MTH1001M-Algebra

Slides Week 2

Why the Euclidean algorithm works.
A variant of integer division and its application to the Euclidean algorithm.
The extended Euclidean algorithm, and Bézout's lemma.
Solving the equation $ax + by = c$ in the integers.
Four Arithmetical Lemmas.
The least common multiple.

Recall from week 1:

- DEFINITION (Greatest common divisor). Let $a, b \in \mathbb{Z}$. An integer d is called *a greatest common divisor* of a and b, written (a, b), if
  1. d divides a and b, and
  2. if c is any integer which divides both a and b, then $c \mid d$.
- $d = (a, b)$ is characterized by $D(d) = D(a) \cap D(b)$.
- In words, (a, b) is an integer whose divisors are precisely all common divisors of a and b.
- With this definition the GCD is only unique up to a sign, for example, the GCD of 4 and 6 is either 2 or -2.
- Note: if an integer a divides both integers b and c, then a divides each of $b + c$, $b - c$, and bc (see a question in Practical 1).

Why does the Euclidean algorithm work?

- The reason depends on the following Lemma.
- LEMMA. *If* $a = bs + c$*, then* $(a, b) = (b, c)$*.*
- PROOF. It is enough to prove that $(a, b) \mid (b, c)$, and that $(b, c) \mid (a, b)$, because then it follows that $(a, b) = (b, c)$. (Actually $(a, b) = \pm(b, c)$, but we may ignore the sign in a GCD.)
  - We start with proving $(b, c) \mid (a, b)$.
  - The GCD (b, c) divides both b and c (by property (1) of the def.).
  - In particular, (b, c) divides bs, and then it divides $bs + c = a$.
  - Hence (b, c) is a common divisor of a and b, and so it divides (a, b) (by property (2) of the def. of GCD, but this time for (a, b)).
  - Now we may reverse the roles of a and c, because $c = b(-s) + a$.
  - Hence the same argument shows $(b, a) \mid (c, b)$, as desired. □

- Instead of a formal proof that the Euclidean algorithm *is correct,* let us see *why it works* on an example, with $a = 57$ and $b = 21$:

$$\begin{aligned} 57 &= 21 \cdot 2 + 15 \\ 21 &= 15 \cdot 1 + 6 \\ 15 &= 6 \cdot 2 + 3 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

  - Because of the Lemma the first division $57 = 21 \cdot 2 + 15$ tells us that $(57, 21) = (21, 15)$.
  - The second division tells us that $(21, 15) = (15, 6)$, etc., and so we find $(57, 21) = (21, 15) = (15, 6) = (6, 3) = (3, 0)$.
  - But $(3, 0) = 3$ because every integer divides 0.
  - Hence the GCD of 57 and 21 is 3.

A variant of division with remainder in the integers

- The following variation of the standard division allows for negative r, and aims at making r as small as possible *in absolute value*, which is better in certain situations.
- THEOREM (A variant of division). *Given $a, b \in \mathbb{Z}$, with $b > 0$, there exist unique $q, r \in \mathbb{Z}$ such that $a = b \cdot q + r$, with $-b/2 < r \leq b/2$.*
- EXAMPLE. When $a = 33$ and $b = 5$, using this variant we get $33 = 5 \cdot 7 - 2$ instead of $33 = 5 \cdot 6 + 3$, so we get $r = -2$. When $a = 21$ and $b = 6$, we have $21 = 6 \cdot 3 + 3$ or $21 = 6 \cdot 4 - 3$, but our condition on r chooses $r = 3$ over $r = -3$.

