# 1.1 Proof.

- def. a series of convincing arguments that leaves no doubt that a given provision is true
  ① language ✓ ② notation ✓ ③ logic ✓ ④ detail ✓
- universally quantified statements

$\forall s \in S$

for all / for any

the domain

$P(s) \to$ symbol for a statement $P$ that depends on the variable $s \in S$

$\exists s \in S \quad Q(s)$

there exists

# 1.2 Set

- def. a well defined, unordered collection of distinct objects
- empty set $\emptyset = \{\ \}$

$\mathbb{N} = \{1, 2, 3 \cdots\}$ 正整数

$\mathbb{Z}$ = all integers $\{\cdots, -1, 0, 1, 2 \cdots\}$

$\mathbb{Q} \to \frac{a}{b}\ (b \neq 0)$ rational numbers 有理数

$\mathbb{R}$ = real number

$\mathbb{C} \to$ complex number

$\forall \to$ 任何

$\exists \to$ 存在一个

# 1.3 Statement

$\boxed{\text{truth value of statement} \quad \text{判断statement正误}}$

- def. a sentence that has definite state of being either true or false

ex. $n \in \mathbb{N}$, $n^2+13$ isn't perfect square

X. $n=6$, $n^2+13=49=7^2$

"a counter example"

$m-7=5$ 不是 statement

∵对m无定义

# 1.4. Quantifiers

- a sentence that contains a variable, where the truth of the sentence is determined by the value of variable
- We can turn an open sentence into a statement by adding a quantifier
  - quantifier → $\forall$. $\exists$

ex. for all $x \in \mathbb{R}$. $x^2 - x \geq 0$

quantifier　variable　domain

↳ 可取任何一个数

**open sentence + 限制 = statement**

- $\neg(\exists x \in \mathbb{R}.\ \exists y \in \mathbb{R},\ \forall z \in \mathbb{N},\ xy = z) \equiv (\forall x \in \mathbb{R}\ \forall y \in \mathbb{R}\ \exists z \in \mathbb{N}\ \neg(xy = z))$

$\forall x \in \mathbb{Z}\ (x \geq 5 \Rightarrow 2^x > x^2)$

- Universal quantifier ($\forall$) (存在所有值)

ex. $\forall x \in \mathbb{R}$, $x^2 - x \geq 0$. ✗

- Existential Quantifier ($\exists$) (只存在个别值) → there exists / → for some

ex. 64 is perfect square → $\exists k \in \mathbb{Z}$, $64 = k^2$

- quantified statement

4部分: ① quantifier ($\forall$, $\exists$) ② variable ③ domain ④ open sentence → for every variable

universally quantified statement $\forall x \in S, P(x)$

existentially quantified statement $\exists x \in S, P(x)$

- Negating Universal quantifier ($\neg\forall$)

$\neg(\forall x \in S, P(x)) \equiv \exists x \in S, \neg P(x)$

$\neg(\exists x \in S, P(x)) \equiv \forall x \in S, \neg P(x)$

ex. negate $\forall x \in \mathbb{R}$, $|x| < 5$. → given $\exists x \in \mathbb{R}$, $|x| \geq 5$. False

- Negating Existential Quantifier ($\neg\exists$)

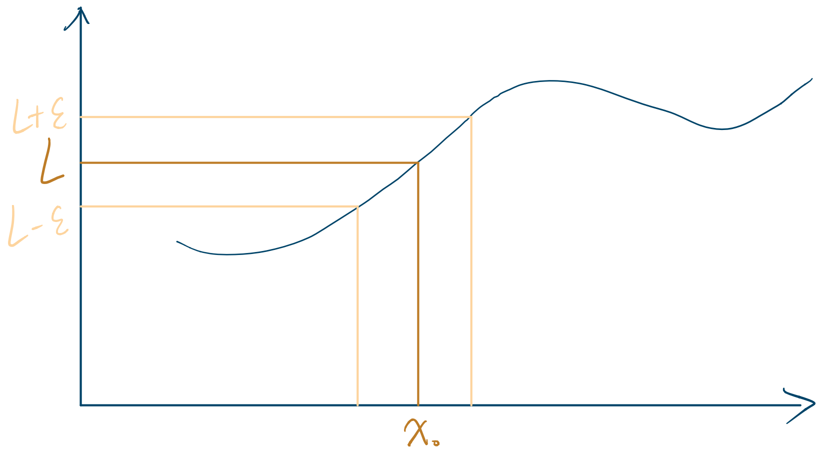
ex. negate $\exists x \in \mathbb{R}$, $|x| < 5$ → given $\forall x \in \mathbb{R}$, $|x| \geq 5$. True

$\neg(\exists x \in S, f(x)) \equiv \forall x \in S, \neg P(x)$

# 1.5 Nested quantifier (多于1个 quantifier)

- ① $\forall s \in \mathbb{R},\ \exists t \in \mathbb{R},\ s > t$
  ② $\exists t \in \mathbb{R},\ \forall s \in \mathbb{R},\ s > t$

  different




$$\forall \varepsilon > 0 \quad \exists \delta > 0 \quad \forall x \ \left( |x - x_0| < \delta \Rightarrow |f(x) - L| < \varepsilon \right)$$

$$(\forall \varepsilon > 0)\ (\exists \delta > 0)\ (\forall x \in \operatorname{dom} f)\ \left( |x - x_0| < \delta \Rightarrow |f(x) - L| < \varepsilon \right)$$

# 2.1 Truth Tables & Negation

- negation of statement "¬" asserts the exact opposite

eg. statement $\neg(5<8)$
negation is $5 \geq 8$

- double negation (negation "¬")

$\neg(\neg A)$ is the same as $A$.

$\neg(\neg A) \equiv A$ logically equivalent

# 2.2 Conjunction & Disjunction

- Conjunction (= and) 符号: ∧ 需同时满足

| $A$ | $B$ | $A \land B$ | $\neg(A \land B)$ |
|---|---|---|---|
| T | T | T | F |
| T | F | F | T |
| F | T | F | T |
| F | F | F | T |

| $\neg A$ | $\neg B$ | $(\neg A) \lor (\neg B)$ |
|---|---|---|
| F | F | F |
| F | T | F |
| T | F | F |
| T | T | T |

Disjunction (= or) 符号: ∨ 满足其中一个即可

| $A$ | $B$ | $A \lor B$ | $\neg(A \lor B)$ |
|---|---|---|---|
| T | T | T | F |
| T | F | T | F |
| F | T | T | F |
| F | F | F | T |

| $\neg A$ | $\neg B$ | $(\neg A) \land (\neg B)$ |
|---|---|---|
| F | F | T |
| F | T | T |
| T | F | T |
| T | T | F |

**Commutative Laws**:

- $A \land B \equiv B \land A$
- $A \lor B \equiv B \lor A$

**Associative Laws**:

- $A \land (B \land C) \equiv (A \land B) \land C$
- $A \lor (B \lor C) \equiv (A \lor B) \lor C$

**Distributive Laws**:

- $A \land (B \lor C) \equiv (A \land B) \lor (A \land C)$
- $A \lor (B \land C) \equiv (A \lor B) \land (A \lor C)$

# 2.3 DML

- De Morgan's Laws (DML)

1. $\neg(A \land B) \equiv (\neg A) \lor (\neg B)$
2. $\neg(A \lor B) \equiv (\neg A) \land (\neg B)$

- Distributive laws

Prove: $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$

| $A$ | $B$ | $C$ | $B \vee C$ | $A \wedge (B \vee C)$ | $A \wedge B$ | $A \wedge C$ | $(A \wedge B) \vee (A \wedge C)$ |
|---|---|---|---|---|---|---|---|
| T | T | T | T | T | T | T | T |
| T | T | F | T | T | T | F | T |
| T | F | T | T | T | F | T | T |
| T | F | F | F | F | F | F | F |
| F | T | T | T | F | F | F | F |
| F | T | F | T | F | F | F | F |
| F | F | T | T | F | F | F | F |
| F | F | F | F | F | F | F | F |

## 2.4 Implication

- Implication = if … then …  符号: $\Rightarrow$

| $A$ | $B$ | $A \Rightarrow B$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

($A$ implies $B$)

$A$: hypothesis  $B$: conclusion

- Negation of an implication law

$A \Rightarrow B \equiv \neg A \vee B$  $\neg(A \Rightarrow B) \equiv A \wedge \neg B$

Prove $A \Rightarrow B \equiv \neg A \vee B$:

$$
\begin{aligned}
A \Rightarrow B &\equiv \neg(\neg(A \Rightarrow B)) && \text{double negation rule} \\
&\equiv \neg(A \wedge \neg B) && \text{negation of implication law} \\
&\equiv \neg A \vee \neg(\neg B) && \text{De Morgan's law} \\
&\equiv \neg A \vee B && \text{double negation}
\end{aligned}
$$

## 2.5 Converse and Contrapositive

- def. implication $B \Rightarrow A$ is the converse of $A \Rightarrow B$

| $A$ | $B$ | $A \implies B$ | $B \implies A$ |
|---|---|---|---|
| T | T | T | T |
| T | F | F | T |
| F | T | T | F |
| F | F | T | T |

$A \Rightarrow B \equiv ((\neg B) \Rightarrow (\neg A))$

contrapositive

- def. implication $\neg B \Rightarrow \neg A$ is the contrapositive of $A \Rightarrow B$

Prove $A \Rightarrow B \equiv \neg B \Rightarrow \neg A$

$$
\begin{aligned}
A \Rightarrow B &\equiv \neg(\neg(A \Rightarrow B)) && \text{double neg} \\
&\equiv \neg(A \vee (\neg B)) && \text{neg of implication} \\
&\equiv \neg(B \wedge (\neg A)) && \text{commutativity} \\
&\equiv \neg((\neg B) \wedge \neg(\neg A)) && \text{DML} \\
&\equiv \neg(\neg((\neg B) \Rightarrow (\neg A))) && \text{neg implication} \\
&\equiv \neg B \Rightarrow \neg A && \text{double negation}
\end{aligned}
$$

- Prove $(\neg(P \Rightarrow \neg Q)) \not\equiv (\neg P \Rightarrow Q)$

If we choose the state of P to True and that of Q to be false, then we get
$\neg(P \Rightarrow \neg Q)$ is F.
$\neg P \Rightarrow Q$ is T. This establish that the 2 statements are not equivalent

- Prove $(A \vee \neg B) \Rightarrow \neg C \equiv \neg(C \wedge A) \wedge (\neg C \vee B)$

$$
\begin{aligned}
(A \vee \neg B) \Rightarrow \neg C &\equiv \neg(\neg((A \vee \neg B) \Rightarrow \neg C)) && \text{double} \\
&\equiv \neg((A \vee \neg B) \wedge \neg(\neg C)) && \text{negation of implication} \\
&\equiv \neg(A \vee \neg B) \vee \neg C && \text{DML} \\
&\equiv (\neg A \wedge B) \vee \neg C && \text{DML} \\
&\equiv (\neg A \vee \neg C) \wedge (B \vee \neg C) && \text{distributive Law} \\
&\equiv (\neg C \vee \neg A) \wedge (\neg C \vee B) && \text{Commutativity} \\
&\equiv \neg(C \wedge A) \wedge (\neg C \vee B) && \text{DML}
\end{aligned}
$$

- $(A \wedge B) \Rightarrow C \equiv (A \Rightarrow C) \wedge (B \Rightarrow C)$

## 2.6 If and Only if $(A \Leftrightarrow B)$

| $A$ | $B$ | $A \iff B$ | $A \implies B$ | $B \implies A$ | $(A \implies B) \wedge (B \implies A)$ |
|---|---|---|---|---|---|
| $T$ | $T$ | $T$ | $T$ | $T$ | $T$ |
| $T$ | $F$ | $F$ | $F$ | $T$ | $F$ |
| $F$ | $T$ | $F$ | $T$ | $F$ | $F$ |
| $F$ | $F$ | $T$ | $T$ | $T$ | $T$ |

Useful Tool Logical

De Morgan's Laws (DML)

- $\neg(A \vee B) \equiv \neg A \wedge \neg B$.
- $\neg(A \wedge B) \equiv \neg A \vee \neg B$.

Commutative Laws

- $A \vee B \equiv B \vee A$.
- $A \wedge B \equiv B \wedge A$.

Associative Laws

- $A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$.
- $A \vee (B \vee C) \equiv (A \vee B) \vee C$.

Distributive Laws

- $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$.
- $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$.

Some more properities

- $A \Rightarrow B \equiv \neg A \vee B$ negation of implication
- $A \vee \neg A \equiv T$
- $A \wedge \neg A \equiv F$

# 3.1 Proving universally quantified statements

arbitrary 任意的

## - Types of statement

hypothesis 假设 : ( no evidence )

proposition 命题 : mathematical claim . 陈述. 需有效论证 证明 T/F

theorem 定理 : a significant proposition

lemma 引理 : "辅助"命题

corollary 推论 : 由定理推得

contrapositive 对照

conjecture 猜想

Implication 的常见结构

$$\forall x \in D_1, \forall y \in D_2 \ \cdots, [P(x, y, \cdots) \Rightarrow Q(x, y, \cdots)]$$

没有 Variables 的时候, $A \Rightarrow B$, e.g., if tomorrow is raining, I am going to SavvyUni for Math137.

if ( Hypothesis ), then ( Conclusion )

- Hypothesis $P(x, y, \cdots)$
- Conclusion $Q(x, y, \cdots)$
- Converse If $Q(x, y, \cdots)$, then $P(x, y, \cdots)$
- Inverse If $\neg P(x, y, \cdots)$, then $\neg Q(x, y, \cdots)$
- Contra-positive If $\neg Q(x, y, \cdots)$, then $\neg P(x, y, \cdots)$
- Negation $P(x, y, \cdots) \wedge \neg Q(x, y, \cdots)$

Let $x, y \in \mathbb{Z}$. $\underbrace{\text{If } x \text{ is even } y \text{ is odd}}_{\text{hypothesis}}$, $\underbrace{\text{then } x+y \text{ is odd}}_{\text{conclusion}}$

converse : If $x+y$ is odd, then $x$ is even and $y$ is odd.

contrapositive : If $x+y$ is not odd, then $x$ is not even or $y$ is not odd

ex. There is a smallest natural number

$\exists n \in \mathbb{N} \quad \forall m \in \mathbb{N} \quad n \leq m$

- ✪ Do not assume what u trying to proof 结论不得作为假设

✪ Sometimes it's easier to break up the domain.

ex. let $x \in \mathbb{R}$ prove $|x-3| + 2|x+2| \geq 5$

✪ 注意 extraneous solution 证完将值带入题中验证

ex. $\log x$ ($x$ 应 $>0$) 若 prove 出 $x<0$ 的结果, 应 ignore

## - Disproving universally quantified statements

use counter example

proof
- … true 直接证
- … false 证 $\neg(\cdots)$ true

- method

Proof: $\forall s \in S.\ P(s)$ Let $s \in S$ be arbitrary

## 3.2 Proving existentially quantified statements

- method

Proof: $\exists s \in S.\ P(s)$ 找一个例子

## 3.3. Proving implications

- Proof: $P \Rightarrow Q$ Assume $P$ is true,
use this assumption to show $Q$ is true.

- Proof: $P \Leftrightarrow Q$ 要同时证明 "$\Rightarrow$" 与 "$\Leftarrow$"

ex. Proof $m \in \mathbb{Z}$ is even if and only if ($\Leftrightarrow$) $7m^2+4$ is even

($\Rightarrow$) If $m$ is even, $m=2k$ (for some $k \in \mathbb{Z}$)
then $7m^2+4 = 7\times(2k)^2+4 = 2\times(14k^2+2)$, which is an even integer.

($\Leftarrow$) Conversely, assume $7m^2+4$ is even, and assume $m$ is odd,
then, $7m^2$ is also odd. $7m^2+4$ is odd, which contradicts assumption.

## 3.4 Divisibility of integers

- $n = k \cdot m$

能整除 $m$ is a divisor / factor of $n$ $m \mid n$
$n$ is a multiple of $m$

不能整除 写作 $m \nmid n$ $0 \mid 0$ ✓

- transitivity of divisibility (TD)

$\forall a.b.c \in \mathbb{Z}$, if $a|b$ & $b|c$, then $a|c$

Proof: Let $a.b.c \in \mathbb{Z}$ be arbitrary.

