MATH1081 2016 S2 Scan Week 3

§2 Integers, Modular Arithmetic, and Relations

FACTORISATION

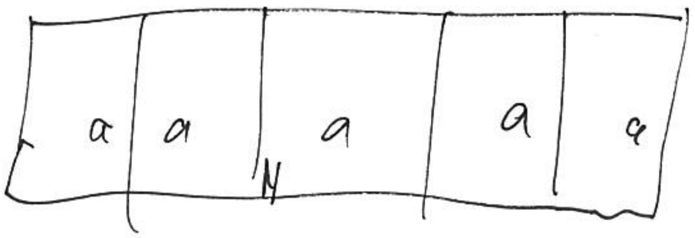
- We recall the commonly-used sets in our number system:
  - *Positive integers* $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$.
  - *Natural numbers* $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.
  - *Integers* $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
  - *Rational numbers* $\mathbb{Q} = \left\{\frac{p}{q} \,\middle|\, p, q \in \mathbb{Z},\ q \neq 0\right\}$.
  - *Real numbers* $\mathbb{R}$ (includes $\mathbb{Q}$ and *irrational numbers* such as $\sqrt{2}$, π, e).

  Note that $\mathbb{Z}^+ \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.
- *Number theory* focuses on $\mathbb{Z}$ and its subsets.
- We can add, multiply, subtract, and divide in $\mathbb{Q}$ and $\mathbb{R}$, but we cannot always divide in $\mathbb{Z}$; for instance, $\frac{2}{3} \notin \mathbb{Z}$.

- Let a and b be integers. If there is an integer m such that $b = am$, then we say
  - b is a *multiple* of a,
  - a is a *factor* or *divisor* of b,
  - a *divides* b,
  - b is *divisible* by a,
  - am is a *factorisation* of b

  and we write $a \mid b$.
- We write $a \nmid b$ if a does not divide b.
- If a and b are positive integers and $a \mid b$, then we must have $a \leq b$.
- $a|b$ ("a divides b") is a statement about *divisibility* that is either true or false. $\frac{a}{b}$ ("a divided by b") is a number that we get by carrying out *division*. The divisibility symbol $a \mid b$ and the division symbol a/b are not to be confused.
- Divisibility by zero is well-defined but mostly pointless, since $0 \mid b$ only holds when $b = 0$.

$a|b$



$b = 5a$

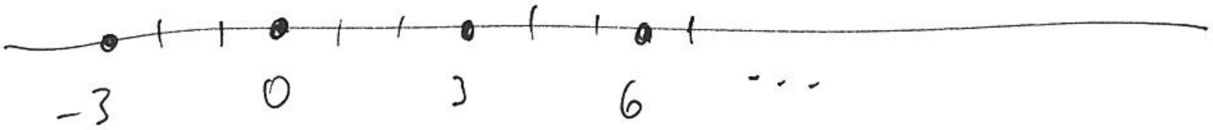
Ex What is the smallest number that is divisible by 1, 2, 3, 4 and 5?

As. 60

$60 = 2^2 \times 3 \times 5$

Ex $3 \,|\, (n-1)\,n\,(n+1)$ for any integer n

because one of any 3 consecutive numbers is divisible by 3



Exercise. Compare the following notations.

$12/48 = \frac{1}{4} = \frac{12}{48}$ $\qquad 12 \mid 48$ T $\qquad 12 \nmid 48$ F

$48/12 = 4 = \frac{48}{12}$ $\qquad 48 \mid 12$ F $\qquad 48 \nmid 12$ T

- **Properties of divisibility:** let a, b, and c be integers, then

  (i) $a \mid 0$, (Each integer is a factor of 0 and 0 is a multiple of every integer.)

  (ii) if $a \mid b$, then $a \mid bc$;

  (iii) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;

  (iv) if $a \mid b$ and $a \mid c$, then $a \mid (sb+tc)$ for all integers s and t; **(Important!)**

  (v) if $a \mid b$ and $b \mid c$, then $a \mid c$. (*Transitivity* of divisibility)

Proof. (v) Suppose that $a \mid b$ and $b \mid c$.
Then $b = am$ and $c = bn$ for some integers m and n. Thus, we have

$$c = bn = (am)n = a(mn) = ak,$$

where $k = mn$ is an integer. Hence, $a \mid c$.

