Discrete Mathematics 2[1]

Mathematics from high school to university

Hania Uscka-Wehlou

A short table of contents

A detailed table of contents follows (see next pages).

Books to read along with the course, with more practice problems (often suggested in the outline and in some videos, as I have found these books before I started to record the series):

1 *Discrete Mathematics, An Open Introduction*, 4th Edition (2024): Oscar Levin; School of Mathematical Science, University of Northern Colorado.

2 *Mathematics for Computer Science* (LibreTexts): Eric Lehman, F. Thomson Leighton, Albert R. Meyer; MITOpenCourseWare.

3 *Book of Proof*: Richard Hammack; Richmond, Virginia.

4 *Abstract Algebra: Theory and Applications* (LibreTexts): Thomas W. Judson; Stephen F. Austin State University.

The first book is added as a resource to V1 in each part of the DM series, with kind permission of Professor Oscar Levin (given by e-mail on 2 April 2025); the second one is added as a resource to V1 in DM2 and DM3, with kind permission of the Authors (given by e-mail on 20 June 2025). The fourth one is added as a resource to V1 in DM2, with kind permission of the LibreTexts Office (given on 20 July, 2023).

[1] Recorded November 2025 – February 2026. Published on `www.udemy.com` on 2026-03-XX.

An extremely detailed table of contents; the videos (titles in green) are numbered

In blue: problems solved on an iPad (the solving process presented for the students; active problem solving)

In red: solved problems demonstrated during a presentation (a walk-through; passive problem solving)

In magenta: additional problems solved in written articles (added as resources).

In dark blue: *Read along with this section*: references for further reading and exercises in three books named on the previous page: *Discrete Mathematics* (The DM Book), *Mathematics for CS*, and *Abstract Algebra*.

S1 Introduction to the course

You will learn: about this course: its content and the optimal way of studying.

1 Introduction to the course.

Extra material: this list with all the movies and problems. **Extra material: formula sheet for DM.**

Extra material: books named on the previous page (The DM Book, *Mathematics for CS*, and *Abstract Algebra*).

2 Combinatorics in DM1.

3 Elementary Number Theory in DM1.

4 Algebraic structures in DM1.

S2 Combinatorics: the art of counting, cont. from DM1

You will learn: a continuation of topics started in DM1 (permutations, variations, combinations; mathematical modelling), some new stuff (some problems left from DM1, counting functions, counting integer solutions to equations, a generalisation of the Inclusion–exclusion principle, counting derangements), and an introduction to some advanced topics (partitions, multinomial coefficients, Stirling numbers, *Twelvefold Way*); combinatorial problem solving.

Read along with this section: *DM Book*, Chapter 3: *Counting*, pp.191–310 (without Sections 3.6 and 3.7).

5 Why we need combinatorics.

6 Different paths to the same destination: 1. in DM1.

7 Different paths to the same destination: 2. in the DM Book.

New terminology: bit string, its length and weight.

8 Some useful terminology: coins, dice, cards, and balls.

9 More terminology: experiments, outcomes, events, favourable outcomes.

10 Repeating (outcomes) or not: two cases with illustrations and diagrams.

Example: Numbers p and q are chosen randomly from the set $\{1, 2, \ldots, 10\}$

- ∗ Case 1: with replacement,
- ∗ Case 2: without replacement.

Illustrate the sample spaces in both cases (call them Ω_1 and Ω_2) and determine their cardinalities. Define events A: $q > 2p$ and B: $q < 2p$; determine the cardinality of the set of all outcomes favourable for events A and B in both cases. (This example is a preparation for a harder problem that we will solve later in this section, in Video 29, and revisit in Section 4.)

11 Combining outcomes.

Recommended reading: Sections 3.2 and 3.3 in the DM Book: various situations and principles for combining outcomes: **Sum Principle** (additive principle; for combining the *sets* of outcomes, [*or*]), **Product Principle** (multiplicative principle; for combining the *outcomes* in a set, [*and*]), and **PIE** (Principle of Inclusion/Exclusion; a version of the Sum Principle [*or*] in case of *overlapping* outcomes).

In the next videos, we look together at plenty examples from the DM Book (Sections 3.2 and 3.3).

12 Combining outcomes: Sum Principle.

Example 3.2.3. How many two-letter *words* start with either A or B? (A word is just a sequence of letters; it doesn't have to be English, or even pronounceable; there are 26 letters in the English alphabet.)