Now $b|c$ means $c=kb$ for some $k \in \mathbb{Z}$
$a|b$ means $b=ma$ for some $m \in \mathbb{Z}$

Then $c=kb=(k.m)a$. Hence $a|c$ since $km \in \mathbb{Z}$

$\forall a.b.c \in \mathbb{Z}$. If $a|b$ or $a|c$, then $a|bc$

$(A \vee B \Rightarrow C) \equiv ((A \Rightarrow C) \wedge (B \Rightarrow C))$

- divisibility of integer combinations (DIC)

$\forall a.b.c \in \mathbb{Z}$, if $a|b$ & $a|c$, then $\forall x.y \in \mathbb{Z}$, $a|(bx+cy)$

Proof. Let $a.b.c \in \mathbb{Z}$, and assume $a|b$ and $a|c$.

$am=b$ & $ak=c$ given any $x.y \in \mathbb{Z}$. We have $(bx+cy) = a(xm+yk)$

Hence $a|(bx+cy)$.

- converse of DIC

$\forall a.b.c \in \mathbb{Z}$. if $a|(bx+cy)$ for all integer $x$ & $y$, then $a|b$ & $a|c$

Proof. Let $a.b.c \in \mathbb{Z}$

Assume $a|(bx+cy)$ $\forall x.y \in \mathbb{Z}$

Then this must be true when $x=1$. $y=0$ So $a|(b\cdot 1+c\cdot 0)$ $\therefore a|b$

Also, this is true when $x=0$ $y=1$. So $a|(b\cdot 0+c\cdot 1)$ $\therefore a|c$

Therefore $a|b$. and $a|c$

ex. Proof. For all $a.b.c \in \mathbb{Z}$, if $a|(b+c)$ and $a|(3b+c)$, then $a|b$ and $a|c$ is wrong

Let $a.b.c \in \mathbb{Z}$. Assume that $a|(b+c)$ and $a|(3b+c)$

$\because$ DIC. $\therefore a|x(b+c)+y(3b+c)$ for any $x.y \in \mathbb{Z}$

Take $x=-1$, $y=1$, we get $a|-(b+c)+(3b+c) \Rightarrow a|2b$

Take $x=-3$. $y=1$ we get $a|-2c$.

# 3.5 Proof by Contrapositive

- 若证 $A \Rightarrow B$, replace with " $(\neg B) \Rightarrow (\neg A)$

assume $\neg B$ true, $\neg A$ also true.

证明 $(\neg B) \Rightarrow (\neg A)$ true
↓
得 $A \Rightarrow B$ true

ex. $\forall x \in \mathbb{R}$. $x^2-7x+10 \geq 0 \Rightarrow x \leq 3$ or $x \geq 4$

Prove by contrapositive: $3 < x < 4 \Rightarrow x^2-7x+10 < 0$

$$x^2-7x+10 = (x-2)(x-5)$$

$\because x > 3 \quad x-3 > 0 \quad \therefore x-2 = (x-3)+1 > 0$
$\because x < 4 \quad x-4 < 0 \quad \therefore x-5 = (x-4)-1 < 0$

Since the contrapositive is true, the original implication is true. QED

# 3.6 Proof by Contradiction 反证法

$A$ is statement. $A$ 与 $\neg A$ 必有一个错误

$A \wedge (\neg A)$ always false. " $A \wedge (\neg A)$ is true" is contradiction

ex. Prove $\sqrt{2}$ is irrational

证 $\neg A$ false
↓
得 $A$ true

Prove by contradiction: Suppose $\sqrt{2} \in \mathbb{Q}$.
We have $\sqrt{2} = \frac{a}{b}$ ($a, b \in \mathbb{Z}$, $b \neq 0$, $a, b$ 互质)

$2 = \frac{a^2}{b^2} \quad a^2 = 2b^2 \rightarrow a$ is even. let $a = 2k$

$4k^2 = 2b^2 \quad b^2 = 2k^2 \rightarrow b$ is also even.

$a$ & $b$ both even contradicts to $a, b$ relatively prime

The contradiction is false. So, the statement is true.

- $A \Rightarrow B \equiv \neg A \vee B$ negation of implication

## 3.7 Proof "If & Only if" Statement

- $A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$

ex. Let $n \in \mathbb{Z}$, prove $2 \mid (n^4 - 3)$ if and only if $4 \mid (n^2+3)$ 证 $A \Leftrightarrow B$ true

需证 $A \Rightarrow B$ true. $B \Rightarrow A$ true

Prove:

($\Rightarrow$) ① If $n = 2k$ for some $k$ (i.e. $n$ is even), then $n^4 - 3 = 16k^4 - 3$ which is odd

$2 \mid (n^4-3)$ is always false, $2 \mid (n^4-3) \Rightarrow 4 \mid (n^2+3)$ is true

② If $n = 2k+1$ for some $k$, then $n^4 - 3 = 16k^4 + 32k^3 + 24k^2 + 8k - 2$

$n^2 + 3 = 4k^2 + 4k + 4 = 4(k^2+k+1)$ divisible by 4.

($\Leftarrow$) Conversely, if $4 \mid (n^2+3)$, we can't have $n$ to be even (otherwise we get $n^2+3$ is odd, and hence $4 \nmid (n^2+3)$)

- Prove or disprove

① if $2 \nmid xy$, then $2 \nmid x$ & $2 \nmid y$ True

② if $2 \nmid y$ and $2 \nmid x$ then $2 \nmid xy$.

contradiction. $2 \mid xy \Rightarrow 2 \mid y$ or $2 \mid x$

☆ If for all ..., then ... 仅需要举一个正确例子.

## Proof by elimination

$A \Rightarrow (B \vee C) \equiv (A \wedge \neg B) \Rightarrow C$

$\equiv (A \wedge \neg C) \Rightarrow B$

# 4.1 Notations

## - Proving uniqueness

ex. prove that for any odd $n \in \mathbb{Z}$, there exists a unique $m \in \mathbb{Z}$ s.t $n^2 = 8m+1$

proof. Let $n = 2k+1$ be and odd integer, where $k \in \mathbb{Z}$.

Then $n^2 = (2k+1)^2 = 4k^2+4k+1 = 8 \times \frac{k(k+1)}{2} + 1$

Either $k$ or $k+1$ is even integer, $\frac{k(k+1)}{2} \in \mathbb{Z}$.

# 4.2 Proof by Mathematical Induction

POMI

## - POMI

Let $P(n)$ be a statement depending on $n$.

If $P(1)$ is true
$\forall k \in \mathbb{N}$. $P(k) \Rightarrow P(k+1)$ } inductive step.

Then $\forall n \in \mathbb{N}$, $P(n)$ is true

ex. proof $n \in \mathbb{N}$, $n \geq 5$. $2^n > n^2$

proof. we proceed by induction on $n$.

Base case : At $n=5$, we have $2^n = 2^5 = 32$, and $n^2 = 5^2 = 25$

Inductive Step: Let $k \geq 5$. $(k \in \mathbb{N})$. The statement holds at $k$. $\rightarrow 2^k > k^2$.

Assume induction hypothesis : $2^{k+1} > (k+1)^2$.

$2^{k+1} = 2 \times 2^k > 2k^2$
$\phantom{2^{k+1} = 2 \times 2^k > } \ \| $
$\phantom{2^{k+1} = 2 \times 2^k > } k^2+k^2$

*Lemma : $\forall m \in \mathbb{N}$, if $m \geq 3$ then $m^2 \geq 2m+1$

proof: Base case : At $m=3$, we have $m^2 = 9 > 7 = 2m+1$

Inductive step: Let $m \geq 3$ be arbitrary. Assume $m^2 \geq 2m+1$, then.

$(m+1)^2 = m^2+2m+1 \geq (2m+1)+(2m+1) > 2(m+1)+1$.

By POMI. the statement is true for all $m \geq 3$

ex.

[6] 5. Use induction to prove that for every integer $n \geq 7$,

$$\sum_{i=7}^{n} i = \frac{n(n+1)}{2} - 21$$

*Proof.* We begin by formally writing out our inductive statement

$$P(n): \sum_{i=7}^{n} i = \frac{n(n+1)}{2} - 21$$

**Base Case** We verify that $P(7)$ is true where $P(7)$ is the statement

证第一项 true.

$$P(7): \sum_{i=7}^{7} i = \frac{7(7+1)}{2} - 21$$

The left hand side evaluates to $\sum_{i=7}^{7} i = 7$ and the right hand side evaluates to $\frac{7(7+1)}{2} - 21 = 28 - 21 = 7$ so $P(7)$ holds.

**Inductive Hypothesis** We assume that the statement

Assume P(k) true

$$P(k): \sum_{i=7}^{k} i = \frac{k(k+1)}{2} - 21$$

is true for some integer $k \geq 7$.

**Inductive Conclusion** Now we show that the statement $P(k+1)$ is true. That is, we show

证 P(k+1) true

$$P(k+1): \sum_{i=7}^{k+1} i = \frac{(k+1)(k+2)}{2} - 21$$

Now

$$\begin{aligned}
\sum_{i=7}^{n} i &= \left[\sum_{i=7}^{k} i\right] + [k+1] && \text{(partition into } P(k) \text{ and other)} \\
&= \left[\frac{k(k+1)}{2} - 21\right] + [k+1] && \text{(Inductive Hypothesis)} \\
&= \frac{k(k+1) + 2(k+1)}{2} - 21 && \text{(arithmetic)} \\
&= \frac{(k+1)(k+2)}{2} - 21 && \text{(factor)}
\end{aligned}$$

The result is true for $n = k+1$, and so holds for all $n$ by the Principle of Mathematical Induction.

□

# 4.3 Binomial Theorem

## – Summations

① $\sum_{i=m}^{n} x_i = x_m + x_{m+1} + \cdots + x_n$

② $\sum_{i=1}^{m} cx_i = c\sum_{i=1}^{m} x_i$

③ $\sum_{i=1}^{m} (x_i + y_i) = \sum_{i=1}^{m} x_i + \sum_{i=1}^{m} y_i$

## – Products

$$\prod_{i=1}^{n} x_i = x_1 x_2 \cdots x_n$$

ex. 证 $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(n+2)}{6}$

Prove by induction

Base case: $n=1$. $\sum_{i=1}^{1} i^2 = \frac{1\times2\times3}{6} = 1$ ✓

Induction: Assume $\sum_{i=1}^{k} i^2 = \frac{k(k+1)(k+2)}{6}$ for some $k \geq 1$ $(k \in \mathbb{Z})$

$$\sum_{i=1}^{k+1} i^2 = (k+1)^2 + \sum_{i=1}^{k} i^2$$

$$= (k+1)^2 + \frac{k(k+1)(k+2)}{6}$$

$$= (k+1)\left(\frac{6(k+1)+k(2k+1)}{6}\right)$$

$$= \frac{k+1}{6}(2k^2+7k+6)$$

$$= \frac{k+1}{6} \times (2k+3)(k+2)$$

$$= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}$$

## – *Binomial series*

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{r}a^{n-r}b^r + \ldots + b^n \qquad (n \in \mathbb{N})$$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

"n choose k"

where $\binom{n}{r} = {}^{n}C_r = \frac{n!}{r!(n-r)!}$

$$(1+x)^n = 1 + nx + \frac{n(n-1)}{1\times2}x^2 + \ldots + \frac{n(n-1)\ldots(n-r+1)}{1\times2\times\ldots\times r}x^r + \ldots (|x|<1,\ n \in \mathbb{R})$$

## - Pascal's Identity

For all positive $n, m \in \mathbb{Z}$. $m < n$. $\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$

$$
\begin{aligned}
\binom{n-1}{m-1} + \binom{n-1}{m} &= \frac{(n-1)!}{(n-m)!\,(m-1)!} + \frac{(n-1)!}{(n-m-1)!\,m!} \\
&= \frac{(n-1)!\,m + (n-1)!\,(n-m)}{(n-m)!\,m!} \\
&= \frac{(n-1)!\,n}{(n-m)!\,m!} \\
&= \frac{n!}{(n-m)!\,m!} \\
&= \binom{n}{m}
\end{aligned}
$$

## - Binomial Theorem 1

For all integers $n \geq 0$ and all real number $x$. $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^k$

Proof. We proceed by induction on $n$.

Base case: At $n=1$, $(a+b)^1 = a+b = \binom{0}{1} a^1 b^0 + \binom{1}{1} a^0 b^1 = \sum_{k=0}^{1} \binom{k}{1} a^{1-k} b^k$

Inductive step: Assume the statement holds at $n \geq 0$ and let us use this to prove it holds at $n+1$

$$
\begin{aligned}
(1+x)^{n+1} &= (1+x)(1+x)^n = (1+x)\sum_{k=0}^{n}\binom{n}{k}x^k \\
&= \sum_{k=0}^{n}\binom{n}{k}x^k + x\sum_{k=0}^{n}\binom{n}{k}x^k \\
&= \sum_{k=0}^{n}\binom{n}{k}x^k + \sum_{k=0}^{n}\binom{n}{k}x^{k+1} \qquad \text{let } k+1=j \quad k=j-1 \\
\Rightarrow &= \sum_{k=0}^{n}\binom{n}{k}x^k + \sum_{j=1}^{n+1}\binom{n}{j-1}x^j \\
&= \binom{n}{0}x^0 + \sum_{k=1}^{n}\binom{n}{k}x^k + \sum_{j=1}^{n}\binom{n}{j-1}x^j + \binom{n}{n}x^{n+1} \qquad \text{let } j=k \\
\Rightarrow &= \binom{n}{0}x^0 + \sum_{k=1}^{n}\binom{n}{k}x^k + \sum_{k=1}^{n}\binom{n}{k-1}x^k + \binom{n}{n}x^{n+1} \\
&= \binom{n}{0}x^0 + \sum_{k=1}^{n}\left[\binom{n}{k}+\binom{n}{k-1}\right]x^k + \binom{n}{n}x^{n+1}
\end{aligned}
$$

By Pascal's Identity

$$
\begin{aligned}
&= \binom{n}{0}x^0 + \sum_{k=1}^{n}\binom{n+1}{k}x^k + \binom{n}{n}x^{n+1} \\
&= \binom{n+1}{0}x^0 + \sum_{k=1}^{n}\binom{n+1}{k}x^k + \binom{n+1}{n+1}x^{n+1} \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}x^k
\end{aligned}
$$

POMI. (principal of mathematical induction) $P(a) \Rightarrow P(a+1)$

## – Binomial Theorem 2

For any $a, b \in \mathbb{R}$, and any non-negative $n \in \mathbb{Z}$.

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Proof: case 1 $(a=0)$:

$$(a+b)^n = b^n, \quad \text{and} \quad \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \binom{n}{0} \times 1 \times b^n = b^n$$

case 2 $(a \neq 0)$:

$$(a+b)^n = a^n \left(1+\frac{b}{a}\right)^n = a^n \sum_{k=0}^{n} \binom{n}{k} \left(\frac{b}{a}\right)^k$$

$$= \sum_{k=0}^{n} \binom{n}{k} a^n \frac{b^k}{a^k}$$

$$= \sum_{k=0}^{n} \binom{n}{k} b^k a^{n-k}$$

$$= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

# 4.4 Principle of Strong Induction POSI

– If $\begin{cases} P(1) \text{ is true} \\ \text{For an arbitrary } k \geq 0, \quad P(1) \wedge P(2) \wedge \cdots \wedge P(k) \Rightarrow P(k+1) \end{cases}$

Then $P(n)$ is true for any $n$.

## – Prove by Strong induction

① 写 base case (后面需要几个写几个)

② IS. Assume $P(x)$ is true for $x = 1, 2, \ldots, k$ ← 需要的值

Then $P(x+1)$ ....

ex. Suppose $x_1 = 3$ $x_2 = 5$ ... $x_n = 3x_{n-1} + 2x_{n-2}$ for $n \geq 3$.

Prove $x_n < 4^n$ for all positive integers $n$.