(i) $0 = a \times 0$. Thus, $a \mid 0$.

Exercise. Prove ~~(ii)-~~(iv).

Suppose $a \mid b$ and $a \mid c$

$b = am$ and $c = an$ for Some integes m, n

So $sb + tc = sam + tan$ (fa any intges s, t)

$= a(sm + tn)$

So $a \mid (sb + tc)$ because $sm + tn$ is an integer

- **Simple divisibility tests:**

2	Last digit is 0, 2, 4, 6, or 8.
3	Sum of digits is divisible by 3.
4	Last two digits is divisible by 4.
5	Last digit is 0 or 5.
6	Divisible by 2 and 3.
7	Double the last digit and subtract it from the remaining leading truncated number. If the result is divisible by 7, then so was the original number. Apply this rule over and over again as necessary.
8	Last three digits is divisible by 8.
9	Sum of digits is divisible by 9. See over
10	Last digit is 0.
11	The difference between the sum of digits in the odd positions and the sum of digits in the even positions is divisible by 11.
⋮	

Exercise.
Is 408254 a multiple of 3? Is 408254 divisible by 7? Does 11 divide 408254?

Sum of digits = 23, so not divisible by 3

For 11: $4+8+5 = 17$
$0+2+4 = 6$ difference is 11

So the number is divisible by 11.

For 7: $40825 - 8$ = whatever, then continue

- An *even* number is an integer that is divisible by 2, so can be written as $n = 2k$ for some integer k. So zero is even

- An *odd* number is an integer that is not an even number so can be written as $n = 2k + 1$ for some integer k.

A number is divisible by 9 if and only if the sum of its digits is divisible by 9

Proof Let the number have digits $a_n \ldots a_2 a_1 a_0$

Then the number itself is $10^n a_n \ldots + 100a_2 + 10a_1 + a_0$

and the sum of its digits is $a_n + \ldots + a_2 + a_1 + a_0$

The difference of these is $\underset{\overset{\shortparallel}{999\ldots9}}{(10^n-1)}a_n + \ldots + 99a_1 + 9a_1$

which is a multiple of 9.

So if the number is a multiple of 9, so is the sum of its digits

and if the sum of the digits is a multiple of 9, so is the number.

- A *prime* is an integer larger than 1 whose only positive factors are 1 and itself.
  - The first few primes are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$.
  - There are infinitely many primes; this has been known for over two thousand years.
  - Primes of the form $2^p - 1$, where p is prime, are called *Mersenne primes*. The largest prime currently known (March 1st 2014) is a Mersenne prime, $2^{57,885,161} - 1$, discovered in January 2013. It has 17,425,170 digits. Check out GIMPS for the latest information.
  - Primes of the form $2^{2^n} + 1$ are known as *Fermat primes*. Only five Fermat primes are known: $3, 5, 17, 257, 65537$.
  - *Twin primes* are pairs of primes that differ by 2, such as 3 and 5, 5 and 7, 11 and 13, 17 and 19, and 1000000000061 and 1000000000063. There are thought to be infinitely many twin primes but no proof exists.
- An integer greater than 1 that is not a prime is called a *composite* number.
- 1 is neither prime nor composite.

- **The Fundamental Theorem of Arithmetic.**
  Any positive integer n has a prime factorization, that is, can be expressed as a product of primes

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

  for distinct primes $p_1, p_2, \ldots, p_k$ and exponents $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{Z}^+, k \geq 0.$
- The factorisation is unique up to permuting factors.
- A prime number is a product of just one prime, namely itself.
- 1 is a product of no primes.
- Any positive divisor d of the above n has prime factorisation

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

  for some $0 \leq \beta_1 \leq \alpha_1, \ldots, 0 \leq \beta_k \leq \alpha_k.$

Example.

$$1000 = 2^3 \times 5^3; \quad 1001 = 7 \times 11 \times 13; \quad 1002 = 2 \times 3 \times 167.$$

Consultation time: Wed 3-4 RC 6109 or email

"Algorithm" to find the prime factorisation of n. If n is prime, we are done. Otherwise, we can factorise $n = ab$ with a, b positive factors not equal to 1. Repeat procedure with a and b.