Example 3.2.4. How many 10-bit strings of weight 6 start with either 11 or 00?

Example 3.2.5. How many 10-bit strings of weight 6 have at least one 1 in their first three bits?

13 Combining outcomes: Product Principle.

Example 3.2.6. How many two-letter words start with one of the 5 vowels?

Example 3.2.1. How many ways can you select a letter from $\{A, B, C, D, E\}$ followed by a digit from $\{1, 2, 3\}$?

Example 3.2.9. How many lattice paths from $(0, 0)$ to $(10, 10)$ pass through the point $(4, 7)$?

Example 3.2.10. How many license plates can you make out of three letters followed by three numerical digits?

Example 3.2.11. Suppose you roll a 12-sided die seven times, recording the number that appears after each roll. How many sequences of seven rolls are possible?

Example 3.2.12. How many different pizzas can you make if you can choose from 10 toppings and you can have any number of toppings on your pizza?

Example. Toss a coin 10 times. How many possible outcomes of this experiment can you get?

Example 3.3.8. How many 3-letter *words* (sequences of letters) are there when

- repeats are allowed?
- repeats are not allowed?

(The last example uses the Product Principle in the same way as we used it in DM1 for determining the number of permutations in V61: the sets of all possible outcomes in some step don't need to be the same, but as long as they have the same cardinalities, we are fine!)

14 Combining outcomes: combining principles.

Example on p.213. How many ways can you select two cards from a standard deck of 52, so that the first one is a red card and the second one is a face card?

Example 3.2.14. How many lattice paths from $(0, 0)$ to $(9, 9)$ pass through either $(2, 6)$ or $(6, 2)$?

Example 3.2.15. How many two-digit numbers, using only the digits from the set $\{1, 2, 3, 4, 5\}$ have the sum of their digits even?

More solved problems: on pp.215–217 (solutions on pp.482–484). Exercise 3.2.7.2 on p.217 is solved in V27, but I recommend that you try to solve it by yourself.

15 Combining outcomes: PIE.

Examples 3.3.2. and 3.3.5. How many 7-bit strings of weight 4 start with 11 or end with 00, or both?

Examples 3.3.7. How many of the numbers in $\{1, 2, \ldots, 50\}$ are multiples of 2, 3, or 5?

More solved problems: on pp.227–229 (solutions on pp.484–485).

16 Finally some formulas in Pascal's Triangle: read Section 3.4.

Example 3.4.1. How many sequences (permutations) are there of the letters a, b, c, d, e, f?

Example 3.4.4. How many four-letter *words* can you make from the letters a, b, c, d, e, f, g, with no repeated letters?

Example 3.4.8. Your basketball team has 12 players. Assuming everyone can play every position, how many ways can you choose 5 players to be on the court at the same time? (This example helps the Author finally derive the closed formula for $C(n, k)$.)

Example 3.4.11. How many 3-letter *words* are there in which

- the letters appear in alphabetical order?
- the letters in the word can come in any order?

(The last example illustrates some subtleties around the concept of order.)

More solved problems: on pp.241–242 (solutions on pp.485–487). Exercise 3.4.7.1 on p.243 is solved in V18, but I recommend that you try to solve it by yourself.

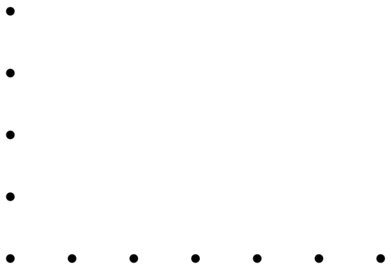
17 The same as above, formulated in terms of functions.

Given two sets K and N such that $|K| = k$ and $|N| = n$ (where $k, n \in \mathbb{N}^+$). Find the number of:

- all functions $f : K \to N$
- all injections $f : K \to N$
- all surjections $f : K \to N$
- all bijections $f : K \to N$
- all increasing (non-decreasing) functions $f : K \to N$, if $K = \{1, 2, \ldots, k\}$ and $N = \{1, 2, \ldots, n\}$.

18 Counting stuff, Problem 1.

Problem 1 (**Exercise 3.4.7.1** on p.243 in the DM Book): How many triangles are there with vertices from the points shown below? Note that we are not allowing degenerate triangles–ones with all three vertices on the same line–but we do allow non-right triangles. **Three methods for solving this problem will be given.**



Extra material: notes with solved Problem 1.

