15) 56 (3
45
11

56 mod 15

Exclidean Alg.

gcd (56, 15)

gcd (56, 15)

60, 24 → 12 · 2 = 12 · 5

(12)

a mod

Modular Arithmetic

3x mod 7 = 1

x

7 mod 3 = 4

7 mod 3 7 ≡ 4.

4 mod 3

Extended Exclidean Alg

$(56 \cdot s + 15 \cdot t) = \gcd(56, 15)$

a b

$a = bq + r$

~~56 = 15 · (3) + (11)~~

$a \equiv b$

a mod b

24

12 · 2

4 = 2 · 2

$a = bq + r \Rightarrow \gcd(a,b) = \gcd(b,r)$

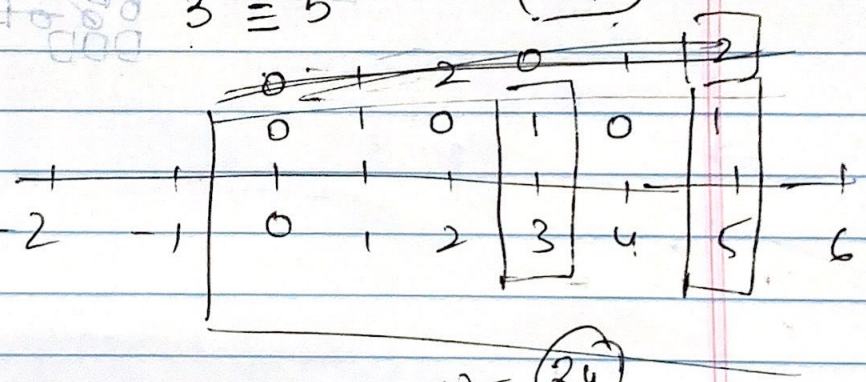
$a = bq + r$ $\quad \gcd(a,b) = d$ if $\gcd(b,r) = d$

$a \equiv b$

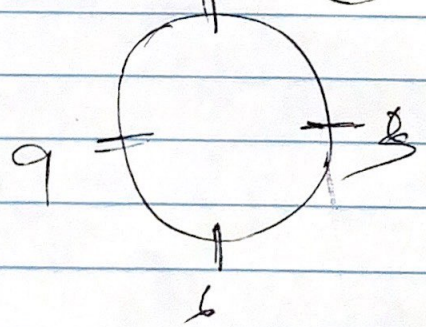
$\mathbb{Z}_2 = \{0, 1, 2\}$

$3 \equiv 5$

(0 1)



(24)



9
24
33

(33)

(9 am)

$a \equiv b$

$a \bmod b = b \bmod a$

$g(a,b) = g(b,r)$

~~15 · 5 + ·~~

$56 \cdot s + 15 \cdot t = \gcd(56,15)$

$a \cdot s + b \cdot t = \gcd(a,b)$

(1)

$a = bq + r$

$56 = 15(3) + (11)$

$15 = 11(1) + (4)$

$11 = 4(2) + (3)$

$4 = (3)(1) + (1)$

~~$3 = (1)(3) + (0)$~~

Proved Euclidean Alg

$\gcd(56,15) = 1$ (1)

$a \bmod b$

$56 \bmod 15 = 11$

$a_1 \bmod b_1$

$15 \bmod 11$

$a_2 \bmod b_2$

$11 \bmod 4$

Rewrite →

$56(\ ) + 15(\ ) = 1$

$56(\ ) + 15(\ ) = 11$

$56 \bmod 15 = 11$

$$-11 + 3 \cdot 4 = 1$$

$$-11 + 3\left[15 - 11(1)\right] = 1$$

$$-11 + 3 \cdot 15 - 11 \cdot (3) = 1$$

$$-11 \cdot 4 + 3 \cdot 15 = 1$$

$$-\left[56 - 15(3)\right] 4 + 3 \cdot 15 = 1$$

$$\Rightarrow 56 \cdot (-4) + 15 \cdot 12 + 3 \cdot 15 = 1$$

$$\Rightarrow 56(-4) + 15 \cdot 15 = 1$$

$$56(s) + 15(t) = \underline{\gcd(56, 15)}$$

$$1$$

$s = -4$

$t = 15$

$s \cdot t$

↳ ↳

computing variable

$Z_t \{1, 2, 3\}$

$56 \bmod 15$

$11 \bmod 15$

Congruent modulo / Modular Arithmetic

how to ~~do~~ compute modular way.

→ Two integers a and b are said to be congruent modulo n if

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

This can be written ↓

$$a \equiv b \pmod{n} \quad (\text{or}) \quad b \equiv a \pmod{n}$$