Proof: By induction on $n$.

Let $P(n)$ be the open sentence. $x_n < 4^n$

Base case : Prove $P(1)$ and $P(2)$

$x_1 = 3$ and $4^1 = 4$. So $x_1 < 4^1$ . $P(1)$ is true
$x_2 = 5$ and $4^2 = 16$. So $x_2 < 4^2$ . $P(2)$ is true

Inductive Step : Let $k$ be an arbitrary natural number

Assume $P(i)$ is true for all integers $i$ , $1 \le i \le k$
$\Rightarrow x_i < 4^i$ for $i = 1, 2, \cdots k$

Let's prove $P(k+1)$ $x_{k+1} < 4^{k+1}$.

By recursive definition,

$$\begin{aligned} x_{k+1} = 3x_k + 2x_{k-1} &< 3 \times 4^k + 2 \times 4^{k-1} \\ &= 4^{k-1}(3 \times 4 + 2) \\ &= 14 \cdot 4^{k-1} < 16 \times 4^{k-1} \\ &= 4^{k+1}. \end{aligned}$$

$\therefore P(k+1)$ is true , so $P(n)$ is true for all $n \in \mathbb{N}$. by POSI

## 一 二进制

$$\underbrace{13}_{\downarrow\ 1101} = 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$$

Prove every positive integer $n$ can be expressed as a sum of distinct non-negative powers of 2

Base Case : At $n=1$ , we have $1 = 2^0$. which establishes the result in this case

Inductive Step : Let $k \ge 1$ be arbitrary, and assume the statement holds for all numbers $\le k-1$

Case 1 : $k$ is odd . $k-1$ is even , $2^0$ is not present in this sum.

$k-1 = \alpha_t 2^t + \alpha_{t-1} 2^{t-1} + \cdots + \alpha 2^1$  $\alpha_i \in \{0, 1\}$. for all $1 \le i \le t$  $t \in \mathbb{N}$.

$k = \alpha_t 2^t + \alpha_{t-1} 2^{t-1} + \cdots + \alpha 2^1 + 2^0$.

Case 2 : $k$ is even.

By induction hypothesis $\frac{k}{2}$ can be written as a sum of distict non-negative power of 2 ex

[6] 6. Let the sequence $\{x_i\}$ be defined by

- $x_0 = 3$, $x_1 = 2$, and
- $x_n = 3x_{n-1} - 2x_{n-2}$.

Prove that $x_n = 4 - 2^n$ for all integers $n \geq 0$.

*Proof.* We will use Strong Induction. Our statement $P(n)$ is

$$P(n) : x_n = 4 - 2^n$$

**Base Case** We verify that $P(0)$ and $P(1)$ are true.

$$P(0) : x_0 = 4 - 2^0$$

From the definition of the sequence $x_0 = 3$. The right side of the statement $P(0)$ evaluates to 3 so $P(0)$ is true.

$$P(1) : x_1 = 4 - 2^1$$

From the definition of the sequence $x_1 = 2$. The right side of the statement $P(1)$ evaluates to 2 so $P(1)$ is true.

**Inductive Hypothesis** We assume that the statement $P(i)$ is true for $1 \leq i \leq k$, $k \geq 1$.

$$P(i) : x_i = 4 - 2^i$$

**Inductive Conclusion** Now we show that the statement $P(k+1)$ is true.

$$P(k+1) : x_{k+1} = 4 - 2^{k+1}$$

$$\begin{aligned}
x_{k+1} &= 3x_k - 2x_{k-1} && \text{(by the definition of the sequence)} \\
&= 3 \cdot (4 - 2^k) - 2 \cdot (4 - 2^{k-1}) && \text{(by the Inductive Hypothesis)} \\
&= 12 - 3 \cdot 2^k - 8 + 2^k && \text{(expand)} \\
&= 4 - 2 \cdot 2^k \\
&= 4 - 2^{k+1}
\end{aligned}$$

The result is true for $n = k+1$, and so holds for all $n$ by the Principle of Strong Induction.

$\square$

## 5.1 Introduction of Sets

$\emptyset$ 空集

$\{\emptyset\}$ a set with only element is $\emptyset$

$|S|$ 指 S 里有多少项

ex. $A = \{1, 2, 3, 4\}$ $\quad |A| = 4$

$\therefore |\emptyset| = 0 \qquad |\{\emptyset\}| = 1$

## 5.2 Set-builder Notation

### - Set-builder Notation Type 1

$$S = \{x \in \mathcal{U} : P(x)\}$$

all element $\quad$ from universe 全集 $\quad$ such that $\quad$ every element follows $P(x)$

ex. $\{n \in \mathbb{N} : n \mid 12\} = \{1, 2, 3, 4, 6, 12\}$

$\{n \in \mathbb{Z} : 2 \mid n\}$ → 所有偶数的集合

### - Set-builder Notation Type 2

$$S = \{f(x) : x \in \mathcal{U}\}$$

指 S 为 $f(x)$ 里的每一个项，且 $x$ 存在于集合 $\mathcal{U}$ 中

ex. $\{2k : k \in \mathbb{Z}\}$ → 所有偶数的集合

### - Set-builder Notation Type 3

$$S = \{f(x) : x \in \mathcal{U}, P(x)\}$$

指 S 为 $f(x)$ 里的每一个项，且 $x$ 存在于集合 $\mathcal{U}$ 中，$P(x)$ 是对的

# 5.3 Set Operations

交集 union $S \cup T = \{x \in \mathcal{U} : x \in S \vee x \in T\}$

并集 intersection $S \cap T = \{x \in \mathcal{U} : x \in S \wedge x \in T\}$

差集 set-difference $S - T = \{x \in \mathcal{U} : x \in S \wedge x \notin T\}$

补集 complement $\overline{S} = \{x \in \mathcal{U} : x \notin S\}$

子集 subset $S \subseteq T$

Let $\mathcal{U} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $C = \{3, 5, 7, 10\}$, and $D = \{1, 3, 6, 7, 8\}$.

Calculate

ex.

1. $C \cup D = \{1, 3, 5, 6, 7, 8, 10\}$
2. $C \cap D = \{3, 7\}$.
3. $C - D = \{5, 10\}$.
4. $D - C = \{1, 6, 8\}$
5. $\bar{C} = \{1, 2, 4, 6, 8, 9\}$
6. $\{x \in \mathcal{U} : (x \in D) \implies (x \in C)\} = \{2, 3, 4, 5, 7, 9, 10\}$.
7. $|D - C| = 3$

# 5.4 Subsets of a set

## - def. subsets

$S$ is a subset of set $T$, 写作 $S \subseteq T$.

$\equiv$ $T$ is a superset of $S$

$S$ is a proper subset of set $T$. 写作 $S \subsetneq T$

$\equiv$ 满足 subset. 但 $S \neq T$

ex. $A$ & $B$ are sets. Prove $A - (A - B) \subseteq A \cap B$

Let $x \in \mathcal{U}$.

Assume $x \in A - (A - B)$ So $x \in A \wedge x \notin (A - B)$

$\equiv x \in A \wedge (\neg x \in (A - B))$

$\equiv x \in A \wedge (\neg (x \in A \wedge x \notin B))$

$\equiv x \in A \wedge (x \notin A \vee x \in B)$

Since $x \in A$ is true. $x \notin A$ is false. $x \in B$ is true

Thus $x \in (A \wedge B)$ $A - (A - B) \subseteq A \cap B$

## - def. Set equality.

We say two sets $S$ & $T$ are equal. 写作 $S = T$. 相同元素

## 6.1 The division algorithm

### - Bounds by divisibility (BBD)

Proposition $\forall x \in \mathbb{R}.\quad x \le |x| \quad (*)$

For all integers a & b, if $b|a$ and $a \neq 0$, then $b \le |a|$

proof: Let a & b be any integers. Assume $a \neq 0$ and $b|a$.

Then $a = qb$ for 非0整数q.

$\Rightarrow |q| \geq 1$. So $|a| = |qb| = |q||b| \geq 1 \cdot |b| \overset{\text{by } *}{\geq} b$

### - The division algorithm (DA)

$\forall a.b \in \mathbb{Z}.\ \exists q.r \in \mathbb{Z}.\ (q \neq r)$ s.t $a = qb + r \quad 0 \le r < b$

ep. $a = 47 \quad b = 16 \Rightarrow 47 = 2 \times 16 + 15$

proof: by contradiction

For uniqueness, assume there exist $q_1, q_2, r_1, r_2 \in \mathbb{Z}$.

where $0 \le r_1 < b \wedge 0 \le r_2 < b$. s.t $q_1 b + r_1 = a = q_2 b + r_2$

$\Rightarrow 0 = (q_1 - q_2) b + (r_1 - r_2) \quad (\star)$

we have $\left.\begin{matrix} 0 \le r_1 < b \\ -b < -r_2 \le 0 \end{matrix}\right\} -b < (r_1 - r_2) < b \quad (\star\star)$

$\because \star \quad \therefore b | (r_1 - r_2). \quad b \le |r_1 - r_2|$

$\because \star\star \quad \therefore |r_1 - r_2| < b$ contradicts

So $r_1 - r_2 = 0 \quad r_1 = r_2$

Finally, put $r_1 = r_2$ in $(\star)$

$0 = (q_1 - q_2) b + 0$

$\because b > 0. \quad q_1 - q_2 = 0 \quad q_1 = q_2$

So, q & r are unique

## 6.2 The greatest common divisor (gcd)

### - GCD The greatest common divisor 最大公因数

definition: $a.b \neq 0$. 存在 gcd : $d$ $(d \in \mathbb{N})$

① $d \mid a$ & $d \mid b$.

② if $c$ is any other divisor, then $c \le d$

※ if $a=0=b$. $\gcd(0,0)=0$  $\gcd(0,15)=15$  $\gcd(-3,0)=3$

### - GCD with remainders (GCD WR)

$0 \le r < b$

$\forall a.b.q.r \in \mathbb{N}$. if $a=qb+r$. then $\gcd(a,b)=\gcd(b,r)$.

※ $b$ & $r$ 没有限制

ex. $\gcd(72,40)$

$72 = 1\times 40+32$
$\therefore \gcd(72,40)=\gcd(40,32)$ by gcd WR

$40 = 1\times 32+8$
$\therefore \gcd(40,32)=\gcd(32,8)$ by gcd WR

$32 = 4\times 8$
$\therefore \gcd(32,8)=\gcd(8,0)$ by gcd WR

$\therefore \gcd(72,42)=\gcd(8,0)=8$

ex. $\gcd(39751, 13081)$

$39751 = 3\times 13081+508$
$\therefore \gcd(39751,13081)=\gcd(13081,508)$ by gcd WR.

$13081 = 25\times 508+381$
$\therefore \gcd(13081,508)=\gcd(508,381)$ by gcd WR

$508 = 1\times 381+127$
$\therefore \gcd(508,381)=\gcd(381,127)$ by gcd WR

$381 = 3\times 127+0$
$\therefore \gcd(381,127)=\gcd(127,0)$ by gcd WR

$\therefore \gcd(39751,13081)=\gcd(127,0)=127$

The process with gcd WR is called "Euclidean Algorithm"

EA 在得到 0 的时候结束

**Proof:**

Let $a = qb + r$. $d = \gcd(a, b)$. Let's show $d = \gcd(b, r)$

We'll need to show

① $d \mid b$ & $d \mid r$ (d is a common divisor)

② if $c \mid b$ & $c \mid r$ then $c \le d$ (c 为一个因数)

Proof ①: 也可证 $\gcd(a,b) \mid \gcd(b,r)$

$d \mid b$ Since $d = \gcd(a, b)$ 且 $\gcd(b,r) \mid \gcd(a,b)$

$\because d \mid a$ & $d \mid b$. $\therefore$ By DIC $d \mid a \times 1 + b \times (-q) = r$ 则两者相等

Proof ②:

assume $c \mid b$ & $c \mid r$. By DIC. $c \mid q \cdot b + 1 \cdot r = a$.

$\therefore c \mid a$ & $c \mid b$. Since $d = \gcd(a, b)$ $c \le d$

ex. Let $a, b \in \mathbb{Z}$. Prove $\gcd(3a+b, a) = \gcd(a, b)$

Proof. Let $a, b \in \mathbb{Z}$

$3a + b = 3 \times a + b$

So $\gcd(3a+b, a) = \gcd(a, b)$ by GCD WR

ex. use Euclidean Algorithm and back substitution to find integers s.t

s.t $481s + 1053t = \gcd(481, 1053)$

$1053 = 2 \times 481 + 91$

$481 = 5 \times 91 + 26$

$91 = 3 \times 26 + 13$

$26 = 2 \times 13 + 0$

$\therefore$ by EA, $\gcd(481, 1053) = 13$

$13 = 91 - 3 \times 26$

$= 91 - 3 \times (481 - 5 \times 91)$

$= 16 \times 91 - 3 \times 481$

$= 16 \times (1053 - 2 \times 481) - 3 \times 481$

$= 481 \times (-35) + 1053 \times 16$

$\therefore s = -35$. $t = 16$.

## 6.3 Certificate of correctness and Bézout's Lemma

- GCD Characterization Theorem (GCD CT) → gcd 未知 / needed.

$\forall a.b.d \in \mathbb{Z}$ $d>0$

If $d \mid a$ and $d \mid b$ and $\exists s.t \in \mathbb{Z}$ $as+bt=d$

Then $d = \gcd(a, b)$

proof: let $a.b.d \in \mathbb{Z}$. $d>0$ $\exists s.t \in \mathbb{Z}$. s.t. $as+bt=d$

case 1: $a \neq 0$ or $b \neq 0$.
assume $\exists s.t \in \mathbb{N}$. s.t. $as+bt=d \neq 0$

prove: $c$ is arbitrary. s.t $c \mid a \wedge c \mid b$, when $\exists x=s$, $y=t$

by DIC. $c \mid (a.s+bt)=d$

$c \mid d \Rightarrow$ BBD $\Rightarrow c \leq |d|$, $c \leq d$

↳ $c \geq d$ $\therefore c=d$

case 2: $a=b=0$.
assume $\exists s.t \in \mathbb{N}$. s.t. $as+bt=d=0$

$\because 0s+0t=0$. $0 \mid 0$. $\therefore d \mid a$ $d \mid b$

$\because \gcd(0,0)=0$. $\therefore d=\gcd(a,b)$

*. $a.b \in \mathbb{Z}$. if $\gcd(a,b) \neq 0$, and $\exists x.y \in \mathbb{Z}$. s.t $ax+by=\gcd(a,b)$
then $\gcd(x,y)=1$

proof. Let $d=\gcd(a,b)=ax+by$. So, $d \mid a$. $d \mid b$.

Let $\exists m.n \in \mathbb{Z}$ $a=dm$. $b=dn$

Then $d=dmx+dny$. $\underline{mx+ny}=1$

$\because$ GCD CT. $\underline{as+bt}=d \Rightarrow d=\gcd(a,b)$

$\therefore \gcd(x,y)=1$

ex. Let $n \in \mathbb{Z}$, Prove $\gcd(n, n+1) = 1$.

Proof:

$\boxed{\text{def.}}$

Let $n \in \mathbb{Z}$

$\because$ $n$ & $n+1$ are consecutive integers

$\therefore$ $n$ & $n+1$ are positive integers.

Suppose $c \mid n$. $c \mid n+1$

by DIC. $c \mid (n+1) \times 1 + n \times (-1)$ so $c \mid 1$.

Therefore, $c = 1$ or $c = -1$.

In both cases, $c \le 1$. So $\gcd(n, n+1) = 1$. by def.

