100
60 40
25 15 Quizzes (3)
mid

التاريخ: Divisibility الموضوع: Lec 1

Divisibility :-

$b \mid a \Leftrightarrow$ b يقسم a عندما يوجد عدد صحيح k بحيث $a = bk$

Theorem- Definition :- If $a, b \in \mathbb{Z}$, $b \neq 0$ then a is divisible by b (or b divides a) ($b \mid a$) if there is an integer k such that $a = bk$

$b \mid a$ → boolean value → true / false

(b) is a factor of a
(a) is a multiple of b
• if b doesn't divide a write $b \nmid a$

ex
$4 \mid 20$ $\quad -4 \mid 12$ $\quad 4 \nmid 15$

Properties $\quad a, b, c \in \mathbb{Z}$

1) • if $c \mid a \wedge c \mid b \longrightarrow c \mid (a \pm b)$
2) • if $a \mid b \longrightarrow a \mid bc$
3) • if $a \mid b \wedge b \mid c \longrightarrow a \mid c$
4) • if $a \mid b \wedge a \mid c \rightarrow a \mid (mb + nc)$ for $m, n \in \mathbb{Z}$

Proofs

① $c \mid a \wedge c \mid b$
$a = k_1 c$, $b = k_2 c$
for some $k_1, k_2 \in \mathbb{Z}$
$a + b = (k_1 + k_2) c$
$a - b = (k_1 - k_2) c$

② If $a \mid b$
$b = ka$ * c
$bc = (kc)a$
$\therefore a \mid bc$ (int)

③ If $a \mid b \wedge b \mid c$
$\therefore b = k_1 a$, $c = k_2 b$
for some $k_1, k_2 \in \mathbb{Z}$
$c = (k_2 k_1) a = a *$ int
$\therefore a \mid c$

④ $a \mid b \wedge a \mid c \rightarrow a \mid (mb + nc)$, $m, n \in \mathbb{Z}$
$b = k_1 a$, $c = k_2 a$ for some $k_1, k_2 \in \mathbb{Z}$
$mb + nc = mk_1 a + nk_2 a = (mk_1 + nk_2) a$
$= int * a$
$\therefore a \mid (mb + nc)$, $m, n \in \mathbb{Z}$

التاريخ: / /

الموضوع:

Division remainders:-

Assume $b \in \mathbb{Z}^+$, $a \in \mathbb{Z}$

$$\frac{a}{b} = q + \frac{r}{b}, \quad q \in \mathbb{Z}, r \in \mathbb{Z}$$

(r: remainder, q: quotient)

$$0 \leq r < b$$

$$\boxed{a = qb + r}$$

يعني لو قسم a عدد الى مجموعات حجمها b ، بنزل مجموعات واحد واحد ممكن يبقى بعض العناصر في a مش كافيين اني اكون مجموعة جديدة $\in$ عدد العناصر المتبقية r عدد المجموعات q

∴ There exists a unique pair (q, r) for every $a \in \mathbb{Z}, b \in \mathbb{Z}^+$

If $r = 0 \longrightarrow b \mid a$

Existance:

$$\boxed{q = \left\lfloor \frac{a}{b} \right\rfloor} \rightarrow \text{int}$$

$$r = a - qb \rightarrow \text{int}$$

$$\boxed{r = a - \left\lfloor \frac{a}{b} \right\rfloor b}$$

$$\frac{a}{b} - 1 < \left\lfloor \frac{a}{b} \right\rfloor \leq \frac{a}{b} \quad \times -b$$

$$-a \leq -\left\lfloor \frac{a}{b} \right\rfloor b < b - a \quad +a$$

$$0 \leq a - \left\lfloor \frac{a}{b} \right\rfloor b < b$$

$$\boxed{0 \leq r < b} \quad \#$$

Uniqueness :- نفترض في pair تحقق الشروط

Assume there exists another pair (q_2, r_2)

$$a = qb + r = q_2 b + r_2$$

$$(q - q_2)b = r_2 - r$$

- $q = q_2$, $r_2 = r$ — Same pair
- $q \neq q_2$, assume w.l.o.f $q > q_2$

$$q \geq q_2 + 1$$

$$q - q_2 \geq 1$$

$$(q - q_2)b \geq b$$

$$r_2 - r \geq b$$

$$r_2 \geq r + b$$

if $r < b$

$$r_2 \notin [0, b)$$ Contradiction

∴ there exist unique pair

$$a = qb + r$$
$$q = \lfloor \frac{a}{b} \rfloor$$

$$r = a - q * b$$

التاريخ: / / الموضوع: ______

Ex

$$\frac{15}{4} = 3 + \frac{3}{4}$$

$$\frac{12}{4} = 3 + \frac{0}{4}$$

$$\frac{-13}{4} = -4 + \frac{3}{4}$$

Lemma:

→ Integers a_1 and a_2 have same remainder when divided by b **iff** $a_1 - a_2$ is divisible by b $\quad \boxed{b \mid (a_1 - a_2)}$

proof

① a_1, a_2 have same remainder when divided by b

$$\therefore \frac{a_1}{b} = q_1 + \frac{r}{b} \quad , \quad \frac{a_2}{b} = q_2 + \frac{r}{b}$$

$$\frac{a_1 - a_2}{b} = q_1 - q_2 = \text{Integer}$$

($q_1 - q_2$ → int)

$$\therefore b \mid (a_1 - a_2)$$

② if $b \mid a_1 - a_2 \Rightarrow a_1 - a_2 = q \cdot b$

$$a_1 = a_2 + qb$$ (q → int)

let $a_2 = q_2 b + r_2$ (r_2 → remainder of a_2)

$$a_1 = (q_2 + k)\, b + r_2$$ (r_2 → remainder of a_1)

$\therefore r_2$ = remainder of a_1, a_2 when divided by b

حتة برمجة

$a = qb + r \;, \; 0 \le r < b$

اطرح a من b recursively

كل ما الناتج تبقا +ve integer less than b

الناتج هو r

عدد مرات الطرح q.

طب لو a سالب

← نضيف b بدلا من الطرح

لين توقف لما الناتج يبقا عدد موجب

أقل من b

$a = kb + r$

$0 \xrightarrow{r} b-1$

Ex assume $2 \nmid a$

what possible remainders can a have when divided by 4?

لو odd

$a = 2k + 1$ (b, r)

$\frac{a}{4} = \frac{2k+1}{4}$

لو عوضت (int + رقم/4)

k even	k odd
$k = 2m$ → int	$k = 2m+1$ → int
$\frac{a}{4} = \frac{4m+1}{4}$	$\frac{a}{4} = \frac{4m+2+1}{4}$
$= m + \frac{1}{4}$	$= m + \frac{3}{4}$
$r = 1$	$r = 3$

∴ Possible remainders

$r = 1$ or 3

سؤال! لو even a?

نفس نفس الطريقة

$a = 2k$

كمل ↓↓

Ex: Given 4 integers a, b, c, d

Is it true that two of these four integers have the same remainders divided by 3?

$a = 3q + r$

$r \in \{0, 1, 2\}$

by pigeon hole rule → $\lceil \frac{N}{k} \rceil$

(N = 4, k = 3)

$n = \lceil \frac{4}{3} \rceil = 2$

∴ true

Ex How many 3-digit non negative that have remainder 7 when divided by 101? assume that 1-digit and 2-digit numbers are also 3-digit (start with zero)

sol $a = q \cdot 101 + 7 = 101q + 7$

$b \quad r$

$q : 0, 1, 2, 3, \dots, 9$

req number = 10

another sol

$949 / 101 = 9 + \frac{90}{101}$

remainder = 7

$9 + \frac{7}{101}$

$n = 10$

$a = 1000$ 4 digit

3 digit

Ex: What is the remainder and quotient of 3756 when divided by 10?