19 Counting stuff, Problem 2.

Problem 2: Answer both questions; solve the problems in two ways:

a) In a group of n people, in how many ways can you arrange them in pairs?

b) Given a convex polygon with n sides. How many diagonals does it have?

Extra material: notes with solved Problem 2.

20 Counting stuff, Problem 3.

Problem 3: Given set $\{1, 2, 3, \ldots, 2025\}$.

a) Determine the number of all permutations of its elements.

b) Determine the number of all the permutations such that 1 and 2 stand next to each other. (2 methods)

c) Determine the number of all the permutations such that 1, 2, and 3 stand next to each other, in this order.

d) Determine the number of all the permutations in which 1 stands to the right of 6. (2 methods)

e) Determine the number of all the permutations in which the elements are either arranged in the increasing order, or in the decreasing order, or first increasing, and then decreasing. (3 methods)

f) Determine the number of all permutations such that for all i we have $x_i \geqslant i - 3$.

21 Counting stuff, Problem 4.

Problem 4: Given set $A = \{1, 2, 3, \ldots, 9\}$.

a) Determine the number of all possible 8-digit numbers with different digits from A.

b) How many of these numbers are divisible by 15?

c) Let $n \in \mathbb{N}^+$. Determine the number of all n-digit numbers with digits from A for which the product of their digits is divisible by 10.

Extra material: notes with solved Problem 4.

22 Counting stuff, Problem 5.

Problem 5: Given a group of 40 people. We need to choose seven of them to form a committee: the chairman, the secretary, and five members. In how many ways can we form such a committee?

Extra material: notes with solved Problem 5.

23 Counting stuff, Problem 6.

Problem 6: Given set $A = \{1, 2, 3, \ldots, 3n\}$ for some natural number $n \geqslant 1$. We pick two numbers from this set.

a) In how many ways can we do this?

b) In how many ways can we do this, if we get an additional requirement that the sum of the chosen numbers must be divisible by 3?

Extra material: notes with solved Problem 6.

24 Counting stuff, Problem 7.

Problem 7: Given set $A = \{1, 2, 3, \ldots, 3n\}$ for some natural number $n \geqslant 2$. We pick four numbers from this set.

a) In how many ways can we do this?

b) In how many ways can we do this, if we get an additional requirement that the sum of the chosen numbers must be divisible by 3?

Extra material: notes with solved Problem 7.

25 Counting stuff, Problem 8.

Problem 8: How many ways can you place 5 rooks on an 8×8 chessboard? Consider two cases: 1. the rooks are indistinguishable, 2. the rooks are labeled with different numbers from 1 to 5. In both cases, how many arrangements of the rooks are such that no rook can capture another one?

26 Counting stuff, Problem 9.

Problem 9: In poker, one defines *full house* as hand with three cards of one rank and two of a second rank.

∗ In how many ways can one pick five cards from a deck of 52? In how many ways can one form *full house*? (The quotient of your results will give you the probability of getting *full house*.)

∗ Answer the same questions in a new situation: there are five cards missing in your deck; they are all hearts (ranks: 2, 5, 10, jack, and king).

Extra material: notes with solved Problem 9.

27 Counting stuff, Problem 10.

Example: How many factors does the number 60 have? Explain your answer using the multiplicative principle.

Problem 10 (**Exercise 3.2.7.2** on p.217 in the DM Book): Factor the number $735,000$. How many divisors does it have? Explain your answer using the multiplicative principle.

Extra material: notes with solved Problem 10.

28 Counting stuff, Problem 11.

Problem 11: Given the set $A = \{1, 2, 3, 4, 5, 6\}$. Determine the number of all the 6-digit numbers formed from the distinct digits from A. How many of them are divisible by 4?

Extra material: notes with solved Problem 11.

29 **Optional**: Counting stuff, Problem 12.

Problem 12: Numbers p and q are chosen randomly from the set $\{1, 2, \ldots, 10\}$

∗ Case 1: with replacement,

∗ Case 2: without replacement.

Determine, in each of the two cases, the number of such outcomes (p, q) that the roots of the quadratic equation $x^2 + px + q = 0$ are real.

30 Distributing stuff, without restrictions.

Examples of distributing stuff:

(1) How many ways can one distribute n balls over k boxes?

(2) How many ways can one distribute n cookies to k children?

(3) Three possible remainders in division by 3 over four positions (as in Problem 7 in Video 24).