- To make the Euclidean algorithm even faster we can also do the divisions in the variant where the remainders can be negative.
  - EXAMPLE. GCD of 29 and 18 (standard way left, variant right):

$$\begin{aligned} 29 &= 18 \cdot 1 + 11 \\ 18 &= 11 \cdot 1 + 7 \\ 11 &= 7 \cdot 1 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \end{aligned} \qquad \begin{aligned} 29 &= 18 \cdot 2 - 7 \\ 18 &= 7 \cdot 3 - 3 \\ 7 &= 3 \cdot 2 + 1 \end{aligned}$$

  - EXAMPLE. GCD of 34 and 21 done using this variant of division:

$$\begin{aligned} 34 &= 21 \cdot 2 - 8 \\ 21 &= 8 \cdot 3 - 3 \\ 8 &= 3 \cdot 3 - 1 \end{aligned}$$

    Hence $(34, 21) = 1$. This took half as many divisions as the standard way. In fact, the remainders, in absolute value, have been $(34), 21, 8, 3, 1$, so every other Fibonacci number instead of all.

The extended Euclidean algorithm

- EXAMPLE. In a previous example we found $(391, 299) = 23$:

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

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

$$92 = 23 \cdot 4$$

- Working through the calculations backwards we find

$$\begin{aligned} \mathbf{23} &= \mathbf{299} - \mathbf{92} \cdot 3 \\ &= \mathbf{299} - (\mathbf{391} - \mathbf{299} \cdot 1) \cdot 3 = -\mathbf{391} \cdot 3 + \mathbf{299} \cdot 4. \end{aligned}$$

Writing $d = (391, 299) = 23$ we have found $d = 391x + 299y$ with $x = -3$ and $y = 4$. This algorithm works in general, and shows:

- BÉZOUT'S LEMMA. *Let $a, b \in \mathbb{Z}$, and let $d = (a, b)$ be their greatest common divisor. Then there exist $x, y \in \mathbb{Z}$ such that*

$$ax + by = d.$$

- To avoid errors I normally write the extended part to the right of the divisions, but working from the bottom up:

$$\begin{aligned} 391 &= 299 \cdot 1 + 92 && = \mathbf{299} - (\mathbf{391} - \mathbf{299} \cdot 1) \cdot 3 = -\mathbf{391} \cdot 3 + \mathbf{299} \cdot 4 \\ 299 &= 92 \cdot 3 + 23 && \mathbf{23} = \mathbf{299} - \mathbf{92} \cdot 3 \\ 92 &= 23 \cdot 4 \end{aligned}$$