$\frac{3756}{10} = 375 + \frac{6}{10}$

proof

has n digits

$a = (a_{n-1}\ a_{n-2} \dots a_1\ a_0)_{10}$

$= a_0 + 10\,a_1 + 10^2 a_2 + \dots + 10^{(n-1)} a_{n-1}$

$\frac{a}{10} = \frac{a_0}{10} + a_1 + 10 a_2 + \dots + 10^{n-2} a_{n-1}$

int $\quad$ int

$0 \le a_0 \le 9$

remainder a_0 last digit

Quotient $q = a_{n-1} \dots a_1$

digit آخر digits

on general (lemma)

suppose we divide a by 10

Then the remainder is the last digit of a

the quotient is the number formed by all digits of a except the last one

التاريخ: / /

الموضوع:

Corollary: An integer is divisible by 10 iff its last digit is 0

Ex Is $\overset{a}{7343}$ divisible by 5?

sol

$a = 734 * 10 + 7$

$\frac{a}{5} = 734 * 2 + \frac{7}{5}$

$= 7342 * 2 + \frac{5+2}{5} = 7342 * 2 + 1 + \frac{2}{5}$ ← remainder

$\therefore a \nmid 5$

Divisibility by 5

Lemma

an integer is divisible by 5 iff its last digit is 0 or 5

sol

let b = last digit of a

$a - b$

The last digit of $a-b$ is zero.

$\therefore 10 \mid (a-b) \Rightarrow a - b = 10k \ (k \in \mathbb{Z}) = 5 * (2k)$

$= 5 * \text{integer}$

$\therefore 5 \mid (a-b)$

$\therefore a, b$ have the same remainder when divided by 5

remainder when dividing b by 5: 0, 1, 2, 3, 4

b: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

(5 ✗)

→ 0, 1, 4, 3, 0, 1, 4, 3, 4

b is divisible by 5 when $b = 0$ or 5

lec②

التاريخ: / / الموضوع: _____

An integer a is divisible by 10 iff last digit is 0

Div. by 2

Int a is divisible by 2 iff it's last digit is 0, 2, 4, 6 or 8

Proof

let b: last digit of a

last digit of (a-b) is 0

(a-b) is divisible by 10

$10 \mid a-b$

$2 \mid 10$

$2 \mid a-b$ ∴ The remainder of $a/2$ is the same as remainder of $b/2$

b: 0, 1, 2, ... 9

remainder: 0, 1, 0, 1, ..., 0, 1 when divides b over 2

b	0	1	2	3	4	5	6	7	8	9
r	0	1	0	1	0	1	0	1	0	1

∴ b is divisible by 2 if b = 0, 2, 4, 6 or 8

∴ a is divisible by 2 if the last digit of a is 0, 2, 4, 6, 8

Modular Congruence: congruence

def: let $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$

a is congruent to b modulo m

$(a \equiv b \bmod m)$ if $m \mid (a-b)$

التاريخ: / /

الموضوع:

Corollary:

1) Congruence modulo m is an equivalence relation
2) $a \equiv b \bmod m$ iff $a \bmod m = b \bmod m$
3) $a \equiv b \bmod m$ iff there exists $k \in \mathbb{Z}$ such that $a = b + km$

Proof

1) $a \rho a$?

$m \mid a-a$

$a \equiv a \bmod m$

$\therefore a \rho a$ for any $a \in \mathbb{Z}$

$\therefore \rho$ is reflexive

2) Let $a \rho b$

$a \equiv b \bmod m$

$m \mid a-b$

$\frac{a-b}{m} = k \in \mathbb{Z}$

$\frac{b-a}{m} = -k \in \mathbb{Z}$

$m \mid b-a$

$\therefore b \equiv a \bmod m$

$\therefore b \rho a$

$\therefore a \rho b \rightarrow b \rho a$

$\therefore \rho$ is Symmetric

3) $a \rho b \wedge b \rho c \rightarrow a \rho c$

Let $a \rho b \wedge b \rho c$

$a \rho b$

$a \equiv b \bmod m \rightarrow m \mid a-b$

$b \equiv c \bmod m \rightarrow m \mid b-c$

هنا التفرقة بالإشارة

$m \mid a-c$

$\therefore a \equiv c \bmod m$

$\therefore a \rho c$

$\therefore$ transitive

$\therefore \rho$ is equivalence relation

equivalence class of a: $[a]_\rho = \{a + km \; , \; k \in \mathbb{Z}\}$.

