Q : ① Today is Thursday.

What day is it in 100 days?

What day is it in 10^{20} days?

② Let $x \in \mathbb{R}\setminus\{0\}$. Define $\bar{x}$ to be a nonzero real number such that $\bar{x} \cdot x = 1$.

1) What is $\bar{2}$?

2) What's $\overline{0.5}$?

3) What have you known $\bar{x}$ as ?

unofficial resource: Discrete Mathematics and Applications by Kenneth Rosen.

GOOD NEWS ★ GOOD NEWS ★ GOOD NEWS

We'll only work with $\mathbb{Z}$ from $\boxed{\text{Lec 8 to Lec 10}}$.

1. Primes and gcd

Recall: Given $a, b \in \mathbb{Z}$, $a \neq 0$, we say a divides b, written $a \mid b$, if $\exists\, c \in \mathbb{Z}$, s.t. $ac = b$.

Def Let $a, b \in \mathbb{Z}$, not both zero. The largest $d \in \mathbb{Z}$ s.t. $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b, denoted $\gcd(a,b)$.

Question: Given such a and b, how do we find $\gcd(a,b)$?

Thm (Fundamental Theorem of Arithmetic) Every integer ≥ 2 can be uniquely written as a product of primes.

Algorithm. If $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ are prime factorization, then $\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_k^{\min(a_k,b_k)}$

E.g. $120 = \boxed{2^3 \cdot 3 \cdot 5}$ and $500 = 2^2 \cdot 5^3 \cdot 3^0$

$\Rightarrow \gcd(120, 500) = 2^2 \cdot 3^0 \cdot 5^1 = 20$

$$\begin{array}{r|l} \cdot 2 & 120 \\ \cdot 2 & 60 \\ \cdot 2 & 30 \\ \cdot 3 & 15 \\ & \cdot 5 \end{array}$$

Rem. But prime factorization is very hard (no efficient algorithm is known). Find $\gcd(91, 287)$.

Lem Let $a = bq + r$, where $a, b, q, r \in \mathbb{Z}$.

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

Pf: [exercise in discussion]

Thm (The Division Algorithm) Let $a, d \in \mathbb{Z}$ and $a > 0$.

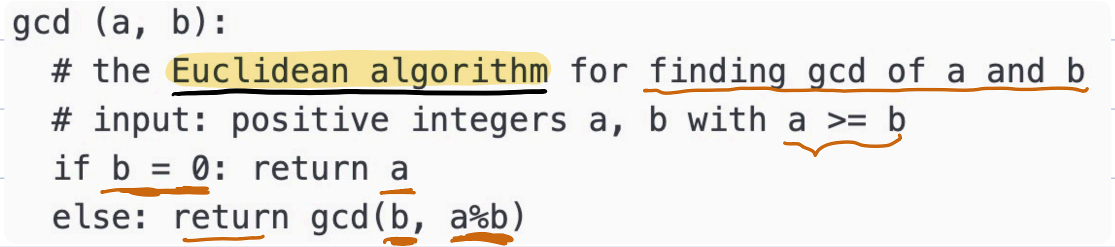
Then there are unique $q, r \in \mathbb{Z}$ with $0 \leq r < d$,

such that $a = qd + r$

in real world in lecture.

Here, r is the ~~remainder~~ remainder, written a mod d or a % d.

Algorithm.



```
gcd (a, b):
  # the Euclidean algorithm for finding gcd of a and b
  # input: positive integers a, b with a >= b
  if b = 0: return a
  else: return gcd(b, a%b)
```

$<a$ $<b$.

E.g. Find gcd(287, 91).

$\overset{a}{287} = \overset{b}{91} \times 3 + 14$

$91 = 14 \times 6 + 7$

$14 = \underset{a}{\underset{\shortparallel}{7}} \times 2 + \underset{b}{\underset{\shortparallel}{0}}$ $\Rightarrow \gcd(287, 91) = 7.$

Thm (Bezout's theorem) If $a, b \in \mathbb{Z}^{+}$, then there exist coefficients $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = sa + tb$.

