ECE 471/571 Modular Arithmetic

b divides a, if $a = b \cdot m$ m is integer

$b \mid a$. b is a divisor of a

24 : 1, 2, 3, 4, 6, 8, 12, 24.

$12 \mid 24$. , $13 \mid 182$, $-5 \mid 30$, $-3 \mid 33$

$17 \mid 0$

properties: ①. if $a \mid b$, and $b \mid c$, $\Rightarrow a \mid c$

e.g $11 \mid 66$, $66 \mid 198$, $11 \mid 198$.

②. if $b \mid g$, $b \mid h$, $\Rightarrow b \mid (m \cdot g + n \cdot h)$

$\forall$, m, n, are integers.

e.g. $7 \mid 14$, $7 \mid 63$.

$7 \mid (2 \times 14 + 3 \times 63) = (2 \times 2) \times 7 + (3 \times 9) \times 7$

Division Alg.

– Given any positive integer n, integer a.

$$a = q \cdot n + r \qquad 0 \le r < n$$

q: quotient. r: remainder / residue.

$$70 = 4 \times 15 + 10. \qquad q = \left\lfloor \frac{a}{n} \right\rfloor$$

$q = 4. \quad r = 10$

$$11 = 1 \times 7 + 4.$$

$q = 1. \quad r = 4.$

△ Modulus. n

$a \bmod n$: remainder of a divided by n.

$11 \bmod 7 = 4.$

$-11 \bmod 7 = 3.$

△ congruence. integers a, b.

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

$a \equiv b \pmod n$

e.g. $73 \equiv 4 \pmod{23}$

$21 \equiv -9 \pmod{10}$

△ properties.

① $a \equiv b \pmod{n} \Leftrightarrow n \mid (a-b)$ (if and only if)

eg $23 \equiv 8 \pmod{5}$ $\quad 23-8=15=5\times 3$.

$5 \mid 15$

② $a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n}$

③ $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$

$\Rightarrow a \equiv c \pmod{n}$

eg $11 \equiv 4 \pmod{7}$ $\quad -3 \equiv 4 \pmod{7}$

$\Rightarrow 11 \equiv -3 \pmod{7}$.

Modular Addition, Multiplication.

- e.g. $(5+7) \bmod 10 = 2$

$(5\times 7) \bmod 10 = 5$

arith. operations with set $\{n-1, 0, 1, \ldots\}$

(group)

properties:

① $(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$.

② $(a-b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$

③ $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

e.g. $(978 + 1047) \bmod 10 = (8 + 7) \bmod 10$

$= 5$

$(111 \times 112) \bmod 10 = 2$

Mod. Exponentiation

$11^7 \bmod 13 = ?$

$11^2 \times 11^2 \times 11^2 \times 11 \bmod 13$

$121 \bmod 13 = 4$

$= 4^3 \times 11 \bmod 13$

$= 16 \times 4 \bmod 13 \times 11 \bmod 13$

$= 3 \times 4 \bmod 13 \times 11 \ldots$

$= 12 \times 11 \bmod 13$

$= 132 \bmod 13 = 2$

Additive Identity (A.I)

$\underline{0}$ is A.I in Z_n.

$a + 0 = a \bmod n$

$b, a, \in Z_n$

$a + b \equiv 0 \bmod n.$

a and b are additive inverse mod n.

$a, -a = b$

$4 + 4 \equiv 0 \bmod 8.$

$7 + 1 \equiv 0 \bmod 8.$

$-7 = 1 \mod 8$.

Multiplicative Identity. . 1

$a \cdot 1 \equiv a \mod n$.

$a \cdot b \equiv 1 \mod n$. $\Leftrightarrow$ -1

multiplicative Inverse $a = b \pmod n$

$5 \cdot 5 \equiv 1 \mod 8$.

$3 \cdot 3 \equiv 1 \mod 8$.

$3^{-1} = 3 \mod 8$

$5^{-1} = 5 \mod 8$.

1, 3, 5, 7.

---

relatively prime

a is rela. prime with n

if $GCD(a, n) = 1$.

greatest common divisor

e.g. 7, 8

☆ Multiplicative Inverse exists iff
a is rela. prime with n