Number theory

Section 4.1: Divisibility, Congruence & Modular Arithmetic

Section 4.3: Primes

Section 4.4: Solving Congruences

Divisibility (Last time)

Theorem 4.1.1

For any $a, b, c \in \mathbb{Z}$, $a \neq 0$,

(i) $a|b \wedge a|c \Rightarrow a|(b+c)$

(ii) $a|b \Rightarrow \forall k \in \mathbb{Z}: a|kb$

(iii) $a|b \wedge b|c \Rightarrow a|c$

(i), (ii) $\Longrightarrow$

Corollary 4.1.1

$a|b \wedge a|c \Rightarrow \forall k, \ell \in \mathbb{Z}: a|(kb+\ell c)$

Ex:

dividend, divisor

$$16 = 3 \cdot 5 + 1$$

quotient

$$16 \text{ div } 3 = \left\lfloor \frac{16}{3} \right\rfloor$$

remainder

$$16 \bmod 3 = 16 - 3 \cdot \left\lfloor \frac{16}{3} \right\rfloor$$

Ex:

$$-16 = 3 \cdot (-6) + 2$$

Congruence

Def 4.1.3:

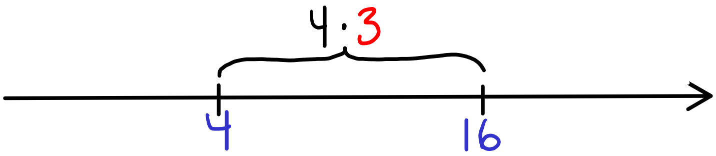
For any $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$,

$$\underbrace{a \equiv b \pmod{m}}_{\text{congruence}} \iff m \mid (a-b)$$

„ a is congruent to b modulo m"

Ex:

$16 \equiv 4 \pmod{3}$, since $3 \mid 12$



$16 \equiv 16 \pmod{3}$, since $3 \mid 0$

$5 \equiv 30 \pmod{5}$, since $5 \mid -25$

$42 \equiv 22 \pmod{5}$, since $5 \mid 20$

$4 \not\equiv -4 \pmod{5}$, since $5 \nmid 8$

Ex: (Parity)

$a \equiv b \pmod{2} \iff$

a and b have the same parity

Ex: (The clock)

$1 \equiv 13 \pmod{12}$

Note that congruence is an equivalence relation.

Theorems 4.1.3 and 4.1.4 give alternative (equivalent) definitions of congruence:

Def. 4.1.3	$a \equiv b \pmod{m}$
	$\Updownarrow$
Thm. 4.1.3	$m \mid (a-b)$
	$\Updownarrow$
Thm. 4.1.4	$a \bmod m = b \bmod m$
	$\Updownarrow$
	$\exists k \in \mathbb{Z} : a = b + km$

Ex:

$16 \equiv 7 \pmod{3}$:

$3 \mid 9$

$16 \bmod 3 = 1 = 7 \bmod 3$

$16 = 7 + 3 \cdot 3$

Notice the difference:

operator

$16 \bmod 3$

$16 \equiv 7 \pmod{3}$

relation

Def. 4.1.3	$a \equiv b \pmod{m}$
	$\Updownarrow$
Thm. 4.1.3	$m \mid (a-b)$
	$\Updownarrow$
Thm. 4.1.4	$a \bmod m = b \bmod m$
	$\Updownarrow$
	$\exists k \in \mathbb{Z} : a = b + km$

<u>Proof</u> of Theorem 4.1.3 :

Exercises 21 and 22

<u>Proof</u> of Theorem 4.1.4 :

$$
\begin{aligned}
& m \mid (a-b) \\
\overset{\text{Def. 4.1.1}}{\Updownarrow} \quad & \exists k \in \mathbb{Z} : a-b = km \\
\Updownarrow \quad & \exists k \in \mathbb{Z} : a = b + km
\end{aligned}
$$

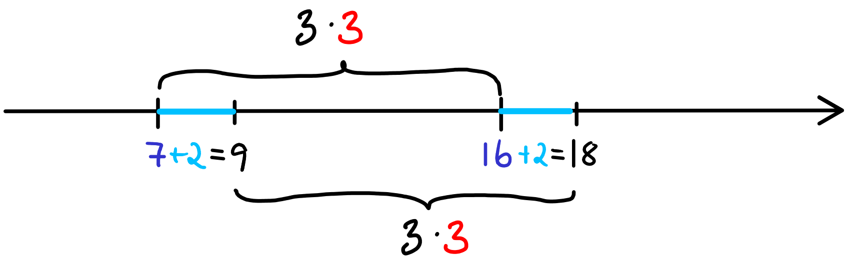
$\square$

How similar are congruences to equations?