Exercise. Find the prime factorisation of 345 and all its positive factors.

$5 \mid 345$ $\quad$ $345 = 5 \times 69$

$= 3 \times 5 \times 23$

- How do we determine whether or not a given positive integer n is prime?
  - The obvious way to do this is to check whether n is a multiple of any of the $n-2$ numbers $2, 3, \dots, n-1$. If none of these is a factor, then n is prime; if any of them is a factor, then n is composite.
  - It is enough to check only the primes among these $n-2$ numbers. (**Why**?)
  - It is enough to check only the primes up to $\sqrt{n}$. (See ~~next page~~.) below
  - There are faster primality tests. (See MATH2400 and MATH3411.) but not that fast

- **Theorem.** If n is composite, then n has a prime factor at most equal to $\sqrt{n}$. ✓

Equivalently...

- **Theorem.** If n has no prime factor less than or equal to $\sqrt{n}$, then it is prime.

Proof. If n is composite

$n = ab$ where $1 < a < n$ and $1 < b < n$

a and b can't be both $> \sqrt{n}$, since then $ab > n$

So ~~at least~~ one of a, b $\leq \sqrt{n}$

That has a prime factor $\leq \sqrt{n}$ (which is a prime factor of n).

Exercise. Is 161 prime? Is 163 prime?

$7 \mid 161$ so 161 is not a prime

$2 \nmid 163$, $3 \nmid 163$, $5 \nmid 163$, $7 \nmid 163$, $11 \nmid 163$ so 163 is prime

(since $13^2 = 169 > 163$. no need to check 13)

- Let a and b be integers, not both zero. Any positive integer d that satisfies $d \mid a$ and $d \mid b$ is called a *common divisor* or a *common factor* of a and b. The largest such d is called the *greatest common divisor* of a and b, and is denoted by $\gcd(a, b)$.
- If $\gcd(a, b) = 1$, then a and b are *coprime* or *relatively prime* to each other.
- Let a and b be positive integers. Each positive integer m that satisfies both $a \mid m$ and $b \mid m$ is called a *common multiple* of a and b. The smallest such m is called the *least common multiple* of a and b, and is denoted by $\mathrm{lcm}(a, b)$.
- If a and b are positive integers, then $\gcd(a, b) \times \mathrm{lcm}(a, b) = ab$.

Example. The positive factors of 12 are $\{1, 2, 3, 4, 6, 12\}$.
The positive divisors of 42 are $\{1, 2, 3, 6, 7, 14, 21, 42\}$.
The common divisors of 12 and 42 are $\{1, 2, 3, 6\}$.
Thus, $\gcd(12, 42) = 6$.

The positive multiples of 12 are $\{12, 24, 36, 48, 60, 72, 84, \ldots\}$.
The positive multiples of 42 are $\{42, 84, 126, \ldots\}$.
Thus, $\mathrm{lcm}(12, 42) = 84$.

Example. Since prime factorisation can be used to find all divisors of an integer, it can also be used to find the gcd and lcm of two numbers. For example, consider

$$14175 = 3^4 \times 5^2 \times 7 \qquad \text{and} \qquad 16758 = 2 \times 3^2 \times 7^2 \times 19\,.$$

For the gcd, we multiply all the prime factors common to both:

$$\gcd(14175, 16758) = 3^2 \times 7 = 63\,.$$

For the lcm, take the smallest product that includes all factors of both numbers:

$$\mathrm{lcm}(14175, 16758) = 2 \times 3^4 \times 5^2 \times 7^2 \times 19 = 3770550\,.$$

Exercise. Find the gcd and lcm of $a = 2^3 \times 3 \times 5^2 \times 11$ and $b = 3 \times 5 \times 7$.