$\boxed{\text{GCD WR}}$

$n+1 = 1 \times n + 1$
$n = 1 \times n + 0$

$\because$ $\gcd(n+1, n) = \gcd(n, 1)$
$\therefore$ $\gcd(n, 1) = \gcd(1, 0) = 1$

$\therefore$ $\gcd(n+1, n) = 1$ by GCD WR

$\boxed{\text{GCD CT}}$

$(n+1) \times 1 + n \times (-1) = 1$

$1 \mid n+1$ & $1 \mid n$ & $1 \ge 0$

So by GCD CT. $\gcd(n, n+1) = 1$

- Bézout's Lemma (BL)

$\forall a, b \in \mathbb{Z}$. if $d = \gcd(a, b)$, then $\exists\, s, t \in \mathbb{Z}$ s.t. $as + bt = d$

(GCD CT 与 BL almost converse)

- Extended Euclidean Algorithm (EEA)

$a, b \in \mathbb{Z}$, $a \ge b > 0$. output $\gcd(a, b)$. and integer $x$ & $y$.

s.t $ax + by = \gcd(a, b)$ in one pass

| $x$ | $y$ | 余数 $r$ | 商 $q$ |
|---|---|---|---|
| 1 | 0 | $a$ | 0 |
| 0 | 1 | $b$ | 0 |
| $1 - 0 \times \boxed{0}$ | $0 - 1 \times \boxed{0}$ | 余数 | $\left\lfloor \frac{a}{b} \right\rfloor$ |

当余数=0 时 stop

然后跟据上一行 $ax + by = \gcd(a, b)$

= 上一行 的 $r$

ex. 计算 gcd (56, 35).

Find integer x, y, s.t $56x+35y = \gcd(56,35)$

| $x$ | $y$ | $r$ 余数 | $q$ 商 |
|---|---|---|---|
| 1 | 0 | 56 | 0 |
| 0 | 1 | 35 | 0 |
| 1 | -1 | 21 | $\boxed{\lfloor \frac{56}{35} \rfloor = 1}$ |
| -1 | 2 | 14 | $\lfloor \frac{35}{21} \rfloor = 1$ |
| 2 | -3 | 7 | $\lfloor \frac{21}{14} \rfloor = 1$ |
| -5 | 8 | 0 | $\lfloor \frac{14}{7} \rfloor = 2$ |

- So $56 \times 2 + 35 \times (-3) = 7$.

$7 = \gcd(56, 35)$

* 若 $a<b$.

$by + ax = \gcd(b, a)$ → 用 EEA

| $y$ | $x$ | $r$ | $q$ |
|---|---|---|---|
| 1 | 0 | $b$ | 0 |
| 0 | 1 | $a$ | 0 |
| ... | | | |

* 若 $a/b < 0$

$\gcd(a,b) = \gcd(|a|, |b|)$

→ 解 $|a|x + |b|y = \gcd(|a|, |b|)$

- Common divisor divides GCD (CDD GCD)

$\forall a, b, c \in \mathbb{Z}$. if $c|a \wedge c|b \Rightarrow c | \gcd(a,b)$

proof: Let $a, b, c \in \mathbb{Z}$.

assume $c|a \wedge c|b$

By BL, $\exists s, t \in \mathbb{Z}$. s.t $as+bt = \gcd(a,b)$

Since $c|a \wedge c|b$. by DIC., $c | as+bt = \gcd(a,b)$

$\therefore c | \gcd(a,b)$

$*$ $\forall a.b.c \in \mathbb{Z}$, if $\gcd(ab, c) = 1 \Rightarrow \gcd(a, c) = \gcd(b, c) = 1$

proof Let $a.b.c \in \mathbb{Z}$

assume $\gcd(ab, c) = 1$

By BL, $\exists s.t \in \mathbb{Z}$ s.t $abs + ct = \gcd(ab, c) = 1$

$\hookrightarrow \therefore a(bs) + c(t) = 1$

$\hookrightarrow b(as) + c(t) = 1$

Since $1 \mid a \wedge 1 \mid c \wedge 1 \geq 0$ by GCDCT, $1 = \gcd(a, c)$

同理 $1 = \gcd(b, c)$

$*$ Converse of $\uparrow$

$\forall a.b.c \in \mathbb{Z}$, if $\gcd(a, c) = \gcd(b, c) = 1 \Rightarrow \gcd(ab, c) = 1$

proof. Let $a.b.c \in \mathbb{Z}$

assume $\gcd(a, c) = 1 \wedge \gcd(b, c) = 1$

By BL $\exists s.t \in \mathbb{Z}$. s.t. $as + ct = 1$ ①

$\exists m.n \in \mathbb{Z}$. s.t. $bm + cn = 1$ ②

① × ②

$asbm + ascn + ctbm + ctcn = 1$

$ab \times sm + c(asn + tbm + tcn) = 1$

Since $sm, (asn + tbm + tcn) \in \mathbb{Z}$

$1 \mid sm$, $1 \mid (asn + tbm + tcn)$ $1 \geq 0$

$\therefore \gcd(a, bc) = 1$ by GCD CT

- Coprimeness Characterization Theorem (CCT)

$\forall a.b \in \mathbb{Z}$. $\gcd(a, b) = 1$. $\Leftrightarrow \exists s.t \in \mathbb{N}$ s.t. $as + bt = 1$

## — Division by GCD (DB GCD)

$\forall a, b \in \mathbb{Z}. \ (a \neq 0 \text{ or } b \neq 0). \ \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1, \quad d = \gcd(a,b)$

Proof: Let $a, b \in \mathbb{Z}$. not both 0.

Assume $d = \gcd(a,b)$

$\because$ a, b not both 0 $\quad \therefore d \neq 0$.

$\because d = \gcd(a,b) \quad \therefore d \mid a \quad d \mid b. \quad \frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$.

$\because d = \gcd(a,b) \quad \therefore \exists s, t \in \mathbb{Z}$. s.t. $as + bt = d$ By BL.

$\frac{a}{d}s + \frac{b}{d}t = 1 \longleftarrow d \neq 0$

$\because \frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$. By CCT $\quad \therefore \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

ex. Prove $\gcd(a,b) = 1 \Rightarrow \gcd(a, bc) = \gcd(a,c) \quad c \in \mathbb{N}$.

$\rightarrow$ Due to BL, $as + bt = 1$

Let $\gcd(a,c) = d \quad am + cn = d$

$(as + bt)(am + cn) = d$

$a^2sm + ascn + abtm + bctn = d$

$a(asm + csn + btm) + bc(tn) = d$

$\rightarrow \because a \cdot s \cdot m \cdot c \cdot n \cdot b \cdot t \in \mathbb{Z}. \quad \therefore asm + csn + btm \in \mathbb{Z}$

$\because d = \gcd(a,c) \quad \therefore d \mid a \quad d \mid c$

$\because c \mid bc \quad \therefore$ By TD $\quad d \mid bc$

$\because d \geq 0$

$\therefore$ By GCDCT $\quad d = \gcd(a, bc)$

So $\gcd(a, bc) = \gcd(a, c)$

- Coprimeness and divisibility (CAD)

$\forall a, b \in \mathbb{Z}.\quad c \mid ab \wedge \gcd(a, c) = 1 \Rightarrow c \mid b$

ex. $4 \mid 5 \times 8 \quad \gcd(4, 5) = 1 \Rightarrow 4 \mid 8.$

proof: Let $a, b, c \in \mathbb{Z}$.

Assume $c \mid ab \quad \gcd(a, c) = 1$

Since $\gcd(a, c) = 1$, by CCT. $\exists x, y \in \mathbb{Z}$, s.t $ax + cy = 1$

Since $c \mid ab$, $\exists k \in \mathbb{Z}$ s.t $ab = ck$

两边同乘 b

$abx + cby = b$

$\because ab = ck \quad \therefore ckx + cby = b \quad c(kx + by) = b$

Since $k, x, b, y \in \mathbb{Z}$. $kx + by \in \mathbb{Z}$. So $c \mid b$

# 6.6 Prime Numbers

- def.

  If $p \in \mathbb{N}$. $p > 1$. and positive divisors are only 1 & p.
  Then p is prime

- Prime Factorization (PF)

  every natural number $n > 1$ can be written as product of primes

- Euclid's Theorem (ET)

  有无穷个质数

- Euclid's Lemma (EL)

  $\forall a, b \in \mathbb{N}$. p is prime. $p | ab \Rightarrow p | a \lor p | b$

  proof. Let $a, b \in \mathbb{Z}$. p is prime num.
  prove by elimination.
  $p | ab \land p \nmid a \Rightarrow p | b$.
  $\because$ p is prime, $\therefore$ its only positive divisors are 1 & p
  $\because p \nmid a$, $\therefore \gcd(a, p) = 1$
  $\because p | ab \land \gcd(a, p) = 1$ $\therefore p | b$ By CAP

- Generalized Euclid's Lemma

  p is prime. $n \in \mathbb{N}$. $a_1, a_2 \cdots a_n \in \mathbb{Z}$.
  $p | a_1 a_2 \cdots a_n \Rightarrow p | a_i$ for some $i = 1, 2, \cdots, n$

## - Unique Factorization Theorem (UFT)

Every $\mathbb{N}$ $(n>1)$ can be written as a product of prime factors uniquely apart from the order of factors. 大于1的自然数只能写成唯一一种 prime 相乘的形式

ex. Let $p$ be a prime. Prove $13p+1$ is perfect square iff $p=11$

$(\Rightarrow)$ $13p+1$ perfect $\Rightarrow p=11$

$x^2 = 13p+1$ $\quad (x \in \mathbb{N})$

$\downarrow$

$13p = x^2-1 = (x+1)(x-1)$

Since 13 & $p$ are prime, by UFT, the prime factorization $(k-1)(k+1)$ must be $p$

case 1. $k-1=13$ $\quad k+1=p$

$k=14$ $\quad p=15$ $\quad$ ($p$ isn't prime, $\therefore$ DNE)

case 2. $k-1=p$ $\quad k+1=13$

$k=12$ $\quad p=11$ $\quad \checkmark$

case 3. $k-1=1$ $\quad k+1=13.$ $\qquad$ ($\because k-1<k+1$ $\quad 1<13p$ $\quad \therefore$ we can't have $k-1=13p$ $\quad k+1=1$)

$k=2$ $\quad p=\frac{3}{13}$ (DNE).

Therefore, if $13p+1$ is perfect square, then $p=11$

$(\Leftarrow)$ Assume $p=11$

Then $13p+1 = 13\times 11+1 = 143+1 = 144.$ $\rightarrow$ a perfect square

## - Divisors from prime factorization (DFPF)

Let $n, c \in \mathbb{Z}$. $\quad n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ $\quad$ ($p$: prime $\alpha \in \mathbb{N}$)

$c \mid n \iff 0 \le \beta \le \alpha \quad c = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$

ex. How many positive multiple of 12 are divisors of 8820?

$12 = 2^2 \times 3^1 \times 5^0 \times 7^0 \qquad 8820 = 2^2 \times 3^2 \times 5 \times 7^2$

By DFPF: The positive divisors of 8820 are exactly numbers of form:

$2^{\beta_1} 3^{\beta_2} 5^{\beta_3} 7^{\beta_4} \qquad 0 \le \beta_1 \le 2 \quad 0 \le \beta_2 \le 2 \quad 0 \le \beta_3 \le 1 \quad 0 \le \beta_4 \le 2$

To be multiple of 12. We further require $\beta_1 \ge 12$ and $\beta_2 \ge 1$

Therefore $2 \le \beta_1 \le 2 \qquad \beta_1 = 2$

$1 \le \beta_2 \le 2 \qquad \beta_2 = 1$ or $2$.

$0 \le \beta_3 \le 1 \qquad \beta_3 = 0$ or $1$.

$0 \le \beta_4 \le 2 \qquad \beta_4 = 0, 1, 2.$

So $1 \times 2 \times 2 \times 3 = 12$ positive multiple

ex. Let $a, b \in \mathbb{Z}$. Prove $a^3 \mid b^3 \iff a \mid b$

($\Rightarrow$) $a^3 \mid b^3 \Rightarrow a \mid b$

Let $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_n} \qquad a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_n}$ $\qquad$ ($p$: prime)

$\therefore b^3 = p_1^{3\beta_1} p_2^{3\beta_2} \cdots p_r^{3\beta_n} \qquad a = p_1^{3\alpha_1} p_2^{3\alpha_2} \cdots p_r^{3\alpha_n}$

By DFPF, $3\beta_i \ge 3\alpha_i \ge 0$

$\therefore \beta_i \ge \alpha_i$ for all $i$. by DFPF, $a \mid b$

($\Leftarrow$) $a \mid b \Rightarrow a^3 \mid b^3$

$\because a \mid b$. $b = ka$ for some $k \in \mathbb{Z}$.

$\therefore b^3 = k^3 a^3 \qquad k \in \mathbb{Z}.\ k^3 \in \mathbb{Z} \qquad \therefore a^3 \mid b^3$

## - GCD from Prime factorization (GCD PF)

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ $\qquad$ $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$

$\gcd(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}.$ $\qquad$ $\gamma_i = \min\{\alpha_i, \beta_i\}$ $(i = 1, 2, \cdots, k)$

ex. use GCDPF to calculate $\gcd(13230, 12936)$

$\gcd(13230, 12936)$

$= \gcd(2 \times 3^3 \times 5 \times 7^2,\ 2^3 \times 3 \times 7^2 \times 11)$

$= 2^{\min\{1,3\}} \times 3^{\min\{1,3\}} \times 5^{\min\{1,0\}} \times 7^{\min\{2,2\}} \times 11^{\min\{0,1\}}$

$= 2^1 \times 3^1 \times 5^0 \times 7^0 \times 11$

$= 6 \times 49$

$= 294$

# 7.1 Linear Diophantine Equations (LDEs)

- def.

both coefficient & variables are integers

ex. ① Does $143x + 253y = 11$ have a sol? Why?
② Does $143x + 253y = 155$ have a sol? Why?
③ Does $143x + 253y = 154$ have a sol? Why?

→ Find $x, y \in \mathbb{Z}$ s.t. $143x + 253y = d$  $d = \gcd(143, 253)$

| y | x | r | q |
|---|---|---|---|
| 1 | 0 | 253 | 0 |
| 0 | 1 | 143 | 0 |
| 1 | -1 | 110 | 1 |
| -1 | 2 | 33 | 1 |
| 4 | -7 | 11 | 3 |
| -13 | 23 | 0 | 3 |

$4 \times 253 - 7 \times 143 = 11$

→ ① Yes. We found $x = -7$ $y = 4$

② No

$\because 11 = \gcd(143, 253)$ $\therefore 11 \mid 143$ $11 \mid 253$

Proof by contradiction: Assume $\exists x_0, y_0 \in \mathbb{Z}$. s.t. $143x_0 + 253y_0 = 155$

$\because 11 \mid 143$ $11 \mid 253$, By DIC $11 \mid 143x_0 + 253y_0$

$\therefore 11 \mid 155$. But $11 \nmid 155$. contradicts.

So $143x + 253y = 155$ have no integer solution

③ Yes.

$11 \mid 143$.  $154 = 14 \times 11$

$143 \times (-7) + 253 \times 4 = 11$

$14 \times [143 \times (-7) + 253 \times 4] = 11 \times 14$

$143 \times (-7 \times 14) + 253(4 \times 14) = 154$

$143 \times (-98) + 253 \times 56 = 154$

## - Linear Diophantine Equation Theorem 1 (LDET 1)

$\forall a\, b\, c \in \mathbb{N}$ $(a \neq 0 \wedge b \neq 0)$

the LDE $ax+by=c$ has integer sol $x, y$. $\iff$ $d \mid c$ $(d = \gcd(a,b))$

Proof: Let $a\, b\, c \in \mathbb{Z}$. $a \neq 0$ $b \neq 0$

Let $d = \gcd(a,b)$

$(\Rightarrow)$ Assume LDE $ax+by=c$ has int sol

Then $\exists x_0\, y_0 \in \mathbb{Z}$, s.t $ax_0 + by_0 = c$

Let $d = \gcd(a,b)$, $d \mid a$ and $d \mid b$.

By DIC, $d \mid ax_0 + by_0$ $\therefore d \mid c$

$(\Leftarrow)$ Assume $d \mid c$

Then $c = kd$ $(k \in \mathbb{Z})$

Since $d = \gcd(a,b)$, By BL, $\exists s, t \in \mathbb{Z}$. s.t $as+bt=d$

$k(as+bt) = kd$

$a(ks) + b(kt) = c$

$\therefore x = ks$. $y = kt$ is a sol to $ax+by=c$.