It is OK to <u>add</u> the same number to both sides.

Ex:

$$16 \equiv 7 \pmod{3}, \quad \text{since} \quad 3 \mid (16-7)$$
$$\Downarrow$$
$$16+2 \equiv 7+2 \pmod{3}, \quad \text{since} \quad (16+2)-(7+2) = 16-7$$

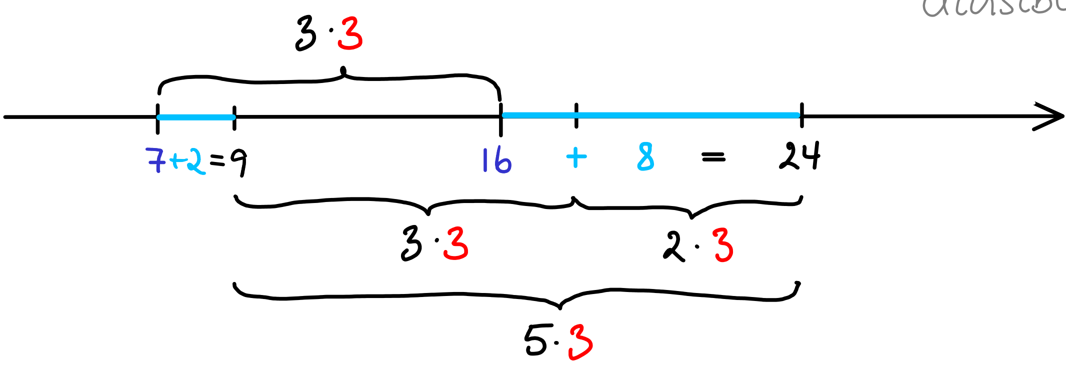


Also OK to <u>add</u> a to one side and b to the other side as long as $a \equiv b \pmod{m}$.

Ex:

$$16 \equiv 7 \pmod{3}, \quad \text{since} \quad 3 \mid (16-7)$$
$$\Downarrow$$
$$16+8 \equiv 7+2 \pmod{3}, \quad \text{since} \quad (16+8)-(7+2) = (16-7)+(8-2)$$

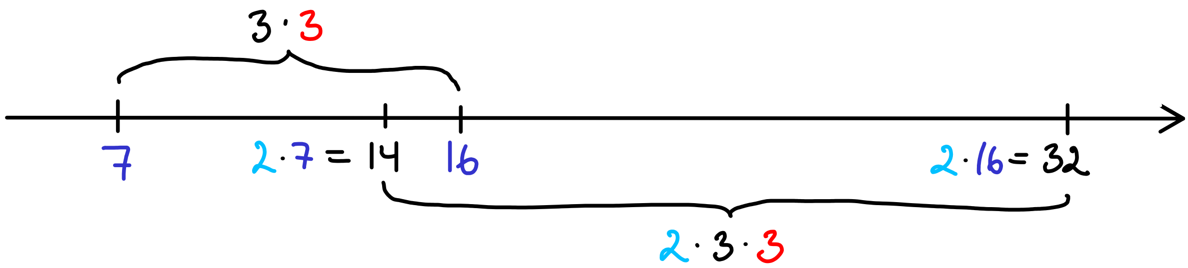
divisible by 3



It is OK to <u>multiply</u> both sides by the same number.

Ex:

$$16 \equiv 7 \pmod 3, \quad \text{since} \quad 3 \mid (16-7)$$
$$\Downarrow$$
$$2\cdot 16 \equiv 2\cdot 7 \pmod 3, \quad \text{since} \quad 2\cdot 16 - 2\cdot 7 = 2\cdot(16-7)$$



Also OK to <u>multiply</u> one side by a and the other side by b, as long as $a \equiv b \pmod m$.

Ex:

$$16 \equiv 7 \pmod 3, \quad \text{since} \quad 3 \mid (16-7)$$
$$\Downarrow$$
$$2\cdot 16 \equiv 8\cdot 7 \pmod 3, \quad \text{since} \quad 2\cdot 16 - 8\cdot 7 = 2\cdot(16-7) - 6\cdot 7$$

divisible by 3

OK to add and multiply on both sides:

Theorem 4.1.5

For any $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$,

$$a \equiv b \pmod{m} \ \wedge\ c \equiv d \pmod{m}$$
$$\Downarrow$$
$$\begin{cases} a + c \equiv b + d \pmod{m} & \wedge \\ a \cdot c \equiv b \cdot d \pmod{m} \end{cases}$$

