19}$

Reduce:

$$x^2 \equiv 11 \pmod{19}.$$

Note: $7^2 = 49 = 19 + 30 = 11 + 2 \cdot 19 \equiv 11 \pmod{19}$

$$(-7)^2 = (-1)^2 \cdot 7^2 \equiv 11 \pmod{19}$$

Since $-7 \equiv 12 \pmod{19}$: $\nexists x \equiv 7$ or $x \equiv 12$.

Ex: $x^3 \equiv 91 \pmod{23}$.

(68)