$\gcd(a, b) = 3 \times 5 = 15$
$\mathrm{lcm}(a, b) = 2^3 \times 3 \times 5^2 \times 7 \times 11$

Exercise. If a is positive and is a factor of b, then what is $\gcd(a, b)$?

a

Exercise. What happens if we try to compute $\gcd(0, 0)$?

Not defined, as every integer is a divisor of zero so no greatest

Exercise. What is $d = \gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)})$?

1

EUCLIDEAN ALGORITHM & INTEGER ARITHMETIC

A key tool in integer arithmetic is

- **The Division Algorithm.** Let a be an integer and b be a positive integer. Then there is a unique pair of integers q and r (called *quotient* and *remainder*) such that $a = qb + r$ and $0 \leq r < b$.

Proof. See textbook [Epp, Section 4.4 and Exercise 18 of Section 3.7].

Example. We can find the quotient and remainder by long division or by repeated subtraction. For example, we divide 92 and -92 by 7.

$$\begin{array}{rrrr}
13 & 13 & -13 & -14 \\
7\,\overline{)92} & 7\,\overline{)92} & 7\,\overline{)\,-92} & 7\,\overline{)\,-92} \\
\underline{7} & \underline{91} & \underline{-91} & \underline{-98} \\
22 & 1 & -1 & 6 \\
\underline{21} & & & \\
1 & & & \\
\textit{long division} & \textit{simplified} & \textit{incorrect} & \textit{correct}
\end{array}$$

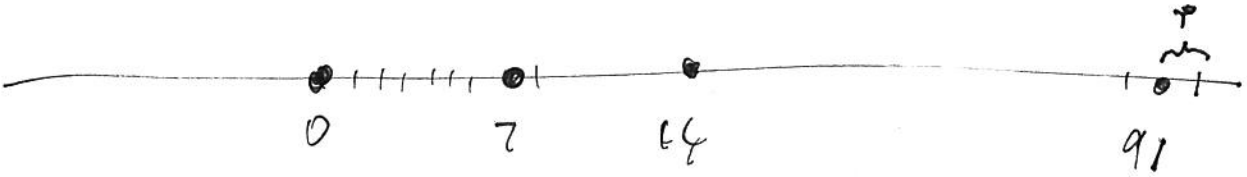
Ex To apply the division algorithm to $\overset{a}{\overset{\shortparallel}{92}}$ and $\overset{b}{\overset{\shortparallel}{7}}$

Calculator: $92/7 \approx 13.14\ldots$

So $q = 13$

$qb = 13 \times 7 = 91$, subtract from 92

$$92 = 13 \times 7 + \underset{\nwarrow r}{1}$$



For negative numbers a, make sure you go left for qb so r is positive (or zero)

We see that $92 = 13 \times 7 + 1$.

Thus, when 92 is divided by 7, the quotient is 13 and the remainder 1.

We have $-92 = (-13) \times 7 + (-1)$ and $-92 = (-14) \times 7 + 6$. Since the remainder should lie between 0 and 6, we conclude that when -92 is divided by 7, the quotient is -14 and the remainder 6.

Exercise. Find the quotient and remainder when -1001 is divided by 101.

$-1001 = -10 \times 101 + 9$

Theorem. Let a, b, q, and r be integers such that $a = q\,b + r$, where a and b are not both zero. Then

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

Proof. Write $d_1 = \gcd(a, b)$ and $d_2 = \gcd(b, r)$.

Since $d_2 \mid b$ and $d_2 \mid r$, we have $d_2 \mid (q\,b + r)$ and thus $d_2 \mid a$.
Thus d_2 is a common divisor of a and b.
But since d_1 is the greatest common divisor of a and b, we must have $d_2 \leq d_1$.

Conversely, we can write $r = a - q\,b$.
Since $d_1 \mid a$ and $d_1 \mid b$, we have $d_1 \mid (a - q\,b)$ and thus $d_1 \mid r$.
This shows that d_1 is a common divisor of b and r, and hence $d_1 \leq d_2$.