Proof:

$$\begin{aligned}
& a \equiv b \pmod{m} \ \wedge\ c \equiv d \pmod{m} \\
\text{Thm 4.1.4} \quad \Updownarrow \quad & a = b + km \ \wedge\ c = d + \ell m, \quad k, \ell \in \mathbb{Z} \\
\Downarrow \quad & a + c = b + km + d + \ell m, \quad k, \ell \in \mathbb{Z} \\
\Updownarrow \quad & a + c = b + d + (k + \ell) m, \quad k + \ell \in \mathbb{Z} \\
\text{Thm 4.1.4} \quad \Updownarrow \quad & a + c \equiv b + d \pmod{m}
\end{aligned}$$

$$\begin{aligned}
& a \equiv b \pmod{m} \ \wedge\ c \equiv d \pmod{m} \\
\text{Thm 4.1.4} \quad \Updownarrow \quad & a = b + km \ \wedge\ c = d + \ell m, \quad k, \ell \in \mathbb{Z} \\
\Downarrow \quad & a \cdot c = (b + km) \cdot (d + \ell m), \quad k, \ell \in \mathbb{Z} \\
\Updownarrow \quad & a \cdot c = b \cdot d + (b\ell + kd + k\ell m) \cdot m, \quad b\ell + kd + k\ell m \in \mathbb{Z} \\
\text{Thm 4.1.4} \quad \Updownarrow \quad & a \cdot c \equiv b \cdot d \pmod{m}
\end{aligned}$$

$\square$

Is it also OK to <u>subtract</u> the „same" number on both sides?

Yes, subtracting c is the <u>same as adding</u> $-c$, and $-c \equiv -d \pmod m \iff c \equiv d \pmod m$:

$$
\begin{aligned}
& c \equiv d \pmod m \\
\overset{\text{Def. 4.1.3}}{\iff}\; & m \mid (c-d) \\
\iff\; & m \mid -(c-d) \\
\iff\; & m \mid (-c-(-d)) \\
\overset{\text{Def. 4.1.3}}{\iff}\; & -c \equiv -d \pmod m
\end{aligned}
$$

Is it OK to <u>divide</u> by the same number on both sides?

First of all, both sides need to be divisible by the number.

For example, 3 divides both 18 and 30:

$$18 \equiv 30 \pmod 4 \quad \text{and}$$
$$6 \equiv 10 \pmod 4$$

6 also divides both 18 and 30:

$$18 \equiv 30 \pmod 4 \quad \text{but}$$
$$3 \not\equiv 5 \pmod 4$$

Hence, the answer seems to be „sometimes".

We will investigate this further in Section 4.3.

Modular Arithmetic

When calculating modulo m, we do not need to handle numbers much larger than m:

Corollary 4.1.2

For any $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$,

- $(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$
- $a \cdot b \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$

Intuition:
Doing mod, one subtracts a multiple of m. The final result is the same whether one subtracts everything in the end or subtracts several smaller multiples during the calculations.

Ex:

$(11+22) \bmod 4 = 33 \bmod 4 = 1 = 33 - 8 \cdot 4$

$11 \bmod 4 = 3 = 11 - 2 \cdot 4$

$22 \bmod 4 = 2 = 22 - 5 \cdot 4$

$(3+2) \bmod 4 = 1 = 5 - 1 \cdot 4$

Proof:

$$\begin{cases} a \equiv a \bmod m \pmod{m}, & \text{by Thm 4.1.3} \\ b \equiv b \bmod m \pmod{m}, & \text{by Thm 4.1.3} \end{cases}$$

$$\text{Thm 4.1.5} \Downarrow \quad a+b \equiv (a \bmod m) + (b \bmod m) \pmod{m}$$

$$\text{Thm. 4.1.3} \Updownarrow \quad (a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

$$\begin{cases} a \equiv a \bmod m \pmod{m}, & \text{by Thm 4.1.3} \\ b \equiv b \bmod m \pmod{m}, & \text{by Thm 4.1.3} \end{cases}$$

$$\text{Thm 4.1.5} \Downarrow \quad a \cdot b \equiv (a \bmod m) \cdot (b \bmod m) \pmod{m}$$

$$\text{Thm. 4.1.3} \Updownarrow \quad a \cdot b \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$$

$\square$

Hence, when doing calculations modulo m, we can restrict ourselves to

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$$

Ex: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

Primes (Section 4.3)

Def 4.3.1

Let $p \in \mathbb{Z}$ and $p \geq 2$.

If 1 and p are the only numbers dividing p, p is a prime (primtal).

Otherwise, p is composite (sammensat).

Ex:

Prime: 2, 3, 5, 7, 11, 13, 17, 19, ... The list is infinite, according Thm. 4.3.3

Composite: 4, 6, 8, 9, 10, 12, 14, 15...