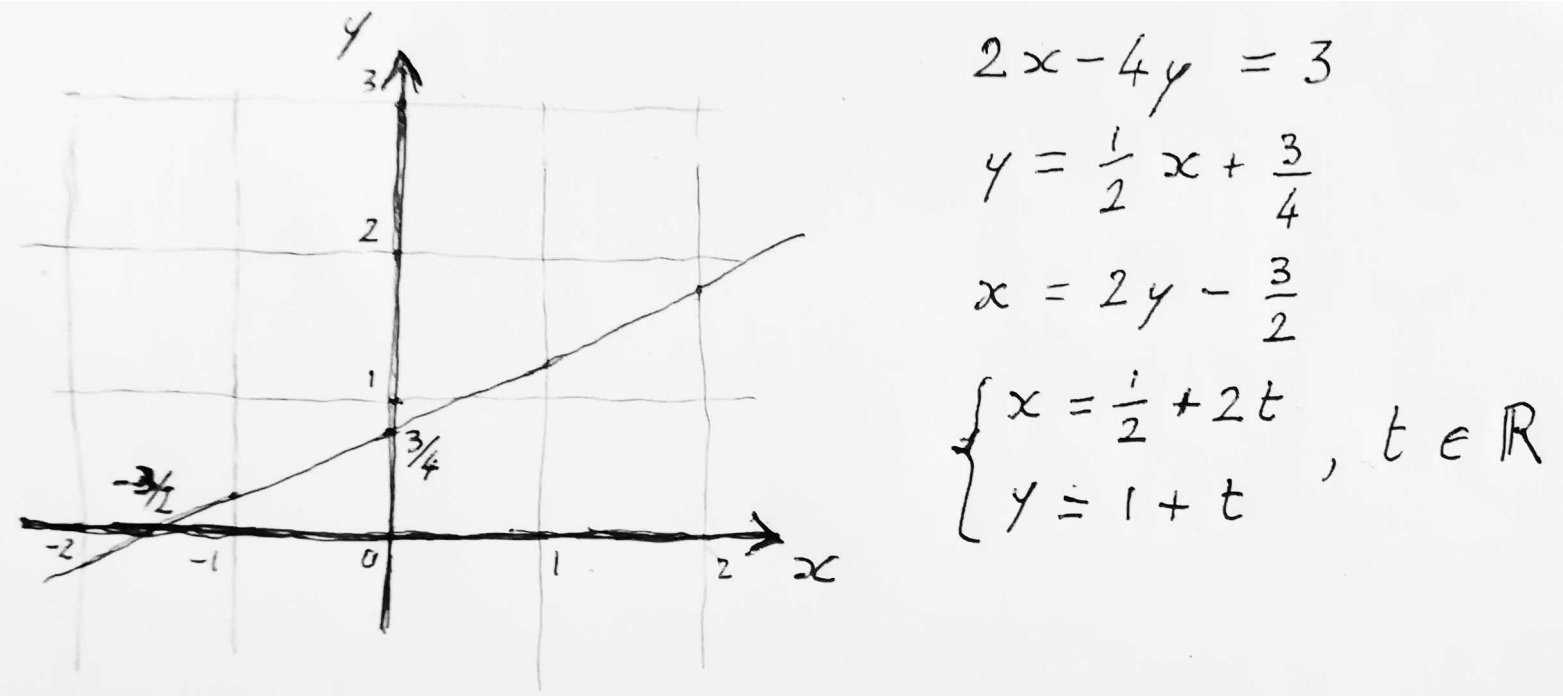
- EXAMPLE. Compute the GCD d of 83 and 53, and then express it in the form $d = 83x + 53y$ for some integers x and y.

$$\begin{aligned} 83 &= 53 \cdot 1 + 30 && = -\mathbf{53} \cdot 13 + (\mathbf{83} - \mathbf{53} \cdot 1) \cdot 23 = \mathbf{83} \cdot 23 - \mathbf{53} \cdot 36 \\ 53 &= 30 \cdot 1 + 23 && = \mathbf{30} \cdot 10 - (\mathbf{53} - \mathbf{30} \cdot 1) \cdot 13 = -\mathbf{53} \cdot 13 + \mathbf{30} \cdot 23 \\ 30 &= 23 \cdot 1 + 7 && = -\mathbf{23} \cdot 3 + (\mathbf{30} - \mathbf{23} \cdot 1) \cdot 10 = \mathbf{30} \cdot 10 - \mathbf{23} \cdot 13 \\ 23 &= 7 \cdot 3 + 2 && = \mathbf{7} - (\mathbf{23} - \mathbf{7} \cdot 3) \cdot 3 = -\mathbf{23} \cdot 3 + \mathbf{7} \cdot 10 \\ 7 &= 2 \cdot 3 + 1 && \mathbf{1} = \mathbf{7} - \mathbf{2} \cdot 3 \end{aligned}$$

- So we find $1 = 83 \cdot 23 + 53 \cdot (-36)$. Always check: $1909 - 1908$.
- Note: one of x and y must be negative, and the other positive.

The equation $ax + by = c$ in the integers

- EXAMPLE. $2x - 4y = -3$ describes a straight line in the plane.



  - Infinitely many real solutions, depending on a single real parameter.
  - But for none of these solutions both x and y are integers, and so the equation $2x - 4y = -3$ has no solution in the integers.
  - This is because the left-hand side will be even if x and y are integers, while the right-hand side -3 is odd.

