Division algorithm:

$$a = q \cdot n + r \quad , \; n > 0 \text{ and } q \in \mathbb{Z}, r \in \mathbb{N}$$

quotient

remainder

$r = \text{rem}(a,n)$

$q = \text{qnt}(a,n)$

ex: $a = 70 \quad , \quad n = 15$

$$\underset{}{70} = \underset{q}{4} \cdot \underset{n}{15} + \underset{r}{10}$$

ex: $a = -11, \; n = 7$

$$-11 = (-2)7 + 3$$

Modular Arithmetic:

We define $\text{rem}(a, n) = a \mod n$

$a = q \cdot n + r$

$= q \cdot n + (a \mod n)$

ex: $11 \mod 7 = 4 \mod 7$

$-11 \mod 7 = 3 \mod 7$

a and b are congruent modulo n if:

$$a \bmod n = b \bmod n$$

is written as:

$$a \equiv b \mod n$$

$$n \mid (a-b)$$

ex:

$$29 \equiv 15 \mod 7 \qquad 7 \mid (29-15) = 7 \mid 14$$

ex:

$7 \equiv 2 \mod 5$ and $11 \equiv 1 \mod 5$

$18 \equiv 3 \mod 5$

$$\boxed{a+c \equiv b+d \mod n}$$

$77 \equiv 2 \mod 5$

$$\boxed{a \cdot c \equiv b \cdot d \mod n}$$

$$(a+b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$$

ex:

$11 \bmod 8 \equiv 3$, $15 \bmod 8 \equiv 7$

$$((11 \bmod 8) + (15 \bmod 8)) \bmod 8$$

$$= (3+7) \bmod 8 = 10 \bmod 8 \equiv 2$$

ex:

$$x \equiv 4 \pmod{23}$$

$$x = 4 + k \cdot 23$$

$$x = \begin{cases} 27 \\ 50 \\ 73 \; \ldots\ldots \end{cases}$$

Greatest Common Divisor: (GCD) gcd

gcd(a, b) is the largest <u>positive</u> integer that divides both a and b.

<u>I</u>f gcd(a, b) = 1, a and b are relatively prime (Co-prime)

The Euclidean Algorithm:

Let $a \geq b > 0$

Input: a, b $\quad a \geq b > 0$

Output: $\gcd(a,b)$

if b divides a
    return b
else return $\gcd(b, a \bmod b)$

__ex:__ $\gcd(65042, 40902)$

$65042 = 1 \cdot 40902 + 24140$

$40902 = 1 \cdot 24140 + 16762$

$24140 = 1 \cdot 16762 + 7378$

$16762 = 2 \cdot 7378 + 2006$

$7378 = 3 \cdot 2006 + 1360$

$2006 = 1 \cdot 1360 + 646$

$1360 = 2 \cdot 646 + 68$

$646 = 9 \cdot 68 + 34$

$68 = 2 \cdot 34 + 0$

$\gcd(65042, 40902) = 34$