For both $d_2 \leq d_1$ and $d_1 \leq d_2$ to be true we require that $d_1 = d_2$.

Euclidean Algorithm. Use the above theorem together with the Division Algorithm repeatedly to calculate the greatest common divisor of two numbers.

Note that we undeline a, b, r and the successive remainders as we need to keep track of them, particularly later.

Example. We use the Euclidean Algorithm to compute the greatest common divisor of 16758 and 14175 as follows:

$$\begin{array}{rcll}\underline{16758} &=& 1\times\underline{14175}+\underline{2583}, & \text{so } \gcd(16758,14175)=\gcd(14175,2583).\\ \underline{14175} &=& 5\times\underline{2583}+\underline{1260}, & \text{so } \gcd(14175,2583)=\gcd(2583,1260).\\ \underline{2583} &=& 2\times\underline{1260}+\underline{63}, & \text{so } \gcd(2583,1260)=\gcd(1260,63).\\ \underline{1260} &=& 20\times\underline{63}+0, & \text{thus } 63\mid 1260 \text{ and so } \gcd(1260,63)=63.\end{array}$$

Hence, $\gcd(16758, 14175) = 63$. Moreover, we have

$$\operatorname{lcm}(16758,14175) = \frac{16758\times 14175}{\gcd(16758,14175)} = 3770550\,.$$

Exercise. Use the Euclidean Algorithm to find gcd~~(854, 651)~~. (7, 5)

$7 = 1\times 5 + 2$

$5 = 2\times 2 + 1$ ↖ gcd = last non-zero remainde

$2 = 2\times 1$

- We can use the Euclidean Algorithm to find an integer solution x and y to the equation
$$ax + by = \gcd(a,b)\,.$$
This is done by working backward through the Euclidean Algorithm; this process is known as the *Extended Euclidean Algorithm*.

Example. We look for an integer solution of x and y to the equation

$$16758x + 14175y = 63\,.$$

Recall that we obtained $\gcd(16758, 14175) = 63$ by the Euclidean Algorithm

$$\begin{array}{rcll}\underline{16758} &=& 1\times\underline{14175}+\underline{2583} & (3)\\ \underline{14175} &=& 5\times\underline{2583}+\underline{1260} & (2)\\ \underline{2583} &=& 2\times\underline{1260}+\underline{63} & (1)\\ \underline{1260} &=& 20\times\underline{63}+0\,. & \end{array}$$

We work backwards, re-writing the remainders using (1)-(3):

$$\underline{63} = \underline{2583} - 2\times\underline{1260} \qquad \text{by equation (1)}$$

$$
\begin{aligned}
&= \underline{2583} - 2\,(\underline{14175} - 5 \times \underline{2583}) && \text{by equation (2)}\\
&= 11 \times \underline{2583} - 2 \times \underline{14175} && \text{collect like terms}\\
&= 11\,(\underline{16758} - \underline{14175}) - 2 \times \underline{14175} && \text{by equation (3)}\\
&= 11 \times \underline{16758} - 13 \times \underline{14175} && \text{collect like terms}\,.
\end{aligned}
$$

Thus,

$$16758 \times 11 \;+\; 14175 \times (-13) \;=\; 63\,.$$

Hence, $16758x + 14175y = 63$ has an integer solution $x = 11$ and $y = -13$.

Doubling this equation we see that $16758x + 14175y = 126$ has an integer solution $x = 22$ and $y = -26$, since

$$16758 \times (11{\times}2) \;+\; 14175 \times (-13{\times}2) \;=\; 63{\times}2.$$

Tripling this equation we see that $16758x + 14175y = 189$ has an integer solution $x = 33$ and $y = -39$, since

$$16758 \times (11{\times}3) \;+\; 14175 \times (-13{\times}3) \;=\; 63{\times}3.$$

However, $16758x + 14175y \;=\; 60$ has no integer solution, since $63 \nmid 60$ but $63|$ LHS.

Above examples show the extended Euclidean algorithm gives (i) & (ii) below.

