# MTH1001M-Algebra

## Slides Week 1

Divisibility in the integers.
The greatest common divisor.
Euclid's algorithm.

# Divisibility in the integers ($\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$)

- What does it mean that an integer $b$ divides an integer $a$?

  3 divides 6 because $6/3 = 2$, an integer.

  However, it is better to avoid fractions and say

  3 divides 6 because $6 = 3 \cdot 2$.
- DEFINITION. Let $a, b \in \mathbb{Z}$. We say that $b$ divides $a$, and we write $b \mid a$, if there exists (at least one) $c \in \mathbb{Z}$ such that $a = b \cdot c$.
- One can also say: $b$ is a divisor of $a$; $b$ is a factor of $a$; $a$ is a multiple of $b$; $a$ is divisible by $b$.
- Hence $4 \nmid 6$, because there is no $c \in \mathbb{Z}$ such that $6 = 4 \cdot c$.
- Do not mix up $\mid$ (*divides*) with a fraction sign $/$ (*divided by*):

  $3 \mid 6$ is a statement (true in this case);

  $6/3$ is an operation (possible here, and giving 2 as the result).

- Hence the integer $b$ divides the integer $a$ when the equation

$$a = bc$$

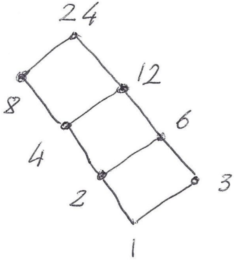
has a solution $c$ in the integers (meaning *at least one*). Hence 2 divides 6 because the equation $6 = 2c$ has a solution $c = 3$.

- $b \mid a$ is equivalent with $a/b$ being an integer, but only for $b \neq 0$.
- So although $0/0$ makes no sense, $0 \mid 0$ is true, because $0 = 0 \cdot 1$ (or $0 = 0 \cdot 3$, or $0 = 0 \cdot 0$, etc.; $c$ *exists* but need not be *unique*).
- The same fact $6 = 2 \cdot 3 = 3 \cdot 2$ tells us that $3 \mid 6$ and that $2 \mid 6$. Any divisor $b$ of $a$ has a matching divisor $a/b$ (possibly $= b$, if $a = b^2$).
- For $a \in \mathbb{Z}$ we write

$$D(a) = \{x \in \mathbb{Z} : x \mid a\},$$

the set of divisors of $a$. Note that if $b \in D(a)$ then $-b \in D(a)$ as well, and also $D(-a) = D(a)$ for every $a$.
(This is because $a = bc \iff a = (-b)(-c) \iff -a = b(-c)$.)

- EXAMPLE. $D(24) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24\}$. Found by factorising $24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$, and better arranged as

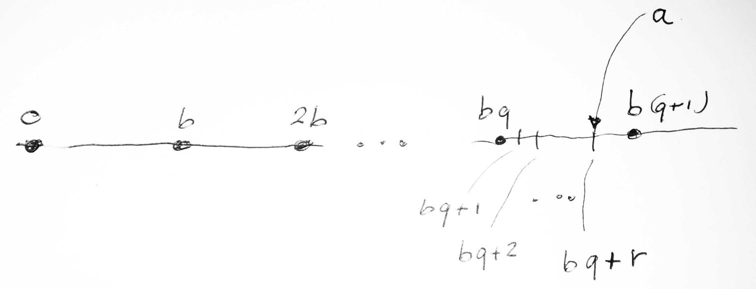



- This is a *Hasse diagram*: lines indicate that the number below divides the one above. We have omitted the $\pm$ signs for simplicity.
- For $120 = 2^3 \cdot 3 \cdot 5$, the Hasse diagram would look best in three dimensions, but we just draw a projection on the plane.

- EXAMPLE. Every $b \in \mathbb{Z}$ divides 0, because $0 = b \cdot 0$, so $D(0) = \mathbb{Z}$.
- EXAMPLE. If 0 divides $a$, then $a = 0 \cdot c = 0$ for some $c$, and so $a = 0$. Hence the only integer $a \in \mathbb{Z}$ such that $0 \in D(a)$ is $a = 0$.
- Note that $b \mid a$ implies $b \leq a$ in the positive integers (but not in $\mathbb{Z}$). Here is a formal proof: if $a = bc$ and $a, b > 0$, then $c > 0$, but then being an integer $c \geq 1$ , and so $a = bc \geq b \cdot 1 = b$.
- Hence if $b \mid a$ and $a \mid b$ for positive integers, then $a = b$. For arbitrary integers, $b \mid a$ and $a \mid b$ imply only $a = \pm b$.