31 Distributing stuff, with restrictions: back to some old problems from DM1.

Three equivalent problems, formulated in V60 of DM1:

(1) Given $n, k \in \mathbb{N}^+$ and $n \geqslant k$. Determine the number of positive natural solutions to $x_1 + x_2 + \ldots + x_k = n$.

(2) Given $n, k \in \mathbb{N}^+$ and $n \geqslant k$. We have k boxes and n (indistinguishable) objects. In how many ways can one put all these objects in the boxes in such a way that no box is empty?

(3) Given $n, k \in \mathbb{N}^+$ and $n \geqslant k$. A train has k compartments. In how many ways can you distribute n passengers (that are *indistinguishable* in the meaning that only the *number* of people counts, not who is where in particular) over these compartments so that no compartment is empty?

32 How they do this in the book: multisets, sticks and stones.

Example 3.5.2. You grab a handful of ten jelly beans from a bag that contains six flavors. Write down three possible outcomes using both multisets, strings of numbers, and sticks and stones.

Problem 3.5.5.1 (difference between sets and multisets):

∗ How many *sets* of size 9 can be made using the 10 numeric digits 0 through 9?

∗ How many *multisets* of size 9 can be made using the 10 numeric digits 0 through 9?

33 Sticks and stones: two more examples from the DM Book.

Example 3.5.6. How many integer solutions are there to the equation

$$x_1 + x_2 + x_3 + x_4 + x_5 = 13.$$

(An **integer solution** to an equation is a solution in which the unknown must have an integer value.)

∗ where $x_i \geqslant 0$ for each x_i?

∗ where $x_i > 0$ for each x_i?

∗ where $x_i \geqslant 2$ for each x_i?

Example 3.5.5. How many 7 digit phone numbers are there in which the digits are non-increasing? That is, every digit is less than or equal to the previous one.

34 Partitions of sets, multinomial coefficients, and permutations of multisets.

Ordered and unordered partitions:

∗ Example 1: Suppose set A has 7 elements. We want to find the number m of ordered partitions of A into three cells, say $[A_1, A_2, A_3]$, so that they contain 2, 3, and 2 elements, respectively.

∗ Example 2: Find the number m of ways to partition 10 students into four teams $[A_1, A_2, A_3, A_4]$ so that two teams contain 3 students and two teams contain 2 students.

∗ Example 3: We have six signal flags: three of them are blue, two of them are red, and one of them is white, and we will lift them all in a row, to send a signal. How many different signals can we produce in this way?

35 **Optional**: Partitions and distributions, some references.

36 **Optional**: A word about partitions and Stirling numbers of the second kind.

Stirling numbers (of the second kind) $S(n, k)$ show the number of *unordered* partitions of an n-set A into k *non-empty* parts, for $1 \leqslant k \leqslant n$. These numbers are sometimes denoted by $\left\{ {n \atop k} \right\}$.

Theorem: Let $1 \leqslant k \leqslant n$. The following holds:

$$S(n, 1) = 1, \qquad S(n, n) = 1, \qquad S(n, k) = S(n-1, k-1) + k \cdot S(n-1, k) \quad (2 \leqslant k \leqslant n-1).$$

Example 1: An illustration for Theorem above, and a *triangle* of values of $S(n, k)$ for some values of n and k.

Example 2: An illustration of the connection between Stirling numbers and multinomial coefficients: How can we partition a 5-element set into 3 (non empty) parts?

Lemma: Let S denote the set of surjections from an n-set A to a k-set X. Then $|S| = k! \cdot S(n, k)$. (See V41.)

Problem: Given two sets: $A = \{1, \ldots, 7\}$ and $B = \{1, \ldots, 13\}$. Determine the number of functions $f : A \to B$ that attain exactly four different values. How many of these functions attain at least one odd value?

37 **Optional**: A word about the *twelvefold way*.

38 A generalization of the Inclusion–exclusion principle.

Exercise: Assume that the formula $|A \cup B| = |A| + |B| - |A \cap B|$ is true for all finite sets A and B. Show that then also the formula $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$ is true for any three finite sets. The same method is used in the (induction) proof of a generalised PIE, for n finite sets, for the induction step (assuming that the formula, as given in the video, is true for n finite sets for some $n \geqslant 2$, we show that it is also true for $n+1$ finite sets). The base case: motivate with a picture, as in V115 of DM1.

Extra material: notes with solved Exercise.