The Bézout Property. Consider the equation

$$ax + by \;=\; c\,.$$

where a, b, and c are integers, with a and b not both zero. Then

(i) if $c = \gcd(a,b)$, then the equation has integer solutions;

(ii) if $c = e\gcd(a,b)$ for some $e \in \mathbb{Z}$, then the equation has integer solutions; In fact if $(x,y) = (x_0, y_0)$ is a solution to $ax + by = \gcd(a,b)$ then $(x,y) = (ex_0, ey_0)$ is a solution to $ax + by = e\gcd(a,b)$.

(iii) if c is not a multiple of $\gcd(a,b)$, then the equation has no integer solution.

Proof of (iii) Let $d = \gcd(a,b)$. Suppose now that c is not a multiple of d and x and y are numbers satisfying $ax +.by = c$. If x, y were integers, then we would have $d \mid (ax + by)$ and hence $d \mid c$, which contradicts the fact that c is not a multiple of d. Hence, in this case x and y cannot be integers and (iii) is proved.

[Note: to find all solutions: see p. 17]

Exercise. Use the Extended Euclidean Algorithm to find some(one integer solutions to the equations

$a)520x - 1001y = 13$, $b)520x - 1001y = -26$, and $c)520x - 1001y = 1$.

Note that we solve $520x + 1001z = 13$ then put $y = -z$.

Apply Euclidean algorithm to 1001 and 520

$1001 = 1 \times 520 + 481$

$520 = 1 \times 481 + 39$

$481 = 12 \times 39 + 13$ ← $\gcd(1001, 520)$

$39 = 3 \times 13$

Work back: $13 = 481 - 12 \times 39$

$= 481 - 12 \times (520 - 1 \times 481)$

$= 13 \times 481 - 12 \times 520$

$= 13 \times (1001 - 1 \times 520) - 12 \times 520$

$= 13 \times 1001 - 25 \times 520$

(a) $x = -25$ $y = -13$ (b.) Multiply everything by -2 (c) no solutions as $13 \nmid 1$

MODULAR ARITHMETIC

- Recall that the Division Algorithm states

  > if a is an integer and m is a positive integer, then there exist unique integers q and r, called the quotient and the remainder, respectively, such that $a = qm + r$ and $0 \le r < m$.

  We define $a \textbf{ mod } m$ (reads "*a modulo m*") to be this remainder r.
  We essentially "ignore" multiples of the *modulus* m.

Exercise. Evaluate

$11 \textbf{ mod } 3 = 2$ $5 \textbf{ mod } 7 = 5$ $-11 \textbf{ mod } 3 = 1$ $-5 \textbf{ mod } 7 = 2$

- Let m be a positive integer. Two integers a and b are *congruent modulo* m, denoted by $a \equiv b \pmod{m}$, if

  $$(a \textbf{ mod } m) = (b \textbf{ mod } m),$$

  that is, if a and b have the same remainder when divided by m.

Example. Any two odd numbers are congruent modulo 2.

- **Equivalent definitions of congruence:**

  (i) $a \equiv b \pmod{m}$,

  (ii) $(a \ \mathbf{mod}\ m) = (b \ \mathbf{mod}\ m)$,

  (iii) $m \mid (a-b)$,

  (iv) $a = b + km$ for some integer k.

Proof.
(i) and (ii) are equivalent by definition.

(iii) and (iv) are equivalent by definition.

Let us prove that (ii) implies (iii).
Suppose that $(a \ \mathbf{mod}\ m) = (b \ \mathbf{mod}\ m) = r$ for some integer $0 \leq r < m$. Then $a = q_1 m + r$ and $b = q_2 m + r$ for some integers q_1 and q_2. Thus,

$$a - b = (q_1 m + r) - (q_2 m + r) = (q_1 - q_2)m = km,$$

where $k = q_1 - q_2$ is an integer. Hence, we have $m \mid (a-b)$.

