

Num theory mixed

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \quad \lfloor -2.5 \rfloor = -3$$

$$\lceil x \rceil \geq x > \lceil x \rceil - 1 \quad \lceil -2.5 \rceil = -2$$

$$\lfloor n+x \rfloor = n + \lfloor x \rfloor$$

$$\{x\} \quad \{3.45\} = 0.45$$

$$\{3.451\} = 0.451$$

$$x = \lfloor x \rfloor + \{x\}$$

factor multiple
 $a|b \rightarrow b = a \cdot k$

$$a|b, a|c \Rightarrow a|bx + cy \quad \forall x, y \in \mathbb{Z}$$

$$a|b, c \text{ and } \gcd(a, b) = 1 \Rightarrow a|c$$

gcd(1129, 251)

iterator	r_i	q_i	b_i
	1129		1
0	251	4	1
1	124	2	1
2	3	41	1
$n = 3$	1	3	1
	0		

$$P_0 = q_0 \quad Q_0 = 1$$

$$P_1 = q_0 q_1 + 1 \quad Q_1 = q_1$$

$$P_i = q_i P_{i-1} + P_{i-2} \quad Q_i = q_i Q_{i-1} + Q_{i-2}$$

$$x_0 = (-1)^{n-1} Q_{n-1} \left(\frac{c}{\gcd} \right)$$

$$y_0 = (-1)^{n-1} P_{n-1} \left(\frac{c}{\gcd} \right)$$

E.g. 10 Let x be an integer such that
 $x \equiv 2 \pmod{3}$
 $x \equiv 4 \pmod{5}$
 $x \equiv 1 \pmod{7}$
 Find the smallest positive integer
 k such that $x \equiv k \pmod{105}$

$$\begin{array}{r} m \rightarrow m \\ 5 \cdot 7 \mid 35 \\ 3 \cdot 7 \mid 21 \\ 3 \cdot 3 \mid 15 \end{array}$$

$$\begin{array}{l} u_1 y \\ y_1 \cdot 35 \equiv 1 \pmod{3} \\ y_2 \cdot 21 \equiv 1 \pmod{5} \\ y_3 \cdot 15 \equiv 1 \pmod{7} \end{array} \quad \begin{array}{l} v_1 \\ 2 \\ 1 \\ 1 \end{array}$$

$$\sum a m_i \pmod{M}$$

$$= 2 \cdot 35 \cdot 2 + 4 \cdot 21 \cdot 1 + 7 \cdot 1 \cdot 15$$

$$= 140 + 84 + 105$$

$$= 329 \pmod{105}$$

$$= 26$$

Bi-linear Diophantine. Eq

$$ax + by = c$$

Euler func.

$$\phi(n)$$

$$\phi(p) = p-1$$

$$\phi(mn) = \phi(m) \cdot \phi(n)$$

$$\phi(p^n) = p^n - p^{n-1}$$

$$\phi(n) \equiv 1 \pmod{n}$$

$$x^{\phi(n)} \equiv 1 \pmod{n}$$

$$(\gamma)_{11}^{-1} = [\gamma]_{11}$$

$$(\gamma)_{11}^{-1} = (\gamma)_{11}^{-1} \pmod{11}$$

$$[\gamma]_{11}^{-1} = [\gamma]_{11}^{-1} \pmod{11}$$

$$ah[2]_{11} + [7]_{11} = [x]_{11} \pmod{11}$$

$$[x]_{11} = [7]_{11}^{-1} = [x]_{11}$$

$$[x]_{11} = [7]_{11}^{-1} = [x]_{11}$$

$$[x]_{11} = [7]_{11}^{-1} = [x]_{11}$$

(S1 is a prime number) and (S2 is a prime number) and (S3 is a prime number)

$\{r \leftrightarrow q\} \text{ AND } \{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$

$\{r \leftrightarrow q\}$

$\{q \leftrightarrow p\}$