# 7.2 Finding all solutions in 2 variables

## - LDET 2

Let $a, b, c \in \mathbb{Z}$. $a \neq 0$ $b \neq 0$. $d = \gcd(a, b)$

If $x = x_0 \wedge y = y_0$ is one particular integer sol in LDE $ax + by = c$

then set of all sol is $\{(x, y): x = x_0 + \frac{b}{d} n,\ y = y_0 - \frac{a}{d} n,\ n \in \mathbb{Z}\}$

ex. determine all sol to $\underset{a}{143}x + \underset{b}{253}y = \underset{c}{154}$ , 已知 $x = -98$. $y = 56$

$11 \times 14$

From LDET 2. the complete sol is

$x = -98 + \frac{253}{11} n$

$y = 56 - \frac{143}{11} n$ , $n \in \mathbb{Z}$

化简得 $x = -98 + 23n$ , $y = 56 - 13n$ , $n \in \mathbb{Z}$

So, $\{(x, y): x = -98 + 23n,\ y = 56 - 13n,\ n \in \mathbb{Z}\}$

$y = \frac{154 - 143x}{253}$

$-\frac{143x}{253} + \frac{154}{253} - \frac{143}{253}(x - x_0)$

$\frac{13}{23}(x - x_0)$

$\frac{143}{d}$

$x = x_0 + \frac{b}{d} n$ $y = y_0 - \frac{a}{d} n$

Proof.

- Let $a, b, c$ be arbitrary integers. $a \neq 0$ $b \neq 0$. $d = \gcd(a,b)$

Define $A = \{(x,y) : x = x_0 + \frac{b}{d}n,\ y = y_0 - \frac{a}{d}n,\ n \in \mathbb{Z}\}$

$B = \{(x,y) : x, y \in \mathbb{Z},\ ax + by = c\}$

想证 $A = B$，则需证 $A \subseteq B$，$B \subseteq A$

- Prove $A \subseteq B$. 已知 $(x,y) \in A$ 需证 $(x,y) \in B$

$\because (x,y) \in A$ $\therefore x = x_0 + \frac{b}{d}n$ and $y = y_0 - \frac{a}{d}n$. $n \in \mathbb{Z}$

$ax + by = a(x_0 + \frac{b}{d}n) + b(y_0 - \frac{a}{d}n)$

$= ax_0 + \frac{ab}{d}n + by_0 - \frac{ab}{d}n = ax_0 + by_0 = c$

$\because (x_0, y_0)$ is a sol to $ax+by=c$

So $(x,y) \in B$ $A \subseteq B$

- Prove $B \subseteq A$. 已知 $(x,y) \in B$ 需证 $(x,y) \in A$

$\because (x,y) \in B$ $\therefore ax+by=c$ $(x, y \in \mathbb{Z})$

$(x_0, y_0)$ is a sol to LDE. $ax_0 + by_0 = c$ $\Rightarrow ax + by = ax_0 + by_0$ $(*)$

$a(x - x_0) = b(y_0 - y)$

$\because a \neq 0 \wedge b \neq 0, d \neq 0$. dividing by $d \neq 0$ $\therefore \frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$

$\because \frac{a}{d}$ & $(x - x_0) \in \mathbb{Z}$. $\therefore \frac{a}{d} \mid \frac{b}{d}(y_0 - y)$

$\because \gcd(\frac{a}{d}, \frac{b}{d}) = 1$ by DBGCD. $\therefore \frac{a}{d} \mid y_0 - y$. by CAD

$\frac{a}{d}n = y_0 - y$ $y = y_0 - \frac{a}{d}n$

代入 $*$ $\frac{a}{d}(x - x_0) = \frac{b}{d}(\frac{a}{d})n$

$a(x - x_0) = \frac{ab}{d}n$

$x - x_0 = \frac{b}{d}n$ $(\because a \neq 0)$

$x = x_0 + \frac{b}{d}n$

# 8.1 Congruence

- def.

被除数 ↓, 余数 + n · m

m 为固定正整数　若 $m \mid (a-b)$　$a, b \in \mathbb{Z}$.

"a is congruent to b modulo m"

写作 $a \equiv b \pmod m$　　≡: congruence　　m: modulus

eg. $7 \equiv -1 \bmod 8$.　Since $8 \mid 7-(-1)$

$-1 \equiv 15 \bmod 8$　Since $8 \mid -1-15$

$\Rightarrow a \equiv b \pmod m$　$\Leftrightarrow m \mid (a-b)$

$\Leftrightarrow a-b = km$　$k \in \mathbb{Z}$

$\Leftrightarrow a = b + km$　$k \in \mathbb{Z}$.

# 8.2 Properties of Congruence

- Congruence is an Equivalent Relation (CER)

$\forall a\, b\, c \in \mathbb{Z}$.

① $a \equiv a \pmod m$　Reflexible

② $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$　Symmetric

③ $a \equiv b \pmod m \wedge b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$　Transitive

Proof ①:

Let $a \in \mathbb{Z}$　$a - a = 0$

$\because m \in \mathbb{N}$, $m \mid 0$　$\therefore m \mid a-a$.　$a \equiv a \pmod m$

Proof ②:

Let $a, b \in \mathbb{Z}$.

Assume $a \equiv b \pmod m$　$\rightarrow m \mid (a-b)$

$\because (a-b) \mid -(a-b)$　By TD.　$m \mid -(a-b)$

$\therefore m \mid (b-a)$　$b \equiv a \pmod m$

Proof ③:

Let $a, b, c \in \mathbb{Z}$

Assume $a \equiv b \pmod m$ and $b \equiv c \pmod m$

$\therefore m \mid a-b \qquad m \mid b-c$

By DIC, $m \mid a-b+(b-c) \qquad \therefore m \mid a-c$

$\therefore m \mid a-c \qquad a \equiv c \pmod m$

- Proposition 2.

$\forall a_1, a_2, b_1, b_2 \in \mathbb{Z}$, If $a_1 \equiv b_1 \pmod m \quad a_2 \equiv b_2 \pmod m$

Then ① $a_1 + a_2 \equiv b_1 + b_2 \pmod m$

② $a_1 - a_2 \equiv b_1 - b_2 \pmod m$

③ $a_1 a_2 \equiv b_1 b_2 \pmod m$

Proof ③:

Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$.

Assume $a_1 \equiv b_1 \pmod m$ and $a_2 \equiv b_2 \pmod m$

Then $m \mid a_1 - b_1 \qquad m \mid a_2 - b_2$

By DIC, $m \mid (a_1 - b_1) a_2 + (a_2 - b_2) b_1$

So $m \mid a_1 a_2 - b_1 b_2$

- Congruence Add and Multiply (CAM)

$\forall n \in \mathbb{Z}^+$, $a_1, \cdots, a_n . b_1, \cdots, b_n \in \mathbb{Z}$

If $a_i \equiv b_i \pmod m \qquad 1 \le i \le n$

Then ① $a_1 + a_2 + \cdots + a_n \equiv b_1 + b_2 + \cdots + b_n \pmod m$

② $a_1 a_2 \cdots a_n \equiv b_1 b_2 \cdots b_n \pmod m$

- Congruence Power (CP)

$\forall n \in \mathbb{Z}^+$, $a.b \in \mathbb{Z}$.

$a \equiv b \pmod m \Rightarrow a^n \equiv b^n \pmod m$

- Congruence Divide (CD)

$\forall a.b.c \in \mathbb{Z}$,

互质

$ac \equiv bc \pmod m \wedge \gcd(c, m) = 1 \Rightarrow a \equiv b \pmod m$

ep.
$27 \equiv 3 \pmod 8$ $\quad 8 \mid 27-3 = 3 \times (9-1)$

Since $\gcd(8,3)=1$, by CAD $8 \mid 9-1$ So $9 \equiv 1 \pmod 8$

$27 \equiv 3 \pmod{12}$ $\quad 12 \mid 27-3 = 3(9-1)$

$12 \nmid 9-1$ So $9 \not\equiv 1 \pmod{12}$

Proof. Let $a b c \in \mathbb{Z}$

Assume $ac \equiv bc \pmod m$ and $\gcd(c, m) = 1$

$\because ac \equiv bc \pmod m$ $\therefore m \mid ac - bc = c(a-b)$

$\because \gcd(c, m) = 1$ by CAD $m \mid a-b$

So $a \equiv b \pmod m$

* 1. 若 $\gcd(c, m) \neq 1$, CD tells nothing!

2. If $ac \equiv bc \pmod m$, then $a \equiv b \pmod{\frac{m}{\gcd(c, m)}}$

题目出现要证明

ex. is $5^9+62^{2000}-14$ divisible by 7.

$7 \mid (5^9+62^{2000}-14)-0$

$5^9+62^{2000}-14 \equiv 0 \pmod 7$

$-14 \equiv 0 \pmod 7$ (Since $7 \mid -14-0$)

$62 \equiv (-1) \pmod 7$ (Since $7 \mid 62-(-1)$)

By CP. $62^{2000} \equiv (-1)^{2000} \pmod 7$
$\equiv 1 \pmod 7$

$5 \equiv (-2) \pmod 7$

So $5^3 \equiv (-2)^3 \pmod 7$ by CP
$\equiv 8 \pmod 7$
$\equiv -1 \pmod 7$ (Since $7 \mid -8-(-1)$)

So $5^9 \equiv (5^3)^3 \equiv (-1)^3 \bmod 7$ by CP
$\equiv -1 \bmod 7$

By CAM $5^9+62^{2000}-14 \equiv (-1)+1+0 \pmod 7$
$\equiv 0 \pmod 7$

So $5^9+62^{2000}-14$ is divisible by 7

# 8.3 Congruence and Remainders

## - Congruent Iff Same Remainder (CISR)

$\forall a\ b \in \mathbb{Z}.\ a \equiv b \pmod m \Leftrightarrow a \div m$ 与 $b \div m$ 余数相同

Proof. Let $a\ b \in \mathbb{Z}$

By DA, $a = q_1 m + r_1$  $b = q_2 m + r_2$

for unique $q_1, r_1, q_2, r_2 \in \mathbb{Z}$  $0 \le r_1 < m$ and $0 \le r_2 < m$

"$\Rightarrow$" Assume $a \equiv b \pmod m$  证 $r_1 = r_2$

$\because a \equiv b \pmod m$  $m \mid a-b$

$\because a-b = m(q_1 - q_2) + r_1 - r_2$  $\therefore m \mid [m(q_1-q_2) + r_1 - r_2]$

Also, $m \mid m(q_1 - q_2)$

By DIC, $m \mid [m(q_1-q_2) + r_1 - r_2] - m(q_1 - q_2)$

So $m \mid r_1 - r_2$

So $r_1 - r_2 = km$ for some $k \in \mathbb{Z}$

$\because 0 \le r_1 < m$ and $0 \le r_2 < m$

$\therefore 0 \le r_1 < m$  $0 \ge -r_2 > -m$

$\therefore -m < r_1 - r_2 < m.$

So $-m < km < m$  Since $r_1 - r_2 = km$

同除 $m > 0$  $-1 < k < 1$

$\because k \in \mathbb{Z}$  $k = 0$

$\therefore r_1 - r_2 = 0$  $\therefore r_1 = r_2$

"$\Leftarrow$" Assume a & b have the same remainder when $\div m$

↳ 相当于 assume $r_1 = r_2$

So $a = q_1 m + r_1$ and $b = q_2 m + r_1$

and $a-b = q_1 m + r_1 - q_2 m - r_1 = m(q_1 - q_2)$

Since $q_1 . q_2 \in \mathbb{Z}$, $q_1 - q_2 \in \mathbb{Z}$ So $m \mid a-b$

Therefore, $a \equiv b \pmod{m}$

## - Congruent To Remainder (CTR)

$\forall a\, b \in \mathbb{Z}$, $0 \le b < m$,

$a \equiv b \pmod{m} \Leftrightarrow a \div m \cdots\cdots b$

ex. What remainder of $[77^{100}(999) - 6^{83}] \div 4$

So $77^{100} \equiv 1^{100} \pmod{4}$ by CP
$\equiv 1 \pmod{4}$

$999 \equiv (-1) \pmod{4}$
$6 \equiv 2 \pmod{4}$

So $6^2 \equiv 2^2 \pmod{4}$ by CP
$\equiv 4 \pmod{4}$
$\equiv 0 \pmod{4}$

by CP

So $6^{83} \equiv 6(6^2)^{41} \equiv 6(0)^{41} \equiv 6 \cdot 0 \equiv 0 \pmod{4}$

By CAM, $77^{100} \times 999 - 6^{83} \equiv 1 \times (-1) - 0 \pmod{4}$
$\equiv -1 \pmod{4}$
$\equiv 3 \pmod{4}$

Since $0 \le 3 < 4$ by CTR, remainder is 3.

## - Divisibility by 3

$3 \mid a \Leftrightarrow 3 \mid$ sum of digits

Proof: Let $a$ be non-negative integer

→ Let $d_k . d_{k-1} . \cdots d_2 . d_1 . d_0$ be decimal representation of $a$.
$d_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ $\forall i = 0, \ldots, k$ $(k \ge 0)$

Then $a = d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_0 \cdot 10^0$

→ $\because 10 \equiv 1 \pmod{3}$

$\therefore$ by CP, $10^i \equiv 1^i \equiv 1 \pmod{3}$ $\forall i \in \mathbb{N}$

$\rightarrow$ By CAM and CP, $a \equiv d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_1 10^1 + d_0 \pmod{3}$

$\equiv d_k + d_{k-1} + \cdots + d_2 + d_1 + d_0 \pmod{3}$

$\rightarrow$ By CTR, $3 | a \Leftrightarrow a \equiv 0 \pmod{3}$

$\rightarrow$ $\because$ $a \equiv d_k + d_{k-1} + \cdots + d_2 + d_1 + d_0 \pmod{3}$

$\therefore$ $a \equiv 0 \pmod{3}$ iff $d_k + d_{k-1} + \cdots + d_0 \equiv 0 \pmod{3}$

$3 | a \Leftrightarrow 3 | d_k + d_{k-1} + \cdots + d_0$

- Divisibility by 11

$11 | a \Leftrightarrow 11 | S_e - S_o$

($S_e$ : sum of even digit of a, $S_o$ : sum of odd digit of a)

# 8.4 Linear Congruence

## - linear congruence

$ax \equiv c \pmod m$ is l-c in $x$.

solution to the l-c is $x_0$. s.t $ax_0 \equiv c \pmod m$

## - linear congruence theorem (LCT)

$\forall a, c \in \mathbb{N}$, $a \neq 0$,

$ax \equiv c \pmod m$ has a sol $\Leftrightarrow$ $d \mid c$. $d = \gcd(a, m)$

If $x = x_0$ is a sol of congruence, then $\{x \in \mathbb{Z} : x \equiv x_0 \pmod{\frac{m}{d}}\}$

$\{x \in \mathbb{Z} : x \equiv x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d}, \dots, x_0 + (d-1)\frac{m}{d} \pmod m\}$

ex. Find all sol of $4x - 2 \equiv 6 \pmod{10}$

By CAM equivalent to $4x \equiv 8 \pmod{10}$ by CAM

→

| $x \pmod{10}$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $4x \pmod{10}$ | 0 | 4 | 8 | 2 | 6 | 0 | 4 | 8 | 2 | 6 |

→ ∴ Sol are $x \equiv 2 \pmod{10}$ or $x \equiv 7 \pmod{10}$

☆ 若结果存在，则有 1 sol mod $\frac{m}{d}$

d sol mod $m$

$ax \equiv c \pmod m$ where $x \in \mathbb{Z}$

$\Leftrightarrow$ $c \equiv ax \pmod m$

$\Leftrightarrow$ $m \mid (c - ax)$

$\Leftrightarrow$ $c - ax = km$ $\quad k \in \mathbb{Z}$

$\Leftrightarrow$ $ax + mk = c$ $\quad x, k \in \mathbb{Z}$

$ax + mk = c$ has a sol iff $\gcd(a, m) \mid c$

ex. Find all sol of $12x \equiv 102 \pmod{2010}$

↳ equivalent to solving LDE $12x + 2010y = 102$

→ $\gcd(12, 2010) = 6$ by EEA

∵ $6 \mid 102$ ∴ LDE has solutions.