Finally, let us prove that (iv) implies (ii). (Why does this prove the result?)

see over

- **Properties of congruence:** if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

  (i) $a + c \equiv b + d \pmod{m}$;

  (ii) $a - c \equiv b - d \pmod{m}$;

  (iii) $ac \equiv bd \pmod{m}$;

  (iv) $a^n \equiv b^n \pmod{m}$ for all $n \geq 0$;

  (v) $\ell a \equiv \ell b \pmod{m}$ for all integers ℓ;

  (vi) $a \equiv b \pmod{n}$ for all integers n satisfying $n \mid m$.

To show (iv.) implies (ii).

Suppose $a = b + km$ for some integer k

Let $a = q_1 m + r_1$ with $0 \leq r_1 < m$

and $b = q_2 m + r_2$ with $0 \leq r_2 < m$

So $q_1 m + r_1 = q_2 m + r_2 + km$

$(q_1 - q_2 - k) m = r_2 - r_1$

So $r_1 - r_2 = 0$ since $|r_2 - r_1| < m$ and $r_2 - r_1$ is a multiple of m

$r_1 = r_2$

That is, $a \bmod m = b \bmod m$

Therefore, (iv.) implies (ii.)

Why does this imply the result?

$$\begin{tikzcd}
(i.) \arrow[r, Leftrightarrow] & (ii) \arrow[r, Rightarrow] & (iii.) \arrow[r, Leftrightarrow] & (iv) \arrow[ll, bend left, Rightarrow]
\end{tikzcd}$$

So they're all logically equivalent, no more work needed.

Proof.
Suppose that $a = b + k_1 m$ and $c = d + k_2 m$ for some integers k_1 and k_2.

(i) $a + c = (b + k_1 m) + (d + k_2 m) = (b + d) + (k_1 + k_2)m = (b + d) + km$, where $k = k_1 + k_2$ is an integer. Thus, $a + c \equiv b + c \pmod{m}$.

(ii) Similar to (i).

Careful: you can't cancel (or divide)

eg. $la \equiv lb$ therefore $a \equiv b$ is wrong

e.g. ~~$k \equiv 7 \pmod{6}$~~ but

~~$2 \times 8 \equiv 2 \times 20 \pmod{3}$ so $8 \equiv 10 \pmod{3}$~~)

$2 \times 5 \equiv 2 \times 10 \pmod{2}$ but $5 \not\equiv 10 \pmod{2}$

Example. Suppose $x, y \in \mathbb{Z}$ with $x \equiv 3 \pmod{7}, y \equiv 5 \pmod{7}$.
Find $2x + xy$ **mod** 7.
By v), $2x \equiv 2 \times 3 = 6 \pmod{7}$.
By iii), $xy \equiv 3 \times 5 = 15 \equiv 1 \pmod{7}$.
So i) gives $2x + xy \equiv 6 + 1 = 7 \equiv 0 \pmod{7}$. Hence $2x + xy$ **mod** $7 = 0$.

Exercise. Find $x^3 + 2x^2 y$ **mod** 7.

Upshot You can substitute with congruence equations much as you can with ordinary equations. (but not cancel/divide)

Here's a simple-minded application of modular arithmetic.

Example. The last two digits of the number 1234567 are the number 67. This can be formally expressed as

$$1234567 \ \mathbf{mod}\ 100 = 67 \qquad \text{or} \qquad 1234567 \equiv 67 \pmod{100}\,.$$

Similarly, to find the last two digits of the number $7^{1234567}$, we need to evaluate $7^{1234567}$ **mod** 100. We have

$$\begin{aligned} 7^2 &\equiv 49 \pmod{100}\,;\\ 7^3 &\equiv 49\times 7 \equiv 343 \equiv 43 \pmod{100}\,;\\ 7^4 &\equiv 43\times 7 \equiv 301 \equiv 1 \pmod{100}\,. \end{aligned}$$

Then it is easy to obtain, for example,

$$\begin{aligned} 7^8 &\equiv (7^4)^2 \equiv 1^2 \equiv 1 \pmod{100}\,;\\ 7^{444} &\equiv (7^4)^{111} \equiv 1^{111} \equiv 1 \pmod{100}\,;\\ 7^{446} &\equiv (7^4)^{111}\times 7^2 \equiv 1^{111}\times 49 \equiv 49 \pmod{100}\,; \end{aligned}$$

and in particular, we have

$$7^{1234567} \equiv 7^{4\times 308641+3} \equiv (7^4)^{308641}\times 7^3 \equiv 1^{308641}\times 43 \equiv 43 \pmod{100}\,.$$