When $ax + by = c$ has no solution in the integers

- Consider the equation $ax + by = c$, with $a, b, c \in \mathbb{Z}$.
- Call $d = (a, b)$, the GCD of a and b.
- If the equation has a solution $ax_0 + by_0 = c$, with $x_0, y_0 \in \mathbb{Z}$, then d divides the LHS, and hence d divides also the RHS, c.
- So if $d = (a, b)$ does not divide c, then $ax + by = c$ has no solution in the integers (meaning both x and y integer).
- EXAMPLE. $391x + 299y = 14$ has no integer solution, because $(391, 299) = 23$ (see a previous example), and this does not divide 14.

Finding one solution of $ax + by = c$ in the integers

- EXAMPLE. $391x + 299y = 23$ has at least one integer solution, because the extended Euclidean algorithm gave us $23 = \mathbf{391} \cdot (-3) + \mathbf{299} \cdot 4$, so $x = -3$ and $y = 4$ is a solution.
- EXAMPLE. Then also $391x + 299y = 46$ has a solution, because $46 = 23 \cdot 2$, so $x = -3 \cdot 2 = -6$ and $y = 4 \cdot 2 = 8$ is a solution.
- EXAMPLE. More generally, $391x + 299y = c$ has a solution whenever $c = 23s$, with $s \in \mathbb{Z}$: take $x = -3s$ and $y = 4s$.
- A similar argument works in general: if $d = (a, b)$ divides c then $ax + by = c$ has solutions in the integers.
- To find one, first find a solution of $ax + by = d$ using the extended Euclidean algorithm, and then multiply that solution (both x and y) by c/d to find a solution of $ax + by = c$.

Finding more solutions of $ax + by = c$ in the integers

- If x and y form a solution of $ax + by = c$, and k is any integer, then $x' = x - bk$ and $y' = y + ak$ also form a solution, because

$$a(x - bk) + b(y + ak) = ax - abk + by + abk = ax + by = c.$$

- Do we find all solutions in this way? Not in general.
- However, we do when $(a, b) = 1$. To *prove* that we get all solutions we need a bit of theory which we will see in the next two slides.
- EXAMPLE. Take $391x + 299y = 46$ again.
  - We found one solution, namely $x = -3 \cdot 2 = -6$ and $y = 4 \cdot 2 = 8$.
  - Dividing the equation by $(391, 299) = 23$ we get the equivalent equation $17x + 13y = 2$, but now $(17, 13) = 1$ as we wanted.
  - If k is any integer then $x = -6 - 13k$ and $y = 8 + 17k$ give another solution: $17(-6 - 13k) + 13(8 + 17k) = 17 \cdot (-6) + 13 \cdot 8 = 2$.
  - Because $(17, 13) = 1$ we have found all the solutions, for $k \in \mathbb{Z}$.

Some consequences of Bézout's lemma

- Recall Bézout's lemma: *If $a, b \in \mathbb{Z}$, then there exist $x, y \in \mathbb{Z}$ such that $ax + by = (a, b)$.*
- ARITHMETICAL LEMMA A. *For two $a, b \in \mathbb{Z}$, the following properties are equivalent:*
  1. *a and b are coprime (which means $(a, b) = 1$);*
  2. *there are $x, y \in \mathbb{Z}$ such that $ax + by = 1$.*
- PROOF. We need to show that (1)⇒(2), and that (2)⇒(1).

(1)⇒(2) This is simply Bézout's lemma.

(2)⇒(1) This is easier (but an important argument): the GCD $d = (a, b)$ divides ax and by, hence d divides their sum 1, and so $d = 1$. □

- *Warning:* if $ax + by = d$ for some $x, y \in \mathbb{Z}$, and $d > 1$, then we cannot conclude that $(a, b) = d$, only that (a, b) divides d. For example, $10 \cdot 3 - 6 \cdot 4 = 6$, but $(10, 6) = 2$ (which divides 6).