$x = -2839$ $y = 17$

→ $\{(x,y) : x = -2839 + \frac{2010}{6}n, \ y = 17 - \frac{12}{6}n, \ n \in \mathbb{Z}\}$ by LDET2

∴ $x = -2839 + \frac{2010}{6}n = -2839 + 335n, \ n \in \mathbb{Z}$

→ $x \equiv -2839 \pmod{335} \equiv 176 \pmod{335}$

$\forall k \in \mathbb{Z} \ x = 176 + 335k$ $x \equiv 176 \pmod{335}$

∵ $2010 = 335 \times 6$. $x \equiv 176 \pmod{2010}$

$k=0$ $x = 176 \pmod{2010}$

$k=1$ $x = 511 \pmod{2010}$

$k=2$ $x = 846 \pmod{2010}$

$k=3$ $x = 1181 \pmod{2010}$

$k=4$ $x = 1516 \pmod{2010}$

$k=5$ $x = 1851 \pmod{2010}$

$k=6$ $x = 2186 \equiv 176 \pmod{2010}$

∴ $x = 176, 511, 846, 1181, 1516, 1851, 2186$

① 证LDE有解

写成 $ax + my = c$ 的形式

$\gcd(a, m) = \cdots$

$\cdots \mid c \Rightarrow$ 有解

② LDET2

③ 求x解

ex. Find all sol to $10 \equiv 3 \pmod{14}$

equivalent to solving LDE $10x + 14y = 3$

→ $\gcd(10, 14) = 2$ by EEA.

$2 \nmid 3$. have no sol

ex. Find all sol to $15x \equiv 6 \pmod{18}$

→ Since $\gcd(15, 18) = 3$ $3 \mid 6$

By LCT, the LDE has sols. (3 sols mod 18)

→ $x=4$ is a sol.

By LCT, the complete sol is $\{x \in \mathbb{Z} : x \equiv 4 \bmod \frac{18}{3}\}$ $\frac{m}{d}$

→ $\{x \in \mathbb{Z} : x \equiv 4 \bmod 6\}$

⇒ $\{x \in \mathbb{Z} : x \equiv 4, 10, 16 \pmod{6}\}$

# 8.6 Congruence Classes & Modular Arithmetic

- def. congruence class (属于 set)

CC mod $m$ of Int $a$ is set of Int.

$$[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}$$

* 需要已知 $m$ 只说 $[4]$ is ambiguous
* By CISR, there are $m$ different congruence classes mod $m$ since there are $m$ possible remainders when $\div m$.
* When $m=5$. $[4] = [9] = [-1]$

∴ 一般用 $0 \sim m-1$ 来代指

- $\mathbb{Z}_m$

The Int modulo $m$ to be set of $m$ cc.

$$\mathbb{Z}_m = \{[0], [1], [2], [3], \dots, [m-1]\}$$

- modular arithmetic

$[a]+[b]=[a+b]$ $[a][b]=[ab]$ $[1]^{-1} = [1]$

$[2]^{-1}$ DNE

$[3]^{-1} = [3]$

eg. $\mathbb{Z}_4$

| + | [0] | [1] | [2] | [3] |
|---|---|---|---|---|
| [0] | [0] | [1] | [2] | [3] |
| [1] | [1] | [2] | [3] | [0] |
| [2] | [2] | [3] | [0] | [1] |
| [3] | [3] | [0] | [1] | [2] |

| × | [0] | [1] | [2] | [3] |
|---|---|---|---|---|
| [0] | [0] | [0] | [0] | [0] |
| [1] | [0] | [1] | [2] | [3] |
| [2] | [0] | [2] | [0] | [2] |
| [3] | [0] | [3] | [2] | [1] |

① For any $[a]$ in $\mathbb{Z}_m$ $\quad [a]+[0]=[a+0]=[a]$

$[0]$ is the additive identity in $\mathbb{Z}_m$.

② For any $[a]$ in $\mathbb{Z}_m$ $\quad [a][1]=[a\cdot 1]=[a]$

$[1]$ is the multiplicative identity in $\mathbb{Z}_m$

③ For all $[a]\in\mathbb{Z}_m$ $\quad [a]+[-a]=[a+(-a)]=[0]$

$[-a]$ is the additive inverse of $[a]$ multiplicative identity

④ For any $[a]\in\mathbb{Z}_m$ $\quad [a][b]=[b][a]=[1]$

$[b]$ is the multiplicative inverse of $[a]$. 写作 $[a]^{-1}=[b]$

有时不存在: ep. $\mathbb{Z}_4$. $[-1]^{-1}=[1]$

$[0]^{-1}$ & $[2]^{-1}$ don't have multiplicative inverse

ex. Calculate add~ and mult~ of $[6]$ & $[7]$

add~ of $[6]$ is $[-6]=[3]$

add~ of $[7]$ is $[-7]=[2]$

mult~ of $[6]$ is $[6][x]=[1]$ or equivalently $[6x]=[1]$

True exactly when $6x\equiv 1 \pmod 9$.

$\because \gcd(6,9)=3$ $\quad 3\nmid 1$ by LCT $\quad \therefore$ no sol

So $[6]^{-1}$ DNE in $\mathbb{Z}_9$

mult~ of $[7]$ is $[7][x]=[1]$ or equivalently $[7x]=[1]$

True exactly when $7x\equiv 1 \pmod 9$

$\because \gcd(7,9)=1$ $\quad 1\mid 1$ by LCT $\quad \therefore$ have 1 sol mod 9.

By inspection, $x=4$ is a sol. By LCT. the complete sol is $x\equiv 4 \pmod 9$

So we see that $[7]^{-1}=[4]$

## - Modular Arithmetic Theorem (MAT)

$\forall a, c \in \mathbb{Z}$. $a \neq 0$.

$[a][x] = [c]$ in $\mathbb{Z}_m$ has a sol iff $d \mid c$. $d = \gcd(a, m)$

When $d \mid c$, there are $d$ sols.

$[x_0], [x_0 + \frac{m}{d}], [x_0 + 2\frac{m}{d}], \dots, [x_0 + (d-1)\frac{m}{d}]$

where $[x] = [x_0]$ is 1 sol.

ex. Solve $[25][x] = [12]$ in $\mathbb{Z}_9$ $\qquad 25x \equiv 12 \mod 9$

$\rightarrow [25][x] + [4] = [12]$

$[7][x] = [12] - [4] = [8]$ 化简

$\rightarrow$ By MAT, since $\gcd(7, 9) = 1$ and $1 \mid 8$, there is 1 sol 先看有解

$\rightarrow 9 \mid 7x - 8$. $\quad 9n = 7x - 8 \quad 7x - 9n = 8$ (用EEA解)

By inspection $[5]$ is a sol. since $[7][5] = [35] = [8]$

so the sol is $[x] = [5]$

ex. Solve $[24][x] + [3] = [7]$ in $\mathbb{Z}_9$

$\Leftrightarrow [6][x] = [4]$

$\because \gcd(6, 9) = 3$. and $3 \nmid 4$

$\therefore$ no sol.

# 8.7 Fermat's Little Theorem

## - Fermat's Little Theorem (FlT)

$\forall p \in \text{prime} \wedge p \nmid a.\quad a^{p-1} \equiv 1 \pmod p$

eg. $6^6 \equiv 1 \bmod 7$ $\because 7 \nmid 6$ $\quad 6^2 \equiv 36 \equiv 1 \pmod 7$

$p = 7.\quad a = 6$

$\mathbb{Z}_7.\quad [1]\quad [2]\quad [3]\quad [4]\quad [5]\quad [6]$

$\times[a]$

$[6]\quad [12]\quad [18]\quad [24]\quad [30]\quad [36]$

proof: pgs 138 - 139

$$\begin{array}{ccc} 1 & & a \\ 2 & \times a & 2a \\ 3 & \rightarrow & 3a \\ \vdots & & \vdots \\ p-1 & & a(p-1) \end{array}$$

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot a \cdots (p-1) \pmod p$$

$$a^{p-1}(1 \cdot a \cdots (p-1)) \equiv 1 \cdot a \cdots (p-1) \pmod p$$

$$a^{p-1} \equiv 1 \pmod p$$

ex. determine the remainder when $7^{92}$ is divided by 11.

$\because$ 11 is prime $\wedge$ $11 \nmid 7$, FlT applies $\quad 7^{10} \equiv 1 \pmod{11}$

$\therefore 7^{92} \equiv 7^2 (7^{10})^9 \equiv 49 (1)^9 \pmod{11}$

$\equiv 5 \bmod 11$

$\because 0 \le 5 < 11$. By CTR. remainder is 5

* 1. In $\mathbb{Z}_p$, FlT tells us that $[a] \neq [0]$

$[a^{p-1}] = [1]$, $\quad [a]^{p-1} = [1]$

2. In $\mathbb{Z}_p$, every nonzero congruence class, $[a] \neq [0]$,

has a multiplicative inverse $[a]^{-1}$.

From FlT, $[a]^{-1} = [a^{p-2}]$ $\qquad$ eg. $\mathbb{Z}_{103}$, $[22]^{-1} = [22^{101}]$

## — Corollary 推论

$\forall p \in \text{prime}.\ a \in \mathbb{Z}.\quad a^p \equiv a \pmod p$

proof.

case 1: $p \mid a$

$a \equiv 0 \pmod p \quad a^p \equiv 0^p \equiv 0 \pmod p \quad \therefore a^p \equiv a \pmod p$

case 2: $p \nmid a$

By FLT $\quad a^{p-1} \equiv 1 \pmod p \quad$ 两边$\times a$ $\rightarrow a^p \equiv a \pmod p$

ep. $p \nmid a$ : $6^6 \equiv 1 \pmod 7$ by FLT.

$\Rightarrow 6 \cdot 6^6 \equiv 6 \cdot 1 \pmod 7$

$p \mid a$ : $14^7 \equiv 14 \pmod 7$

ex. determine the remainder when $8^{9^7}$ is divided by 11.

$\because 11$ is prime. $11 \nmid 8$ $\qquad$ ※ $8^{9^7} \neq (8^9)^7$

$\therefore$ Due to FLT, $8^{10} \equiv 1 \pmod{11}$

$9 \equiv (-1) \pmod{10}$ ? $\quad \therefore$ By CP, $9^7 \equiv (-1)^7 \equiv -1 \equiv 9 \pmod{10}$

$\therefore 9^7 = 9 + 10k \quad k \in \mathbb{Z}$

$8^{9^7} \equiv 8^{9+10k} \equiv 8^9 \cdot (8^{10})^k \equiv 8^9 (1)^k \pmod{11}$ by FLT

$\cdots \equiv 7 \pmod{11}$

$\because 0 \le 7 < 11$ by CTR, the remainder is 7

# 8.8 The Chinese Remainder Theorem

## - Chinese Remainder Theorem (CRT)

$\forall a_1, a_2 \in \mathbb{Z}, \quad m_1, m_2 \in \mathbb{Z}^+$

If $\gcd(m_1, m_2) = 1$,

Then $\quad n \equiv a_1 \pmod{m_1}$
$\quad\quad n \equiv a_2 \pmod{m_2}$

$\rightarrow \quad n \equiv \underbrace{n_0}_{\text{unique}} \pmod{m_1 m_2}$ is a unique solution

ep. $n \equiv 8 \pmod{15}$ $\quad n \equiv 5 \pmod 7$

$\because \gcd(15, 7) = 1$ $\quad \therefore n \equiv 68 \pmod{105}$

☆ proof.

$\because \gcd(m_1, m_2) = 1$.

$\therefore$ sols of $n \equiv a_1 \pmod{m_1}$ is $\{a_1 + m_1 x : x \in \mathbb{Z}\}$

存在 $n \equiv a_2 \pmod{m_2} \Leftrightarrow m_1 x \equiv a_2 - a_1 \pmod{m_2}$

$\because$ LCT & def of congruence and divisibility

$\therefore$ sols of $m_1 x \equiv a_2 - a_1 \pmod{m_2}$ is $\{m_2 y + x_0 : y \in \mathbb{Z}\}$

$\because x = m_2 y + x_0$

$\therefore \{m_1(m_2 y + x_0) + a_1 : y \in \mathbb{Z}\} = \{m_1 m_2 y + (m_1 x_0 + a_1) : y \in \mathbb{Z}\}$

congruence class $[n_0]$ in $\mathbb{Z}_{m_1 m_2}$.

$n_0 = m_1 x_0 + a_1$ is a sol

ex. solve $x \equiv 5 \pmod{6}$
$x \equiv 2 \pmod{7}$
$x \equiv 3 \pmod{11}$

→ 先解 $x \equiv 2 \pmod{7}$ $\quad$ $x \equiv 3 \pmod{11}$

∵ $\gcd(7, 11) = 1$ $\quad$ by CRT, there is one sol. (mod 77)

$x \equiv 3 \pmod{11}$ : $x = 3, 14, 25, 36, 47, 58, 69.$

$58 \equiv 3 \pmod{11}$ $\quad$ $58 \equiv 2 \pmod{7}$

∴ By CRT, the complete sol is $x \equiv 58 \pmod{77}$

→ 再解 $x \equiv 5 \pmod{6}$ $\quad$ $x \equiv 58 \pmod{77}$

∵ $x \equiv 58 \pmod{77}$ $\quad$ ∴ $x = 58 + 77k$ $\quad$ $k \in \mathbb{Z}$

代入 $x \equiv 2 \pmod{7}$ $\quad$ $58 + 77k \equiv 5 \pmod{4}$
$4 + 5k \equiv 5 \pmod{4}$
$5k \equiv 1 \pmod{6}$

→ $k = 5$ is a sol.

By LCT, complete sol is $k \equiv 5 \pmod{6}$

∴ $k = 5 + 6s$ $\quad$ $(s \in \mathbb{Z})$

$x = 58 + 77k = 58 + 77 \times (5 + 6s) = 443 + 462s$

∴ complete sol is $x \equiv 443 \pmod{462}$

$\uparrow$
$4 \times 7 \times 11$

- Generalized Chinese Remainder Theorem (GCRT.)

$k, m_1, m_2 \cdots m_k \in \mathbb{Z}^+$. $a_1, a_2 \cdots a_k \in \mathbb{Z}$

If $\gcd(m_i, m_j) = 1 \quad \forall i \neq j$

Then $\{n : n \equiv a_1 \pmod{m_1},\ n \equiv a_2 \pmod{m_2} \cdots n \equiv a_k \pmod{m_k}\}$

$= \{n : n \equiv n_0 \pmod{m_1 \cdot m_2 \cdots m_k}\}$

ex. solve $3x \equiv 2 \pmod 5$
$2x \equiv 6 \pmod 7$

$\because \gcd(2,7) = 1$

$\therefore$ By CD & CAM, $2x \equiv 6 \pmod 7 \Rightarrow x \equiv 3 \pmod 7$

$3x \equiv 2 \pmod 5$ has unique sol $x \equiv 4 \pmod 5$

$\therefore$ equivalent to solving $x \equiv 4 \pmod 5$
$x \equiv 3 \pmod 7$

$\hookrightarrow 3, 10, 17, 24, \cdots$

$x = 24$ is a sol

$\because \gcd(5,7) = 1$

$\therefore$ By CRT, complete sol is $x \equiv 24 \pmod{35}$

ex. solve $x \equiv 1 \pmod 6$
$x \equiv 1 \pmod 8$

$\gcd(6,8) = 2 \neq 1 \quad \therefore$ CRT don't apply

$\because x \equiv 1 \pmod 8 \quad \therefore x = 1 + 8k \quad k \in \mathbb{Z}.$

代入 $x \equiv 1 \pmod 6 \qquad 1 + 8k \equiv 1 \pmod 6$
$8k \equiv 0 \pmod 6$

By LCT, $\because \gcd(8,6) = 2 \quad 2 \mid 0. \quad \therefore$ there are 2 sols $\pmod 6$

They are $k \equiv 0 \pmod 6 \quad k \equiv 3 \pmod 6$

$\therefore k = 6s$ or $k = 3 + 6s \quad s \in \mathbb{Z}.$

$x = 1 + 8k = 1 + 8 \cdot 6s = 1 + 48s$ or $x = 1 + 8k = 1 + 8(3 + 6s) = 25 + 48s$

sols are $x \equiv 1 \pmod{48}$ or $x \equiv 25 \pmod{48}$

# 8.9 Splitting a Modulus

## - Splitting Modulus Theorem (SMT)

$\forall a \in \mathbb{Z}$. $m_1, m_2 \in \mathbb{Z}^+$

$\gcd(m_1, m_2) = 1 \Rightarrow \begin{cases} n \equiv a \pmod{m_1} \\ n \equiv a \pmod{m_2} \end{cases} \equiv n \equiv a \pmod{m_1 m_2}$

proof. Assume $\gcd(m_1, m_2) = 1$.