# Division with remainder in the integers

- THEOREM (Standard division). *Given two integers $a, b$, with $b > 0$, there exist unique $q, r \in \mathbb{Z}$ such that $a = b \cdot q + r$, with $0 \leq r < b$.*




- $q$ and $r$ are unique only because we ask $0 \leq r < b$:
  - bigger range (such as $0 \leq r \leq b$) and we lose uniqueness
  - smaller range (such as $0 < r < b$) and we lose existence

- Notations in use to express the result of dividing $a = 14$ by $b = 4$:
  - $14 = 4 \cdot 3 + 2$ [best for us, it says what it means]
  - The quotient is 3 and the remainder is 2 [good]
  - $q = 3$ and $r = 2$ [OK]
  - $14 : 4 = 3 \text{ r } 2$ [common in school but misleading, it may let you think that $14 : 4 = 3$, which is false; best avoid this]
  - $\frac{14}{4} = 3 + \frac{2}{4}$ [not optimal as it uses rational numbers and not just integers; however, mathematically correct and useful to know]
- EXAMPLE. Dividing $a = -13$ by $b = 5$ gives quotient $q = -3$ and remainder 2, because $-13 = 5 \cdot (-3) + 2$, and $0 \leq 2 < 5$. (Not $-13 = 5 \cdot (-2) - 3$, as the remainder cannot be negative.)

- The theorem extends to $b \neq 0$ but needs a further change:
- THEOREM. *Given two integers $a, b$, with $b \neq 0$, there exist unique $q, r \in \mathbb{Z}$ such that $a = b \cdot q + r$, with $0 \leq r < |b|$.*
- COROLLARY. *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. The following assertions are equivalent:*
  1. *$b$ divides $a$;*
  2. *the remainder of the division of $a$ by $b$ is zero.*
- PROOF. [(1) $\Rightarrow$ (2)] If $b$ divides $a$ then $a = b \cdot c = b \cdot c + 0$ for some $c$. Because of uniqueness, the remainder must be zero.
  [(1) $\Leftarrow$ (2)] Conversely, if $r = 0$, then $a = b \cdot q + r = b \cdot q$, and hence $b$ divides $a$. $\square$

# Division with remainder on a pocket calculator

- The conditions
$$a = b \cdot q + r \text{ and } 0 \leq r < b$$
are equivalent to
$$\frac{a}{b} = q + \frac{r}{b}, \text{ and } 0 \leq \frac{r}{b} < 1,$$
so $q = \lfloor a/b \rfloor$ is the integer part of the rational number $a/b$, and $r/b$ is the fractional part of $a/b$.
- EXAMPLE. Here is how to divide 95376 by 271 on a (basic!) pocket calculator, with minimal typing:

| You type in | The screen shows | Make note of |
|---|---|---|
| $95376 \div 271 =$ | $\boxed{351.94095}$ | 351 (the quotient) |
| $-351 =$ | $\boxed{0.94095}$ | |
| $\times 271 =$ | $\boxed{254.99745}$ | 255 (the remainder) |

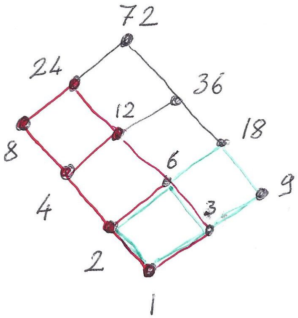
# The greatest common divisor (as from school)

- Here is the school definition. Let $a, b > 0$ be integers. An integer $d$ is called the *greatest common divisor* of $a$ and $b$ if
  1. $d$ divides $a$ and $b$, and
  2. if $c$ is any integer which divides both $a$ and $b$, then $c \leq d$.
- This definition of GCD does not generalise well to $\mathbb{Z}$, or to polynomials, etc. For example, when $a = b = 0$, the divisors of 0 (and 0) are *all the integers*, and there is no *greatest* integer.
- The school's rule to find the GCD of $a$ and $b$ is:
  - find the complete factorisations of $a$ and $b$ (as products of powers of distinct primes);
  - then the GCD equals the product of all common prime factors of $a$ and $b$, each raised to the lower exponent.