Theorem 4.3.1: Fundamental Theorem of Arithmetic

Let $n \in \mathbb{Z}$ and $n \geq 2$.

Then, n can be written as a product of primes in exactly one way (up to rearranging the terms)

Ex:

$$2 = 2$$

$$50 = 2 \cdot 5 \cdot 5$$

$$57 = 3 \cdot 19$$

Greatest Common Divisor & Least Common Multiple

Def 4.3.2:

Let $a, b \in \mathbb{Z}^+$, $a \neq 0$ or $b \neq 0$. Then,

$$\gcd(a,b) = \max\{ d \mid d|a \wedge d|b \}$$

is called the greatest common divisor of a and b
(største fælles divisor)

Thus, gcd(a,b) is the largest number that divides both a and b.

Ex:

$\gcd(18, 24) = 6$

$18 = \boxed{2} \cdot 3 \cdot 3$

$24 = 2 \cdot 2 \cdot 2 \cdot \boxed{3}$

$\gcd(12, 24) = 12$

$12 = \boxed{2 \cdot 2 \cdot 3}$

$24 = 2 \cdot 2 \cdot 2 \cdot 3$

$\gcd(12, 25) = 1 \Rightarrow$ 12 and 25 are relatively prime (Def. 4.3.3)
(indbyrdes primiske)

$12 = 2 \cdot 2 \cdot 3$

$25 = 5 \cdot 5$

Def 4.3.5:

Let $a, b \in \mathbb{Z}^+$, $a \neq 0$ or $b \neq 0$. Then,

$$\operatorname{lcm}(a,b) = \min\{ m \mid a|m \wedge b|m \}$$

is called the smallest common multiple (mindste fælles multiplum) of a and b.

Thus, $\operatorname{lcm}(a,b)$ is the smallest number which is divisible by both a and b.

Ex:

$$\operatorname{lcm}(18, 24) = 72$$

$$18 = 2 \cdot \boxed{3 \cdot 3}$$

$$24 = \boxed{2 \cdot 2 \cdot 2} \cdot 3$$

$$\operatorname{lcm}(12, 24) = 24$$

$$12 = 2 \cdot 2 \cdot 3$$

$$24 = \boxed{2 \cdot 2 \cdot 2 \cdot 3}$$

$$\operatorname{lcm}(12, 25) = 300$$

$$12 = \boxed{2 \cdot 2 \cdot 3}$$

$$25 = \boxed{5 \cdot 5}$$

Ex (summarized):

$\gcd(18, 24) = 6$

$18 = \boxed{2} \cdot 3 \cdot 3$

$24 = 2 \cdot 2 \cdot 2 \cdot \boxed{3}$

$\text{lcm}(18, 24) = 72$

$18 = 2 \cdot \boxed{3 \cdot 3}$

$24 = \boxed{2 \cdot 2 \cdot 2} \cdot 3$

$\gcd(12, 24) = 12$

$12 = \boxed{2 \cdot 2 \cdot 3}$

$24 = 2 \cdot 2 \cdot 2 \cdot 3$

$\text{lcm}(12, 24) = 24$

$12 = 2 \cdot 2 \cdot 3$

$24 = \boxed{2 \cdot 2 \cdot 2 \cdot 3}$

$\gcd(12, 25) = 1$

$12 = 2 \cdot 2 \cdot 3$

$25 = 5 \cdot 5$

$\text{lcm}(12, 25) = 300$

$12 = \boxed{2 \cdot 2 \cdot 3}$

$25 = \boxed{5 \cdot 5}$

Theorem 4.3.5

Let $a, b \in \mathbb{Z}^+$, $a \neq 0 \vee b \neq 0$. Then,

$$a \cdot b = \gcd(a,b) \cdot \text{lcm}(a,b)$$

Contains $p^{\min\{a_p, b_p\}}$ Contains $p^{\max\{a_p, b_p\}}$

where, for each prime factor p in $a \cdot b$,
p occurs a_p times in a and b_p times in b

The Euclidean Algorithm

Described in the book **Elements** by Euclid who lived 325 B.C. – 265 B.C.

Ex:

$$\gcd(287, 91) = ?$$

$$287 = 91 \cdot 3 + 14$$
$$91 = 14 \cdot 6 + 7$$ ← Last remainder $\neq 0$
$$14 = 7 \cdot 2$$

$$\gcd(287, 91) = 7$$

Check:

$$287 = 7 \cdot 41$$
$$91 = 7 \cdot 13$$

Why does it work?

Lemma 4.3.1

$$a = bq + r, \quad a, b, q, r \in \mathbb{Z}$$
$$\Downarrow$$
$$\gcd(a,b) = \gcd(b,r)$$