$\therefore$ Due to CRT, $n \equiv n \pmod{m_1 m_2}$ $n_0$ is a particular sol.

Let $n_0 = a$.

$\because a \equiv a \pmod{m_1}$ $a \equiv a \pmod{m_2}$

$\therefore n \equiv a \pmod{m_1 m_2}$

ex. determine remainder when $8^{97}$ divided by 55

相当于解 $8^{97} \equiv x \pmod{55}$ by CRT

By SMT, $\because \gcd(5, 11) = 1$

$\therefore$ 相当于解 $8^{97} \equiv x \pmod{5}$ $8^{97} \equiv x \pmod{11}$

$\downarrow$ $\downarrow$

$x \equiv 7 \pmod{11}$ $x \equiv 3 \pmod{5}$

By inspection $x \equiv 18 \pmod{55}$ $\therefore 8^{97}$ has remainder 18.

# 9.1 Public-Key Cryptography

## - Private-Key

key management problem : every pair of users needs to share a different private key.

100人互相发消息 → $\binom{100}{2} = 4950$ keys

key distribution problem : How to safely transmit

## - RSA

# 9.2 Implementing RSA Scheme

(a) Setting up RSA

(b) RSA Encryption

(c) RSA Decryption

The three stages are described below.

---

**(a) Setting up RSA:** To set up the RSA encryption scheme, Bob does the following.

1. Randomly choose two large, distinct primes $p$ and $q$ and let $n = pq$.
2. Select an arbitrary integer $e$ so that $\gcd(e, (p-1)(q-1)) = 1$ and $1 < e < (p-1)(q-1)$.
3. Solve the congruence
$$ed \equiv 1 \pmod{(p-1)(q-1)}$$
for an integer $d$ where $1 < d < (p-1)(q-1)$.
4. Publish the public key $(e, n)$.
5. Keep secret the private key $(d, n)$, and the primes $p$ and $q$.

**(b) RSA Encryption:** To encrypt a message as ciphertext and send securely to Bob, Alice does the following.

1. Obtain an authentic copy of Bob's public key $(e, n)$.
2. Construct the plaintext message $M$, an integer such that $0 \le M < n$.
3. Encrypt $M$ as the ciphertext $C$, given by
$$C \equiv M^e \pmod{n} \text{ where } 0 \le C < n.$$
4. Send $C$ to Bob.

**(c) RSA Decryption:** To decrypt the ciphertext received from Alice, Bob does the following.

1. Use the private key $(d, n)$ to decrypt the ciphertext $C$ as the received message $R$, given by
$$R \equiv C^d \pmod{n} \text{ where } 0 \le R < n.$$
2. *Claim:* The received message $R$ equals the original plaintext message $M$, i.e., $R = M$.

---

## 9.3 Proving RSA Scheme Works

### - RSA

$\forall$ p. q. n. e. d. M. C. & R.

If 1. p & q are distinct primes

2. $n = pq$

3. e & d are positive integers s.t. $ed \equiv 1 \pmod{(p-1)(q-1)}$

and $1 < e, d < (p-1)(q-1)$

4. $0 \le M < n$.

5. $M^e \equiv C \pmod{n}$ $\quad 0 \le C < n$

6. $C^d \equiv R \pmod{n}$ $\quad 0 \le R < n$.

Then $R \equiv M$

proof.

$$R \overset{6}{\equiv} C^d \overset{5}{\equiv} (M^e)^d \equiv M^{ed} \pmod{pq}$$

By SMT, equivalent to solve $\begin{cases} M^{ed} \pmod{p} \\ M^{ed} \pmod{q} \end{cases}$

对于

① $p \mid M$.

$M \equiv 0 \pmod{p}$ $\qquad R \equiv 0^{ed} \equiv 0 \pmod{p}$

# 10.1 Standard Form

- def.

$i^2 = -1$

$$\mathbb{C} = \{ \underset{\substack{\uparrow \\ \text{Re} \\ \text{real part}}}{x} + \underset{\substack{\uparrow \\ \text{Im} \\ \text{imaginary part}}}{y} i : x, y \in \mathbb{R} \}$$

- Addition

Let $z = a+bi$ $\quad w = c+di$ $\quad z+w = (a+c) + (b+d)i$

Additive Identity $\quad z+0 = (x+yi) + (0+0i) = z \to 0$ is additive identity

Additive Inverse $\quad z + (-1)z = 0 \quad \to -z$ is additive inverse

- Multiplication

Let $z = a+bi$ $\quad w = c+di$ $\quad zw = (ac-bd) + (ad+bc)i$

Multiplication Identity $\quad z \cdot 1 = (x+yi)(1+0i) = x+yi = z \quad \to 1$ is m-id

Multiplication Inverse $\quad z \cdot z^{-1} = 1$

$$z^{-1} = \frac{1}{z} = \frac{1}{a+bi} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i = \frac{a-bi}{a^2+b^2}$$

ex. $(1+2i)^{-1} = \frac{1-2i}{1^2+2^2} = \frac{1}{5} - \frac{2}{5} i$

- Properties of complex arithmetic (PCA)

① associativity of addition : $(u+v)+z = u + (v+z)$

② commutativity of addition : $u+v = v+u$

③ additive identity : $0 = 0+0i \quad \to \quad z+0 = z$

④ additive inverse : $z + (-z) = 0 \qquad z = a+bi \qquad -z = -a-bi$

⑤ associativity of multiplication : $(uv)z = u(vz)$

⑥ commutativity of multiplication : $uv = vu$

⑦ multiplicative inverses : $1 = 1+0i \quad \to \quad z \cdot 1 = z$

⑧ multiplicative inverses: $z \cdot z^{-1} = 1$. $(z = a+bi \neq 0)$ $z^{-1} = \frac{a-bi}{a^2+b^2}$

⑨ distributivity: $z(u+v) = zu + zv$.

满足以上9个条件的: $\mathbb{C}$ (a kind of field)

* Field 包含: $\mathbb{R}$. $\mathbb{Z}_p$. $\mathbb{Q}$

不包含: $\mathbb{Z}_m$ (m 不是 prime)

ex. 解 $6z^3 + (1+3\sqrt{2}i)z^2 - (11-2\sqrt{2}i)z - 6 = 0$

suppose $r \in \mathbb{R}$ is a solution

$6r^3 + (1+3\sqrt{2}i)r^2 - (11-2\sqrt{2}i)r - 6 = 0$

$(6r^3 + r^2 - 11r - 6) + (3\sqrt{2}r^2 + 2\sqrt{2}r)i = 0 + 0i$

$$\begin{cases} 6r^3 + r^2 - 11r - 6 = 0 \\ 3\sqrt{2}r^2 + 2\sqrt{2}r = 0 \end{cases}$$

$r = 0$ $r = -\frac{2}{3}$

$r = 0$ $6r^3 + r^2 - 11r - 6 = -6 \neq 0$

$r = -\frac{2}{3}$ $6r^3 + r^2 - 11r - 6 = 0$ ✓

# 10.2 Conjugate and Modulus

- def. conjugate $\bar{z}$

$z = x + yi \qquad \bar{z} = x - yi$

- Properties of conjugate (PCJ)

① $\overline{(\bar{z})} = z$

② $\overline{z+w} = \bar{z} + \bar{w}$

③ $z + \bar{z} = 2Re(z) \qquad z - \bar{z} = 2Im(z)i$

④ $\overline{zw} = \bar{z} \cdot \bar{w}$

⑤ $z \neq 0 \qquad \overline{(z^{-1})} = (\bar{z})^{-1}$

- def. modulus $|z|$

$z = x + yi \qquad |z| = \sqrt{x^2 + y^2}$

- Properties of Modulus (PM)

① $|z| = 0 \iff z = 0$

② $|\bar{z}| = |z|$

③ $\bar{z} \cdot z = |z|^2$

④ $|zw| = |z||w|$

⑤ $z \neq 0, \Rightarrow |z^{-1}| = |z|^{-1}$

proof ③: $\bar{z} \cdot z = (a-bi)(a+bi) = a^2 + b^2 = |z|^2$

proof ④: $|zw| = (z \cdot w) \cdot (\overline{zw})$ PM3

$= (zw)(\bar{z} \cdot \bar{w})$ PCJ 2

$= (z\bar{z})(w\bar{w})$ DCA

$= |z|^2 |w|^2$ by PM3

$\because |zw|^2$ & $|z|^2|w|^2$ are non-negative real numbers.

$\therefore$ we can take square roots:

$|zw| = |z||w| \qquad |zw| = -|z||w|$ (X)

$\because |zw| \geq 0. \qquad |z||w| \geq 0.$

$\therefore |zw| = |z||w|$

ex. Let $z, w \in \mathbb{C}$. Prove $|z+w|^2+|z-w|^2=2|z|^2+2|w|^2$

Proof. Let $z, w \in \mathbb{C}$

$$|z+w|^2+|z-w|^2$$
$$= (z+w)(\overline{z+w}) + (z-w)(\overline{z-w}) \quad \text{by PM}$$
$$= (z+w)(\bar z+\bar w) + (z-w)(\bar z-\bar w) \quad \text{by PCJ}$$
$$= z\cdot\bar z + z\bar w + \bar z w + w\bar w + z\bar z - z\bar w - \bar z w + w\bar w$$
$$= 2z\bar z + 2w\bar w$$
$$= 2|z|^2 + 2|w|^2 \quad \text{by PM}$$

- Corollary

$$\overline{z_1+z_2+\cdots+z_n} = \bar z_1 + \bar z_2 + \cdots + \bar z_n$$
$$\overline{z_1\cdot z_2\cdots z_n} = \bar z_1\cdot\bar z_2\cdots\bar z_n$$
$$|z_1\cdot z_2\cdots z_n| = |z_1||z_2|\cdots|z_n|$$

- Triangle Inequality (TIQ)

$\forall z, w \in \mathbb{C}$. we have $|z+w| \le |z|+|w|$

proof:

Let $z=x+yi$ $\quad w=u+vi$

$-w=-u-vi \quad z+w=z-(-w)=(x-(-u))+(y-(-v))i$

$|z+w|=|z-(-w)|=\sqrt{(x-(-u))^2+(y-(-v))^2}$

let $A(0,0)$ $\quad B(z):(x,y)$ $\quad C(-w):(-u,-v)$

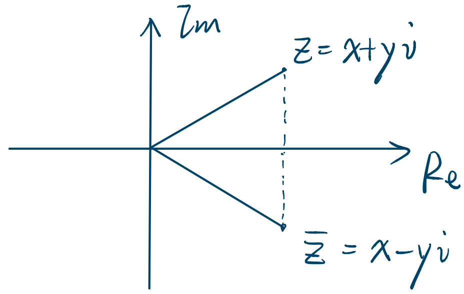
已知，在$\triangle ABC$中， $l_{BC} \le l_{AB}+l_{AC}$

$\because$ By Pythagorean Theorem. $l_{AB}=|z|$, $l_{AC}=|-w|=|w|$, $l_{BC}=|z-(-w)|=|z+w|$

$\therefore |z+w| \le |z|+|w|$

# 10.3 The Complex Plane and Polar Form

- def. Argand plane




← "complex plane" / "Argand plane"

- Cartesian form $z = x + yi$
- Cartesian coordinates $(x, y)$
- polar form $z = r(\cos\theta + i\sin\theta)$

$(r \geq 0,\ r = |z| = \sqrt{x^2+y^2})$ $\theta = \frac{y}{x}$ argument of $z$

- polar coordinates $(r, \theta)$

ep. cartesian form: $z = -3\sqrt{2} + 3\sqrt{6}i$

cartesian coordinates: $(-3\sqrt{2}, 3\sqrt{6})$

polar coordinates: $r = \sqrt{x^2+y^2} = 6\sqrt{2}$ $\tan\theta = \frac{y}{x} = \frac{3\sqrt{6}}{-3\sqrt{2}} = -\sqrt{3}$ $\theta = \frac{2\pi}{3}$

$(6\sqrt{2}, -\sqrt{3})$

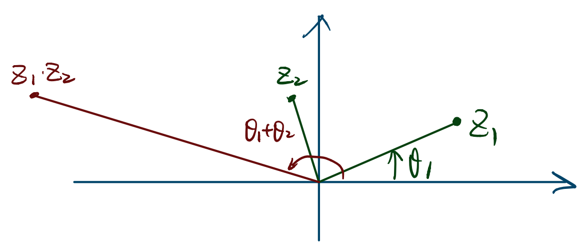
polar form: $r(\cos\theta + i\sin\theta) = r(\cos(\theta+2k\pi) + i\sin(\theta+2k\pi))$

- Polar Multiplication in $\mathbb{C}$ (PMC)

$z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$ $z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$

$z_1 z_2 = r_1 r_2 (\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2))$

ex. calculate $(1-i)\times(-1+i)$




polar form: $1-i = \sqrt{2}\left(\cos\left(\frac{7\pi}{4}\right) + i\sin\left(\frac{7\pi}{4}\right)\right)$

$1+i = \sqrt{2}\left(\cos\left(\frac{3\pi}{4}\right) + i\sin\left(\frac{3\pi}{4}\right)\right)$

$(1+i)(1-i) = \sqrt{2}\cdot\sqrt{2}\left(\cos\frac{5\pi}{2} + i\sin\frac{5\pi}{2}\right)$

$= 2(0+i)$

$= 2i$

$(1-i)(-1+i) = -1+i+i-i^2 = 2i$

# 10.4 De Moivre's Theorem

## - De Moivre's Theorem (DMT)

$\theta \in \mathbb{R}$. $n \in \mathbb{Z}$. $(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$

ex. compute $\left(-\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} i\right)^{-1000}$

write in polar form. $r = \sqrt{\left(-\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2} = 1$

$\tan\theta = \frac{\frac{1}{\sqrt{2}}}{-\frac{1}{\sqrt{2}}} = -1$ $\quad \therefore \theta = \frac{3\pi}{4}$

$$\begin{aligned}\therefore \left(-\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} i\right)^{-1000} &= \left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right)^{-1000} \\ &= \cos\left(-1000\cdot\frac{3\pi}{4}\right) + i\sin\left(-1000\cdot\frac{3\pi}{4}\right) \quad \text{by DMT} \\ &= 1 + 0i \\ &= 1\end{aligned}$$

## - Corollary to DMT.

$\forall z \in \mathbb{C}$, $z = r(\cos\theta + i\sin\theta)$ $\quad z^n = r^n(\cos n\theta + i\sin n\theta)$

For $z \in \mathbb{C}$. $z = r(\cos\theta + i\sin\theta)$.