- EXAMPLE. Let $a = 24$ and $b = 18$. Factorise $a$ and $b$ fully:

$$24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3 \qquad 18 = 2 \cdot 3 \cdot 3 = 2 \cdot 3^2$$

The school's rule tells us that their GCD is $2 \cdot 3 = 6$, and also that the least common multiple is $2^3 \cdot 3^2 = 72$.




- The common divisors of 24 and 18 are precisely the divisors of 6, so $D(24) \cap D(18) = D(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$.
- Important: All common divisors $1, 2, 3, 6$ are not just $\leq 6$ (as in the school def. of GCD) but they actually divide 6.
- Replacing $c \leq d$ with $c \mid d$ will give us a more useful definition of GCD.

# The greatest common divisor (a better definition)

- DEFINITION (Greatest common divisor). Let $a, b \in \mathbb{Z}$. An integer $d$ is called *a greatest common divisor* of $a$ and $b$ (or *GCD* in short) if
  1. $d$ divides $a$ and $b$, and
  2. if $c$ is any integer which divides both $a$ and $b$, then $c \mid d$.
- A GCD of $a$ and $b$ is denoted $\gcd(a, b)$, or more simply $(a, b)$.
- So requirement (2) is stronger than in the school def. (for $c > 0$): the GCD is not just greatest in the sense of $\leq$, but rather of $\mid$. Hence one can draw stronger consequences from this definition.
- However, the GCD is now not unique (no big deal): if $d$ is a GCD of $a$ and $b$, then $-d$ is another GCD, but there are no more GCDs.
- The GCD of 0 and any integer $a$ now exists, and equals $a$, because $D(0) \cap D(a) = D(a)$. Including when $a = 0$.

- The school's rule for finding the GCD works because of the *unique factorisation* of any integer into a product of prime numbers:
- unique factorization implies that all positive divisors of, say, $200 = 2^3 \cdot 5^2$, are precisely the integers of the form $2^i \cdot 5^j$, with $0 \leq i \leq 3$ and $0 \leq j \leq 2$. (This explains the Hasse diagram.)
- The school's rule is not practical for large numbers, because factorisation into products of primes is a hard computational problem: security of some widely used cryptography relies on that.
- We will now see a much better method to compute GCD's, the *Euclidean algorithm*, which is very fast even applied (by computer) to the huge numbers which occur in cryptographical applications.

# The Euclidean algorithm (or Euclid's algorithm)

- EXAMPLE. We compute the GCD of $a = 78$ and $b = 33$, using the Euclidean algorithm, which is the following sequence of divisions:

$$\begin{aligned} 78 &= 33 \cdot 2 + 12 \\ 33 &= 12 \cdot 2 + 9 \\ 12 &= 9 \cdot 1 + 3 \\ 9 &= 3 \cdot 3 + 0 \end{aligned}$$

  - The first step is dividing $a$ by $b$ with remainder $r$: $\quad a = bq + r$.
  - Discard $a$, let $b$ and $r$ take the roles of $a$ and $b$, and divide again.
  - Continue until a division has remainder zero. The remainder of the previous division (hence the last nonzero remainder) is the GCD of $a$ and $b$, so in this case the GCD is $(78, 33) = 3$.
  - Check: $78 = 2 \cdot 3 \cdot 13$ and $33 = 3 \cdot 11$. But we have not used that!
  - Think of the list of remainders as $78, 33, 12, 9, 3, 0$ (incl. $a$ and $b$).

- EXAMPLE. Compute the GCD of 59 and 22:

$$59 = 22 \cdot 2 + 15$$
$$22 = 15 \cdot 1 + 7$$
$$15 = 7 \cdot 2 + 1$$

Hence $(59, 22) = 1$.