- ARITHMETICAL LEMMA B. *Suppose* $(a, b) = 1$.
  If a divides the product $b \cdot c$*, then a divides c.*
- *Warning:* if we omit $(a, b) = 1$ then Lemma B becomes false. For example, 6 divides $60 = 4 \cdot 15$, but $6 \nmid 4$ and $6 \nmid 15$.
- EXAMPLE. Let x be an integer, and suppose that we know that 10 divides $7x$. Because $(10, 7) = 1$ we conclude that 10 divides x.
- PROOF. By Bézout's lemma, $ax + by = 1$ for some $x, y \in \mathbb{Z}$.
  - Multiplying both sides by c we find $a(xc) + (bc)y = c$.
  - Because a divides each of the products at the LHS (left-hand side), it divides their sum as well, which is c. □
- You probably knew a special case of this, when a is a prime:
  if a prime a divides bc but does not divide b, then a divides c.
  Lemma B says that this remains true even if a is not a prime, as long as it is *coprime* with b.

Why we have found all solutions of $ax + by = c$

- EXAMPLE. Take $391x + 299y = 46$ again.
  - Dividing by $(391, 299) = 23$ we got the equivalent equation $17x + 13y = 2$, for which we have found infinitely many solutions: $x = -6 - 13k$ and $y = 8 + 17k$ for $k \in \mathbb{Z}$.
  - Now we will prove that we have found all solutions.
  - If x, y is any solution, then $17x + 13y = 2$; subtract from this $17 \cdot (-6) + 13 \cdot 8 = 2$, rearrange, and find $17(x + 6) = 13(8 - y)$.
  - So $17 \mid 13(8 - y)$, but $(17, 13) = 1$, and so $17 \mid 8 - y$ by Lemma B.
  - Hence $y - 8 = 17k$ for some $k \in \mathbb{Z}$, but then $x + 6 = -13k$.
- *Warning:* given $391x + 299y = 46$, and one solution $x = -6$ and $y = 8$, the formulas $x = -6 - 299h$ and $y = 8 + 391h$ for $h \in \mathbb{Z}$ give *some* solutions, but not all the solutions.

- EXAMPLE. Find all integer solutions of $319x + 198y = 55$.
  - The Euclidean algorithm with 319 and 198 runs as follows:

$$\begin{aligned} 319 &= 198 \cdot 2 - 77 \\ 198 &= 77 \cdot 3 - 33 \\ 77 &= 33 \cdot 2 + 11 \\ 33 &= 11 \cdot 3 + 0 \end{aligned}$$

  - Hence $(319, 198) = 11$, which divides 55, so there are solutions.
  - The extended part of the Euclidean algorithm is

$$\begin{aligned} 11 &= 77 - 33 \cdot 2 \\ &= 77 + (198 - 77 \cdot 3) \cdot 2 = 198 \cdot 2 - 77 \cdot 5 \\ &= 198 \cdot 2 + (319 - 198 \cdot 2) \cdot 5 = 319 \cdot 5 - 198 \cdot 8. \end{aligned}$$

  - Hence one solution of $319x + 198y = 11$ is $x = 5$ and $y = -8$, and so one solution of $319x + 198y = 55 = 11 \cdot 5$ is $x = 5 \cdot 5 = 25$ and $y = -8 \cdot 5 = -40$.
  - To find all solutions we need to divide the equation by 11.

- EXAMPLE (CONTINUATION). Solving $319x + 198y = 55$.
  - Dividing the equation by 11 we get the equivalent equation $29x + 18y = 5$. Now the coefficients 29 and 18 are coprime.
  - We have found the particular solution $x = 25$ and $y = -40$, so the general solution is $x = 25 - 18k$ and $y = -40 + 29k$, with $k \in \mathbb{Z}$.
  - A (better) variant of the procedure would be to divide the equation by $(319, 198) = 11$ as soon as we have found that, so *before* doing the extended part of the Euclidean algorithm. Then rewrite the Euclidean algorithm with the numbers divided by 11, and do the extended part:

$$\begin{aligned} 29 &= 18 \cdot 2 - 7 & &= 18 \cdot 2 + (29 - 18 \cdot 2) \cdot 5 = 29 \cdot 5 - 18 \cdot 8 \\ 18 &= 7 \cdot 3 - 3 & &= 7 + (18 - 7 \cdot 3) \cdot 2 = 18 \cdot 2 - 7 \cdot 5 \\ 7 &= 3 \cdot 2 + 1 & 1 &= 7 - 3 \cdot 2 \end{aligned}$$

  - The calculations are essentially the same (same coefficients in the extended part of the algorithm), but the smaller numbers make it easier to check the intermediate results.