Algorithm: Run Euclidean algorithm backwards to get the coefficients. This is called the **extended Euclidean algorithm**.

E.g. Write gcd(287, 91) as a linear combination of 287 and 91.

$$\left\{\begin{aligned} \boxed{287} &= \boxed{91} \times 3 + 14 \\ 91 &= 14 \times 6 + \boxed{7} \\ 14 &= 7 \times 2 + 0 \end{aligned}\right.$$

Goal: Find $s, t \in \mathbb{Z}$, s.t.

$$\underset{\text{gcd}}{7} = 287s + 91t$$

$$\begin{aligned} 7 &= 91 - \textcircled{14} \times 6 \\ &= 91 - (\overbrace{287 - 91 \times 3}^{14}) \times 6 \\ &= 91 - 287 \times 6 + 91 \times 18 \\ &= 91 \times 19 - 287 \times 6 \end{aligned}$$

2. Modular Arithmetic

Def Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. If $m \mid a-b$, we say a is **congruent to b modulo m**, denoted $a \equiv b \pmod{m}$.

E.g.

- $100 \overset{?}{\equiv} 2 \pmod 7$ $\quad 100 \equiv 2 \pmod{14}$
- $100 - 2 = 98 = 14 \times 7 \Rightarrow 100 \equiv 2 \pmod 7$
- $-11 - 1 = -12 = \underbrace{(-4) \times 3}_{} \Rightarrow -11 \equiv 1 \pmod 3$

  $-11 \overset{?}{\equiv} 1 \pmod 3$

Rem. The notation "$a \equiv b \pmod m$" suggests it might be some sort of equality. The following theorem tells us it is comparing reminders.

$\boxed{\text{Thm}}$ Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then $\underline{a \equiv b \pmod{m}}$ iff

r_a $\underline{a \% m} = \underline{b \% m}$. r_b

Pf: By division algorithm, $\exists\, q_a, q_b \in \mathbb{Z}$, $0 \le r_a, r_b < m$, s.t.

$$\begin{cases} a = q_a m + r_a \\ b = q_b m + r_b \end{cases}$$

$$\Rightarrow a - b = \underbrace{(q_a - q_b)m + (r_a - r_b)}_{}.$$

("$\Rightarrow$") Assume $\underbrace{a \equiv b}_{} \pmod{m}$.

Then $m \mid a - b$.

$\Rightarrow m \mid \underbrace{(q_a - q_b)m}_{} + (r_a - r_b)$

$\Rightarrow m \mid r_a - r_b$.

$0 \le r_a, r_b < m$ $\Rightarrow r_a - r_b = 0 \Rightarrow r_a = r_b$

$$\left\{ \begin{array}{l} 0 \le r_a, r_b < m \\ -m < \underbrace{r_a - r_b}_{} < m \\ \Rightarrow r_a - r_b = 0 \end{array} \right.$$

("$\Leftarrow$") Assume $r_a = r_b$.

Then $a - b = (q_a - q_b)m$

$\Rightarrow m \mid a - b$.

$\Rightarrow a \equiv b \pmod{m}$. □

$100 \% 7 = 2$, $2 \% 7 = 2$.

E.g.
- $\underline{100 = 14 \times 7 + 2} \Rightarrow 100 \equiv 2 \pmod{7}$
- $-11 = -4 \times 3 + 1 \Rightarrow -11 \equiv 1 \pmod{3}$.

$-11 \% 3 = 1$, $1 \% 3 = 1$

$\underline{100 \equiv 2 \pmod{14}}$.

2.1 addition and multiplication

Thm Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $\underline{a+c \equiv b+d} \pmod m$ and $ac \equiv bd \pmod m$.

Pf: $a \equiv b \pmod m \Rightarrow m \mid a-b \Rightarrow \exists k_1 \in \mathbb{Z}$, s.t. $\underline{mk_1} = a-b$.