Exercise. Simplify $10^{123456789}$ **mod** 41.

$$10^2 = 100 = 2\times 41 + 18 \equiv 18 \pmod{41}$$

$$10^3 \equiv 10\times 18 = 180 = 4\times 41 + 16 \equiv 16 \pmod{41}$$

$$10^4 \equiv 10\times 16 = 160 \equiv -4 \pmod{41}$$

$$10^5 \equiv 10\times(-4) = -40 \equiv 1 \pmod{41}$$

So,
$$\begin{aligned} 10^{123456789} &= 10^{123456785}\times 10^4\\ &= (10^5)^{\text{whatever}}\times 10^4\\ &\equiv 1\times(-4) \pmod{41}\ \text{(above)}\\ &\equiv 37 \pmod{41} \end{aligned}$$

Example. We have seen that simplifying a^n **mod** m becomes quite easy if there is a small number k such that $a^k \equiv 1 \pmod{m}$. In a similar way, it is also useful if we have $a^k \equiv -1 \pmod{m}$ for some small k. The trick is to try and keep the numbers between $-m/2$ and $m/2$.

For example, we will try to simplify 5^{115511} **mod** 29. We have

$$\begin{aligned}
5^2 &\equiv 25 \equiv -4 \pmod{29}\,; \quad \text{usual remainder 25 not used!}\\
5^3 &\equiv (-4) \times 5 \equiv -20 \equiv 9 \pmod{29}\,;\\
5^4 &\equiv 9 \times 5 \equiv 45 \equiv 16 \equiv -13 \pmod{29}\,;\\
5^5 &\equiv (-13) \times 5 \equiv -65 \equiv -7 \pmod{29}\,;\\
5^6 &\equiv (-7) \times 5 \equiv -35 \equiv -6 \pmod{29}\,;\\
5^7 &\equiv (-6) \times 5 \equiv -30 \equiv -1 \pmod{29}\,.
\end{aligned}$$

Thus,

$$\begin{aligned}
5^{115511} \equiv 5^{7\times 16501+4} &\equiv (5^7)^{16501} \times 5^4\\
&\equiv (-1)^{16501} \times (-13) \equiv (-1) \times (-13) \equiv 13 \pmod{29}\,.
\end{aligned}$$

Example. Unfortunately, we can't find k with $a^k \equiv \pm 1 \pmod{m}$ if $\gcd(a,m) \neq 1$. Instead we keep an eye out for any "pattern" in the numbers.

For example, we now try to simplify 6^{54321} **mod** 100. We have

$$\begin{aligned}
6^1 &\equiv 6 \pmod{100}\,;\\
6^2 &\equiv 36 \pmod{100}\,;\\
6^3 &\equiv 36 \times 6 \equiv 216 \equiv 16 \pmod{100}\,;\\
6^4 &\equiv 16 \times 6 \equiv 96 \equiv -4 \pmod{100}\,;\\
6^5 &\equiv (-4) \times 6 \equiv -24 \pmod{100}\,;\\
6^6 &\equiv (-24) \times 6 \equiv -144 \equiv -44 \pmod{100}\,;\\
6^7 &\equiv (-44) \times 6 \equiv -264 \equiv 36 \pmod{100}\,.
\end{aligned}$$

Since $6^7 \equiv 6^2 \pmod{100}$, the numbers repeat every 5 steps from here on. Thus,

$$6^{54321} \equiv 6^{54316} \equiv 6^{54311} \equiv \cdots \equiv 6^6 \equiv -44 \equiv 56 \pmod{100}.$$

Since $6^6 \not\equiv 6^1 \pmod{100}$, the pattern does *not* hold for smaller powers.
The pigeon-hole principle (topic 4) ensures there will eventually be a pattern.