Another consequence of Bézout's lemma

- When we saw how to find all solutions of $ax + by = c$, one bit of theory was missing: if we divide $ax + by = c$ by $d = (a, b)$ and get $\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$. Do we then always have $(\frac{a}{d}, \frac{b}{d}) = 1$?
- ARITHMETICAL LEMMA C. *Let $a, b \in \mathbb{Z}$, not both zero. Then*

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1.$$

- PROOF. By Bézout's lemma, $ax + by = (a, b)$ for some $x, y \in \mathbb{Z}$.
  - Divide by $(a, b) \neq 0$ and find $\frac{a}{(a,b)}x + \frac{b}{(a,b)}y = 1$.
  - According to Lemma A then $\frac{a}{(a,b)}$ and $\frac{b}{(a,b)}$ are coprime. □
- Lemma C is relevant to simplifying fractions 'in one go': instead of several steps like $42/60 = 21/30 = 7/10$, because $(42, 60) = 6$ it tells us that $\dfrac{42/6}{60/6} = \dfrac{7}{10}$ cannot be further simplified.

One final arithmetical lemma

- Recall Lemma B: $(a, b) = 1$ and $a \mid bc \Rightarrow\ a \mid c$.
- The next lemma is a generalization of Lemma B.
- ARITHMETICAL LEMMA D. *Let $a, b \in \mathbb{Z}$, not both zero. If $a \mid b \cdot c$, then*

$$\frac{a}{(a, b)} \mid c.$$

- PROOF. By assumption there exists x such that $ax = bc$.
  - Dividing both sides by (a, b) (which is not zero) we get

$$\frac{a}{(a, b)} \cdot x = \frac{b}{(a, b)} \cdot c.$$

  - According to Lemma C then $\frac{a}{(a, b)}$ and $\frac{b}{(a, b)}$ are coprime.
  - Hence Lemma B applies and gives the conclusion. □

Recap of divisibility in the integers

$a \mid b$ means $b = ak$ for some $k \in \mathbb{Z}$.

GCD of $a, b \in \mathbb{Z}$ is denoted (a, b).

BÉZOUT'S LEMMA: $(a, b) = ax + by$ for some $x, y \in \mathbb{Z}$.

ARITHMETICAL LEMMA A:

$(a, b) = 1$ (i.e. coprime) $\Leftrightarrow$ $ax + by = 1$ for some $x, y \in \mathbb{Z}$.

ARITHMETICAL LEMMA B: $(a, b) = 1$ and $a \mid bc \Rightarrow a \mid c$.

ARITHMETICAL LEMMA C: $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.

ARITHMETICAL LEMMA D: $a \mid bc \Rightarrow \frac{a}{(a,b)} \mid c$.

The least common multiple

- DEFINITION (Least common multiple). Let $a, b \in \mathbb{Z}$. An integer m is called *a least common multiple* of a and b (or *lcm* in short) if
  1. a and b divide m, and
  2. if c is any integer which is a multiple of both a and b, then $m \mid c$.
- We can denote an lcm of a and b by $\text{lcm}(a, b)$, or also $[a, b]$.
- THEOREM. For any $a, b \in \mathbb{Z}$, their lcm exists and equals $ab/(a, b)$. Hence $(a, b) \cdot [a, b] = a \cdot b$.
- See the Notes for a proof. (Check that $m = ab/(a, b)$ satisfies the definition of a lcm of a and b, using Lemmas B and D.)