$m \mid (a-x)$

$a - x = km$

$x = a - km$

Congruence relation

① If $a \equiv b \bmod m$ then $a+c \equiv b+c \bmod m$

② if $a \equiv b \bmod m$, $c \equiv d \bmod m$

$\therefore (a+c) \equiv (b+d) \bmod m$

& $ac \equiv bd \bmod m$

EX What is the remainder of $14+41+20+13+29$ when divided by 4

$14 \equiv 2 \bmod 4$

$41 \equiv 1 \bmod 4$

$20 \equiv 0 \bmod 4$

$13 \equiv 1 \bmod 4$

$29 \equiv 1 \bmod 4$

$(14+41+20+13+29) \equiv (2+1+0+1+1) \bmod 4$

$\equiv 1 \bmod 4$

∴ remainder = 1

EX What is the remainder of $17 \times (12 \times 19 + 5) - 23$ when divided by 3?

$17 \equiv 2 \bmod 3$

$12 \equiv 0 \bmod 3$

$19 \equiv 1 \bmod 3$

$5 \equiv 2 \bmod 3$

$-23 \equiv 1 \bmod 3$

$17 \times (12 \times 19 + 5) - 23 \equiv 2 * (0 * 1 + 2) + 1 \bmod 3$

$\equiv 5 \bmod 3$

∴ r = 2

ملاحظة: الـ remainder تأخذ القيم $\{-1, 0, 1\}$

من أقرب الأصغر

التاريخ: / /

المجموعة:

(Ex) What are the last two digits of the number 99^{99}

نقسم على 100.

$99 \equiv -1 \mod 100$.

$99 * 99 \equiv (-1 * -1) \mod 100$

$\underbrace{99 * 99 \cdots 99}_{99} \equiv \underbrace{(-1 * -1 * \cdots * -1)}_{99} \mod 100$

$99^{99} \equiv (-1)^{99} \mod 100 \equiv -1 \mod 100 \equiv 99 \mod 100$

$r = 99$

∴ last two digits = 99

(Ex) Is the number 3475 divisible by 3?

Number is divisible ← 0 → $r = 0$

Odd digits

$10^k \equiv 1 \pmod 3$ for all $k \in \mathbb{Z}$

(sol) $x = 3475$

$x = 3*10^3 + 4*10^2 + 7*10 + 5$

$3*10^3 \equiv (0*1*1) \mod 3$

$4*10^2 \equiv (1*1*1) \mod 3$

$7*10 \equiv (1*1) \mod 3$

$5 \equiv (2) \mod 3$

$x \equiv 4 \mod 3$

$\equiv 1 \mod 3$

$\therefore 3475 = 3q + 1$ ← remainder

3 ∤ 3475

In general $x = (a_3\ a_2\ a_1\ a_0)$

$x_1 = a_0 + 10 a_1 + 10^2 a_2 + 10^3 a_3$

$x = (a_0 + 1*a_1 + 1*1*a_2 + 1*1*1*a_3) \mod 3$

$x = (a_0 + a_1 + a_2 + a_3) \mod 3$

∴ قاعدة

Integer is ≡ sum of its digits (mod 3)

any numb ≡ its remainder (mod m)

الموضوع: Arithmetic Operations on Remainders التاريخ:

Modular Arithmetic modulo 2

العمليات تحفظ التطابق
كلوج مطابق لباقي قسمته على m.

+	0	1
0	0	1
1	1	0

−	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

ex) What is the remainder of $374 * (419 + 267 - 38)$ (-625) when divided by 2?

$\equiv (0 * (1+1 \times 0) - 1 \mod 2 \equiv 0(1) - 1 \mod 2$

$\equiv 0 - 1 \mod 2 = 1 \mod 2$ r=1

modulo 7:-

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

column ↓ x

ex) $3x \equiv 5 \mod 7$

x: column
a: row
b: target

$ax = b \pmod 7$

$x = \frac{b}{a} \pmod 7$ x=4

2 طريقة لحل المعادلة

$a - b = x \mod 7$

$a = (b + x) \mod 7$

$(5 - 2) \mod 7$

$5 \equiv (2 + x) \mod 7$

$(5 - 2) \mod 7$

$2 = (5 + x) \mod 7$

x=4

$3x \equiv 4 \pmod 6$

$x = 0$

التاريخ: / /

الموضوع:

modulo 6

x	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$3x \equiv 1 \pmod 6$

↳ has no sol.