* when $z = 0$ $\quad z^{-1}$ DNE

# 10.5 Complex n-th Roots

- def. complex $n^{th}$ roots of a

  $a \in \mathbb{C}$ $\quad n \in \mathbb{N}^+$ $\quad z^n = a$

  $z$ is complex $n^{th}$ roots of a

ex. Find complex $6^{th}$ roots of $-64$.

cartesian form $z^6 = -64$

polar form. $-64 = 64(\cos\pi + i\sin\pi)$

by DMT. $z^6 = r^6(\cos 6\theta + i\sin 6\theta)$

$\therefore r^6(\cos 6\theta + i\sin 6\theta) = 64(\cos\pi + i\sin\pi)$

$r^6 = 64 \quad r = 2$

$6\theta = \pi + 2k\pi \quad \theta = \frac{\pi}{6} + \frac{k\pi}{3}$

$\theta = \frac{\pi}{6}, \frac{3\pi}{6}, \frac{5\pi}{6}, \frac{7\pi}{6}, \frac{9\pi}{6}, \frac{11\pi}{6}, \cancel{\frac{13\pi}{6}} \left(= \frac{\pi}{6}\right)$

$\therefore$ sols are:

$z_0 = 2(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}) = \sqrt{3} + i$

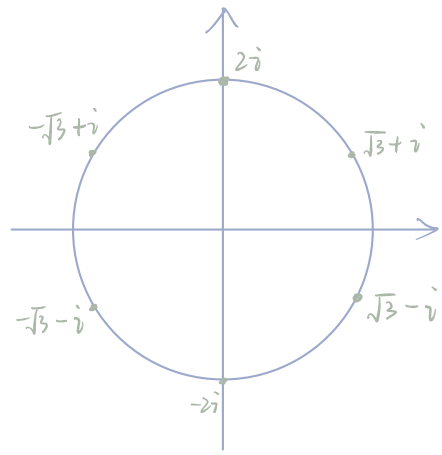
$z_1 = 2(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}) = 2i$

$z_2 = 2(\cos\frac{5\pi}{6} + i\sin\frac{5\pi}{6}) = -\sqrt{3} + i$

$z_3 = 2(\cos\frac{7\pi}{6} + i\sin\frac{7\pi}{6}) = -\sqrt{3} - i$

$z_4 = 2(\cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2}) = -2i$

$z_5 = 2(\cos\frac{11\pi}{6} + i\sin\frac{11\pi}{6}) = \sqrt{3} - i$




- Complex n-th Roots Theorem (CNRT)

  $\forall a \in \mathbb{C}$. $a = r(\cos\theta + i\sin\theta)$. $n \in \mathbb{N}$.

  the complex n-th roots of a are: $\sqrt[n]{r}\left(\cos\left(\frac{\theta + 2k\pi}{n}\right) + i\sin\left(\frac{\theta + 2k\pi}{n}\right)\right) \quad k = 0, 1, \cdots, n-1$

① 所有非0复数有n个不同的 $n^{th}$ root.

② roots lie on a circle. 半径: $\sqrt[n]{r}$. uniformly spaced out of angle $\frac{2\pi}{n}$

③ proof: pg. 174-175.

ex. solve $z^8=1$ for $z \in \mathbb{C}$ (use CNRT)

By inspection $z=1$ is a sol.

By CNRT, there are 8 solutions.

and solutions lies on circle with radius 1.

uniformly spaced out by angle $\frac{2\pi}{8} = \frac{\pi}{4}$

$\therefore$ solutions are:

$z_0 = 1$

$z_1 = 1 \times (\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}) = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$

$z_2 = 1 \times (\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}) = -\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$

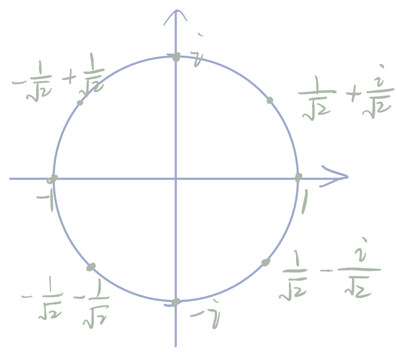
$z_3 = \cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4} = -\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$

$z_4 = \cos\pi + i\sin\pi = -1$

$z_5 = \cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4} = -\frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}$

$z_6 = \cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2} = -i$

$z_7 = \cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4} = \frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}$




ex. solve $z^4 = -27\bar{z}$ (CNRT don't apply) 因为r是负数

let $z = r(\cos\theta + i\sin\theta)$

$z^4 = r^4(\cos 4\theta + i\sin 4\theta)$ by PMT

$\bar{z} = r(\cos\theta - i\sin\theta)$

$-27 = 27(\cos\pi + i\sin\pi)$

$z^4 = -27\bar{z}$ is equivalent to

$r^4(\cos 4\theta + i\sin 4\theta) = 27(\cos\pi + i\sin\pi) \cdot r(\cos\theta - i\sin\theta)$

$= 27r(\cos(\pi-\theta) + i\sin(\pi-\theta))$ by PMC

$r^4 = 27r \quad r(r^3-27) = 0 \quad \Rightarrow \quad r=0 \quad r=3.$

$4\theta = \pi - \theta + 2k\pi \quad \theta = \frac{\pi}{5} + \frac{2k\pi}{5}$

$\therefore$ sols are:

$z_0 = 3(\cos\frac{\pi}{5} + i\sin\frac{\pi}{5})$

$z_1 = 3(\cos\frac{3\pi}{5} + i\sin\frac{3\pi}{5})$

$z_2 = 3(\cos\frac{5\pi}{5} + i\sin\frac{5\pi}{5}) = -3$

$z_3 = 3(\cos\frac{7\pi}{5} + i\sin\frac{7\pi}{5})$

$z_4 = 3(\cos\frac{9\pi}{5} + i\sin\frac{9\pi}{5})$

$z_5 = 0$

# 10.6 Square Roots and quadratic formula

## - Quadratic Formula (QF)

$\forall a, b, c \in \mathbb{C}$, $a \neq 0$. sol of $az^2 + bz + c = 0$ are

$$z = \frac{-b \pm w}{2a}$$

where $w$ is a sol to $w^2 = b^2 - 4ac$

ex. solve $z^2 - 2z + 1 + 8i = 0$ $z \in \mathbb{C}$

by quadratic formula. $z = \frac{-(-2) \pm w}{2 \cdot 1}$ $w^2 = (-2)^2 - 4 \cdot 1 \cdot (1+8i) = -32i$

let $w = a + bi$

$a^2 + 2abi - b^2 = -32i$

$\begin{cases} a^2 - b^2 = 0 \\ 2ab = -32 \end{cases}$ $\begin{cases} a = 4 \\ b = -4 \end{cases}$ $\begin{cases} a = -4 \\ b = 4 \end{cases}$

solutions are $z = \frac{2 \pm (4 - 4i)}{2}$ $z = 3 - 2i$ $z = -1 + 2i$

# 11.1 Introduction of polynomials

## - field $\mathbb{F}$

where the coefficients will always come from a special type

- the rational numbers $\mathbb{Q}$,
- the real numbers $\mathbb{R}$,
- the complex numbers $\mathbb{C}$,
- the integers modulo a prime $\mathbb{Z}_p$.

## - Important property of field

$\forall \mathbb{F}, \forall a, b \in \mathbb{F}. \quad ab = 0 \Rightarrow a = 0$ or $b = 0$

$\forall \mathbb{F}, \forall a, b \in \mathbb{F} \quad a \neq 0$ and $b \neq 0 \Rightarrow ab \neq 0$ ( contrapositive )

## - def.

polynomial in $x$ over the field $\mathbb{F}$:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \qquad (n \geq 0, n \in \mathbb{Z})$$

$x \rightarrow$ indeterminate

$a_0, a_1 \cdots a_n \rightarrow$ element

$a_i \rightarrow$ coefficient

$a_i x^i \rightarrow$ term.

largest power of $x \rightarrow$ degree

分类 $\begin{cases} \text{complex polynomial / polynomial over } \mathbb{C} & \text{带 } \mathbb{C} \text{ in} \\ \text{real polynomial} & \text{实数} \\ \text{rational polynomial} & \text{有理数} \end{cases}$

$\begin{cases} \text{zero} \sim \\ \text{constant} \sim \end{cases} \begin{cases} \text{linear} \sim \\ \text{quadratic} \sim \\ \text{cubic} \sim \\ \cdots \end{cases}$

# 11.2 Arithmetic with Polynomials

Let $f(x) = \sum_{i=0}^{m} a_i x^i$ $\quad g(x) = \sum_{j=0}^{n} b_j x^j$ be polynomials over $\mathbb{F}[x]$

## - Addition

$$f(x) + g(x) = \sum_{k=0}^{\max\{m,n\}} (a_k + b_k) x^k \qquad \begin{cases} k > m & a_k = 0 \\ k > n & b_k = 0 \end{cases}$$

## - Multiplication

$$f(x) g(x) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_i b_j x^{i+j} = \sum_{l=0}^{m+n} c_l x^l$$

$$c_l = a_0 b_l + a_1 b_{l-1} + \cdots + a_l b_0 = \sum_{i=0}^{l} a_i b_{l-i}$$

## - Degree of a Product (DP)

$\forall \mathbb{F}$. $f(x)$ & $g(x)$ are non-zero polynomials in $\mathbb{F}[x]$.

$$\deg f(x) g(x) = \deg f(x) + \deg g(x)$$

## - Division Algorithm for Polynomials (DAP)

$\forall \mathbb{F}$. $f(x)$ & $g(x)$ are polynomials in $\mathbb{F}[x]$. $g(x)$ non-zero

$\exists$ unique $q(x)$ & $r(x)$ in $\mathbb{F}[x]$ s.t.:

$$f(x) = \underbrace{q(x)}_{\text{quotient}} g(x) + \underbrace{r(x)}_{\text{remainder}}$$

$r(x)$ is zero polynomial . $\deg r(x) < \deg g(x)$

ex. Prove $(x-1) \nmid x^2+1$ in $\mathbb{R}[x]$

proof: Assume, for sake of contradiction, $x-1 \mid x^2+1$

then $\exists q(x) \in \mathbb{R}[x]$ s.t. $x^2+1 = q(x)(x-1)$

By DP, $\deg(q(x)) = 1$ So $q(x) = ax+b$ for some $a, b \in \mathbb{R}$

$x^2+1 = (ax+b)(x-1) = ax^2 - ax + bx - b$

comparing coefficients:

$x^2$ : $1=a$

$x'$ : $0=-a+b$

$x^0$ : $b=-1$

for sub in $x'$, $0=-2$ contradicts.

$\therefore$ Statement is true

ex. Prove $(x-1)\nmid(x^2+1)$ in $\mathbb{R}[x]$. Use PAP to find $q(x)$ & $r(x)$

长除法.

$$
\begin{array}{r|l}
 & x+1 \\
\cline{2-2}
x-1 & x^2+0x+1 \\
 & x^2-x \\
\cline{2-2}
 & x+1 \\
 & x-1 \\
\cline{2-2}
 & 2
\end{array}
$$

synthetic division

$$
\begin{array}{c|ccc}
1 & 1 & 0 & 1 \\
 & \downarrow & 1 & 1 \\
\hline
 & \underbrace{1 \quad 1}_{\text{coefficient of quotient}} & & 2
\end{array}
$$

← 余数

C 中可以用长除法

# 11.3 Polynomials

## - Remainder Theorem (RT)

$\forall \mathbb{F}, \quad \forall f(x) \in \mathbb{F}[x], \quad \forall c \in \mathbb{F}.$

$f(x) \div (x-c)$ ------ $f(x)$ 中 no constant

proof:

Let $\mathbb{F}$ be a field, $f(x) \in \mathbb{F}[x]$, $c \in \mathbb{F}$.

By DAP, there exist unique $q(x), r(x) \in \mathbb{F}[x]$.

s.t $f(x) = q(x)(x-c) + r(x)$

where $r(x) = 0$ or $\deg(r(x)) < \deg(x-c)$

Thus $r(x) = 0$ or $\deg(r(x)) = 0$

$\therefore$ $r(x)$ is constant. Let $r(x) = r_0$ where $r_0$ is constant $\mathbb{F}$.

Thus $f(x) = q(x)(x-c) + r_0$

substituting $x = c$: $f(c) = q(c)(c-c) + r_0 = r_0$

$\therefore$ remainder is constant of $f(c)$

ex. remainder of $f(x) = 4x^3 + 2x + 5 \div (x+6)$ is ?

By RT. remainder $= f(-6) = -871$

## - Factor Theorem (FT)

$\forall f(z) \in$ complex polynomials. $\deg f(z) \geq 1$.

$\exists z_0 \in \mathbb{C}$. s.t. $f(z_0) = 0$

## - def. Reducible / Irreducible

reducible polynomial: 可拆成2个 polynomial 相乘的形式

ep. $f(x) = x^2 + 1$ is irreducible in $\mathbb{R}[x]$.

is reducible in $\mathbb{C}[x]$ $\quad (x-i)(x+i)$

## - def. Multiplicity

The multiplicity of root $c$ of polynomial $f(x)$ is the largest positive integer $k$. s.t. $(x-c)^k$ is a factor of $f(x)$

ex. $h(x) = x^4 + 2x^2 + 1. = (x-i)^2(x+i)^2$

$\therefore$ $i$ & $-i$ are roots of $h(x)$ with multiplicity 2.

## - Fundamental Theorem of Algebra (FTA)

$\forall f(z) \in$ complex polynomials, $\deg f(z) \geq 1$.

$\exists z_0 \in \mathbb{C}$. s.t $f(z_0) = 0$

"Every non-constant polynomial $f(z) \in \mathbb{C}[x]$ has a root in $\mathbb{C}$"

## - Complex Polynomials of degree n have n roots (CPN)

$\forall n \in \mathbb{Z}$. $n \geq 1$. $\forall f(z) \in$ complex polynomials

$\exists c \in \mathbb{C}$ $(c \neq 0)$. s.t.

$$f(z) = c(z-c_1)(z-c_2)\cdots(z-c_n)$$

roots of $f(z)$ : $c_1$. $c_2$. $\cdots$. $c_n$

ex. write $f(x) = ix^3 + (3-i)x^2 + (-3-2i)x - 6$ as a product of irreducible polynomials in $\mathbb{C}[x]$ (hint: $-1$ is a root)

$\because$ $-1$ is a root of $f(x)$

$\therefore$ by FT. $x+1 \mid f(x)$

$$\begin{array}{r|rrrr} -1 & i & 3-i & -3-2i & -6 \\ & & -i & -3+2i & 6 \\ \hline & i & 3-2i & -6 & 0 \end{array}$$

remainder.

$\therefore f(x) = (x+1)(ix^2 + (3-2i)x - 6)$

roots of $ix^2 + (3-2i)x - 6$ are $x = \dfrac{-b \pm w}{2a}$ where $w^2 = b^2 - 4ac$

So, $x = \frac{-(3-2i) \pm w}{2i}$

$w^2 = (3-2i)^2 - 4i(-6) = 9 - 12i + 4i^2 + 24i = 5 + 12i$

$w = \pm(3+2i)$

$\therefore\ x = \frac{-(3-2i) \pm (3+2i)}{2i} \rightarrow x = \frac{4i}{2i} = 2$

$x = \frac{-6}{2i} = 3i$

$f(x) = i(x+1)(x-2)(x-3i)$ ← 确认最高次是否带 i

## - Proposition 7.

For all integer $\mathbb{F}$, all integers $n \geq 1$. and all $f(x) \in \mathbb{F}[x]$ of degree $n$. The polynomial $f(x)$ has at most $n$ roots

最高次数为 n → 最多有 n 个 root

# 11.4 Real Polynomials and the Conjugat Root Theorem

## - Conjugate Roots Theorem (CJRT)

$\forall f(x) \in$ polynomial with real coefficient.

$c \in \mathbb{C}$ is a root of $f(x)$ $\Rightarrow$ $\bar{c} \in \mathbb{C}$ is a root of $f(x)$

会同时有 $x+iy$ 与 $x-iy$ 两个根

## - Real Quadratic Factors (RQF)

$\forall f(x) \in$ polynomials with real coefficients.

$c \in \mathbb{C}$ is a root of $f(x)$. $Im(c) \neq 0$

$\Rightarrow \exists\, g(x) \in$ real quadratic polynomial. $q(x) \in$ real polynomial

s.t $f(x) = g(x)\, q(x)$.

$*$ $g(x)$ is irreducible in $\mathbb{R}[x]$

## - Real Factors of Real Polynomials (RFRP)

$\forall f(x) \in$ positive polynomials. $f(x)$ 可写成 linear 与 quadratic 的乘积

## - Rational Roots Theorem (RRT)

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0. \quad n \geq 1.$$

$\frac{p}{q}$ is a rational root, $\gcd(p, q) = 1$. $\Rightarrow p \mid a_0 \wedge q \mid a_n$.