$c \equiv d \pmod m \Rightarrow m \mid c-d \Rightarrow \exists k_2 \in \mathbb{Z}$, s.t. $\underline{mk_2} = c-d$.

$$\underline{(a+c)-(b+d)} = \boxed{\boxed{(a-b)}+(c-d)}$$
$$= mk_1 + mk_2$$
$$= m(k_1+k_2).$$

$m \mid (a+c)-(b+d)$.

$\Rightarrow a+c \equiv b+d \pmod m$.

Showing $ac \equiv bd \pmod m$ is similar; left as an exercise.

either $4 \mid \underline{n^2-0}$, or $4 \mid \underline{n^2-1}$

E.g. **Prop** Let $n \in \mathbb{Z}$. Then $\underline{n^2 \equiv 0 \text{ or } 1 \pmod 4}$.

$n \cdot n$ "

$n \equiv$ ☺ mod 4

$\underline{☺ \cdot ☺} \equiv 0, 1 \pmod 4$

Pf:

Notice that $n \equiv \underline{0}, 1, 2, 3, \pmod 4$

n	0	1	2	3
n^2	0	1	4	9
$n^2 \% 4$	0	1	0	1

$\Rightarrow n^2 \equiv 0 \text{ or } 1 \pmod 4$

a b

$n' \equiv 3 \pmod 4$

c $\underline{n'} \equiv \underline{3}$ d $\pmod 4$.

$(n')^2 \not\equiv 0 \text{ or } 1 \pmod 4$.

$\Rightarrow \underline{(n')^2} \equiv 3^2 \pmod 4$

$\boxed{\text{Prop}}$ $\boxed{m = 4k+3 \text{ for some } k \in \mathbb{N}}$ $\Rightarrow$ m is not the sum of squares of two integers.

Pf: Suppose $m = a^2+b^2$ for some $a, b \in \mathbb{Z}$.

By previous prop, $a^2 \equiv 0$ or $1 \pmod 4$

$b^2 \equiv 0$ or $1 \pmod 4$.

$b^2 \backslash a^2$	0	1
0		
1		2

$\Rightarrow \overset{m \,\shortparallel}{\boxed{a^2+b^2}} \equiv 0, 1, 2 \pmod 4$

However, $\underbrace{m \equiv 3 \pmod 4}_{m-3=4k \;\rightarrow\; 4 \mid m-3}$, contradiction.

Rem. Given $x, y \in \mathbb{R}$, common arithmetic include

$x+y$, xy, $x-y$, $x/y \leftarrow y \neq 0$.

$a - c \equiv b - d \pmod m$
$\Uparrow$
$\left.\begin{matrix} a \equiv b \pmod m \\ c \equiv d \pmod m \end{matrix}\right\}$

- additions and multiplications preserve congruences
- Subtracting $a \in \mathbb{Z}$ is the same as adding $-a \in \mathbb{Z}$, so subtractions preserve congruences
- Dividing $a \in \mathbb{Z}$ is the same as multiplying $\frac{1}{a}$.

  But wait ... $\frac{1}{a} \notin \mathbb{Z}$ in general !!!

2.2 Inverse

$\leftarrow$ existence ? unique ?

Given $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$,

$\boxed{\text{Def}}$ If $x \in \mathbb{Z}$ satisfies $ax \equiv 1 \pmod m$, we say x is a **inverse of a modulo m**, denoted a^{-1} mod(ulo) m

Rem. "a^{-1}" is just a notation. It is NOT the real number $\frac{1}{a}$.
We're only playing with $\mathbb{Z}$ now, remember? ☺

Rem: ① $a, d \in \mathbb{Z}$, $\overbrace{a\% d}^{\text{remainder}} = a \overset{\text{operation.}}{\text{mod}} d$

② (mod m)

$$\underset{\underset{m \mid a-b}{\uparrow \quad \uparrow}}{a \equiv b} \overset{\text{relationship.}}{(\text{mod } m)}.$$

③ $\underbrace{\boxed{a^{-1}} \bmod m}_{}.$ ← an inverse of a modulo m.

denotes a integer $a^{-1} \in \mathbb{Z}$, s.t.

$$a^{-1} \cdot a \equiv 1 \pmod m.$$