لأن 1 مش موجود

التاريخ: / /

Primes & Composite

الموضوع:

Definition

2 is neither (Prime / Composite)

↳ an integer $p > 1$ is Prime if the only positive factor of p are $1, p$, otherwise ⟹ p is Composite

Ex which is Prime? → a) 4 (2|4) b) 17 c) 23 d) 27 (3|27)

Theorem if $n \in \mathbb{Z}^+$, then there is a unique increasing sequence of primes: $p_1, p_2, \dots, p_m$ such that $n = p_1 p_2 \dots p_m$

$p_1, p_2 \dots p_m$: prime factorization of n

Ex. find the prime factorization of n

sol (systematic)

$\frac{100}{2} = 50$

$\frac{50}{2} = 25$

$\frac{25}{2} \neq$ int

$\frac{25}{3} \neq$ int

$\frac{25}{5} = 5$

$\frac{5}{5} = 1$

∴ prime factorization: $100 = 2 * 2 * 5 * 5$

Theorem let $n \in \mathbb{Z}^+$

1) If $n = ab$ then the prime factorization of n is the result of merging the prime factorization of a, b

2) If p is a Prime, $p | n$, and $p_1, p_2, p_3 \dots p_m$ is the PF of n then ⟹ $p = p_i$ for some $1 \le i \le m$

لو P اولى ، ويقسم n ، هلاقيه في ال PF بتاع n.

Theorem

↳ If n is a Composite then n has a prime factor $\le \sqrt{n}$

proof كده نقدر نعمل check لحد ال root بدل من اني اعمل check على كل الموجود

Let $n = ab$ → $a | n$.

assume [by contradiction] → let $a > \sqrt{n}$, $b > \sqrt{n}$ ⟹ $ab > n$ contradiction

$\neg [a > \sqrt{n} \wedge b > \sqrt{n}]$

↳ $a \le \sqrt{n} \vee b \le \sqrt{n}$

assume W.L.O.G that $a \le \sqrt{n}$

- a is Prime: $a | n$, a is prime, we are done
- a is Composite → ∃ some prime p such that $p | a$, ∵ $a | n$ ∴ $p | n$ — $p \le a \le \sqrt{n}$ ✓

التاريخ: / / الموضوع:

Ex:- Determine whether $n = 307$ is Prime or not:

$\rightarrow \sqrt{n} = \sqrt{307} = 17.\ldots$

Primes $< \sqrt{n}$:- → 2, 3, 5, 7, 11, 13

$\frac{307}{2} \neq int$	$\frac{307}{7} \neq int$	$\frac{307}{17} \neq int$
$\frac{307}{3} \neq int$	$\frac{307}{11} \neq int$	∴ 307 is prime
$\frac{307}{5} \neq int$	$\frac{307}{13} \neq int$	

Theorem → There are infinitely many prime.

Proof assume [by contradiction] that they are finite number of primes

assume → Primes = $P_1, P_2, \ldots, P_m$

let $n = P_1 P_2 \ldots P_m$ Composite رقم كبير مضروب

$n' = P_1 P_2 \ldots P_m + 1$ → محاولة اقدر الصف بيه
إنه في Prime هو اكبر الرقم

n' Composite → ∴ there exist a prime P_i | n, P_i | $P_1 P_2 \ldots P_m$
for some i

لو استخدام النظرية هيقسم الفرق بتاعهم

$P_i \mid n - P_1, P_2, \ldots P_m$ ← يقسم ال linear combination

$P_i \mid 1$ → contradiction

→ our assumption is false

∴ there exists ∞ number of primes ;

$\Leftarrow$ prime ≠ 1

PF: prim factorizatn

التاريخ: / /

الموضوع: ممكن اثباتات في الماضرة جاي

PF Uniqueness proof

If $n \in \mathbb{Z}^+$ then $\exists$ a unique PF

proof assume there are 2 distinct PF for n

PF $p_1, p_2 \cdots p_k$

$q_1, q_2 \cdots q_m$

$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$

Dividing by Common elements of p_i, q_i

هنوصل ل primes اخرى ههنا شيل المتساوي منهم

$p_1' p_2' \cdots p_{k'}' = q_1' q_2' \cdots q_{n'}'$

$p_1' \mid$ LHS → = RHS

$p_1' \mid$ RHS

this mean $p_1' = q_j'$, for some $j' \in \{1, 2, \ldots m'\}$

Contradiction

∴ Wrong assumption

∴ PF is unique