- Note that when the Euclidean algorithm reaches a remainder 1 there is no need to write down the last division $7 = 1 \cdot 7 + 0$, because dividing by 1 can only give reminder 0.
- When two integers have greatest common divisor 1, as in this case, we say that they are *relatively prime,* or that they are *coprime*.
- Do not mix up being coprime with being prime: 59 is actually a prime but $22 = 2 \cdot 11$ is not. Two integers may be coprime without either being prime, for example $4 = 2^2$ and $15 = 3 \cdot 5$.

- EXAMPLE. Compute the GCD of 34 and 21:

$$34 = 21 \cdot 1 + 13$$
$$21 = 13 \cdot 1 + 8$$
$$13 = 8 \cdot 1 + 5$$
$$8 = 5 \cdot 1 + 3$$
$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$

  Hence $(34, 21) = 1$, so 34 and 21 are coprime.
  - Here the algorithm has been as slow as it can possibly be, because all quotients happened to be 1. This occurs exactly when the starting numbers $a$ and $b$ are consecutive Fibonacci numbers.
  - *Fibonacci numbers* $F_0, F_1, \ldots$ are defined by the recurrence relation

$$F_n = F_{n-1} + F_{n-2} \qquad (n \geq 2; \quad F_0 = 0, F_1 = 1).$$

    The first ones are $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$

- EXAMPLE. Compute the GCD of 391 and 299:

$$391 = 299 \cdot 1 + 92$$

$$299 = 92 \cdot 3 + 23$$

$$92 = 23 \cdot 4$$

Hence $(391, 299) = 23$. (So 391 and 299 *are not* coprime.)

- In particular, we discover that $391 = 17 \cdot 23$ and $299 = 13 \cdot 23$ without previously factorising either number. Note that factorising 391 directly, for example, would have taken a while, because the standard procedure would be:
  - checking if 391 is divisible by 2: no (because last digit is odd);
  - checking if it is divisible by 3: no ($3 + 9 + 1$ not a multiple of 3);
  - checking if it is divisible by 5: no (last digit is not 0 or 5);
  - checking if it is divisible by 7: no (not so easy, just try division);
  - checking if it is divisible by 11: no ($3 - 9 + 1$ not a multiple of 11);
  - checking if it is divisible by 13: no (not so easy, just try division);
  - checking if it is divisible by 17, and finally finding that it is.

- EXAMPLE. Compute the GCD of 2203 and 1987:

$$
\begin{aligned}
2203 &= 1987 \cdot 1 + 216 \\
1987 &= 216 \cdot 9 + 43 \\
216 &= 43 \cdot 5 + 1
\end{aligned}
$$

Hence $(2203, 1987) = 1$, so these two numbers are coprime.

  - In this case both 2203 and 1987 happen to be prime numbers, hence of course their GCD is 1.
  - However, we did not know that they are prime numbers (we did not need to, and the Euclidean algorithm does not tell us either).

- How long would it take to find $(2203, 1987)$ by the school way?
  - We would try and factorise 1987, dividing it by $2, 3, 5, 7, 11, \ldots$
  - Once found that 1987 is not divisible by $2, 3, 5, 7, 11, \ldots, 43$, we can stop because 47, the next prime, is larger than $\sqrt{1987} \approx 44.5$.
  - Then 1987 must be prime: if not then it would be a product of at least two primes $p, q$ (possibly equal, and possibly more than two), but we have just found that $p > \sqrt{1987}$ and $q > \sqrt{1987}$, hence $1987 \geq pq > \sqrt{1987} \cdot \sqrt{1987}$, which is impossible.
  - Knowing that 1987 is prime we need not factorize 2203: because 1987 does not divide 2203 we conclude $(2203, 1987) = 1$.
  - However, this procedure would have taken a long time, most of that to try and factorise 1987 (14 divisions, by $2, 3, \ldots, 43$).
  - By contrast, the Euclidean algorithm gave us $(2203, 1987) = 1$ very quickly, but does not tell us that they are prime.
  - More generally, when the Euclidean algorithm on $a$ and $b$ tells us $(a, b) = 1$, it gives us no clue about the factorisations of $a$ and $b$.