39 Inclusion–exclusion principle formulated in the negative way.

Example: Let U be the set of positive integers not exceeding 1000. Then $|U| = 1000$. Find $|S|$, where S is the set of such positive integers that are not divisible by 3, 5, or 7.

40 PIE for multisets, two examples from the DM Book

Example 3.8.1 on p.292 in the DM Book: Three kids, Alberto, Bernadette, and Carlos, decide to share 11 cookies. They wonder how many ways they could split the cookies up provided that none of them receive more than 4 cookies (someone receiving no cookies is for some reason acceptable to these kids).

Example 3.8.3 on p.294 in the DM Book: Earlier (Example 3.5.6, Video 33) we counted the number of integer solutions to the equation

$$x_1 + x_2 + x_3 + x_4 + x_5 = 13$$

where $x_i \geqslant 0$ for all i. How many of those integer solutions have $0 \leqslant x_i \leqslant 3$ for each i?

41 Counting surjections.

Example: Let K and N be sets such that $|K| = 6$ and $|N| = 4$. Find the number of all the surjective (onto) functions from K onto N.

42 Fixed points of permutations, and derangements.

Exercise 3.8.6.2. Illustrate how the counting of derangements works by writing all permutations of $\{1, 2, 3, 4\}$ and then crossing out those which are not derangements. Keep track of the permutations you cross out more than once, using PIE.

43 Absent-minded-secretary problem.

Problem: An absent-minded secretary gets n letters that she must send to n different recipients (each letter contains the name of the person it is meant for). She puts each letter in one empty envelope and closes all of them. Then she remembers that she forgot to write addresses on the envelopes. She does it then without knowing which letter is in which envelope. In how many ways can she assign the recipients to envelopes? In how many of these cases at least one recipient gets the letter addressed to him (assuming that the secretary sends all the letters, and that the post is doing a good job)? This problem comes back in Section 4.

S3 Combinatorial (and not only) proofs

You will learn: various types of proofs of binomial identities, including direct proofs, proofs by induction, proofs by telescoping sums, and combinatorial proofs; this topic was already started in DM1, but now you will see more of it.

Read along with this section: *DM Book*, Section 3.6: *Combinatorial Proofs*, pp.256–272.

44 A list of formulas worth remembering, and where to find their derivation.

45 A really cool (non binomial) formula, Problem 1.

Problem 1: Find the following sum:

$$\frac{1^3}{1} + \frac{1^3 + 2^3}{1+3} + \frac{1^3 + 2^3 + 3^3}{1+3+5} + \frac{1^3 + 2^3 + 3^3 + 4^3}{1+3+5+7} + \ldots + \frac{1^3 + 2^3 + \ldots + n^3}{1 + 3 + \ldots + (2n-1)}.$$

Extra material: notes with solved Problem 1.

46 Various methods for proving formulas.

47 Telescoping sums with factorials, induction, Problem 2.

Problem 2: Prove that $1!\cdot 1+2!\cdot 2+3!\cdot 3+\ldots+n!\cdot n=(n+1)!-1.$

Extra material: notes with solved Problem 2.

48 Telescoping sums with factorials, induction, Problem 3.

Problem 3: Prove that

$$\frac{1}{2!}+\frac{2}{3!}+\frac{3}{4!}+\ldots+\frac{n}{(n+1)!}=1-\frac{1}{(n+1)!}.$$

Extra material: notes with solved Problem 3.

49 Absorption/extraction formula, direct and combinatorial proofs, Problem 4.

Problem 4: Prove (with help of direct and combinatorial proofs) the following formula for $n, k \in \mathbb{N}^+$:

$$\binom{n}{k}=\frac{n}{k}\binom{n-1}{k-1}.$$

This is a nice formula that can bring a constant factor in front of binomial coefficients; it will be used together with the formula from V59 somewhere at the end of Section 4. Also: for some formulas later in this section.

Extra material: notes with solved Problem 4.

50 Trinomial revision, a direct proof, Problem 5.

Problem 5: Prove the following formula (that will be later used in V61):

$$\binom{n}{m}\binom{n-m}{k-m}=\binom{n}{k}\binom{k}{m}, \quad 0\leqslant m\leqslant k\leqslant n.$$

A note on terminology: multinomial coefficients: binomial, trinomial, quadrinomial,... coefficients.

Ex1: A combinatorial proof of a special case of this identity from the DM Book, p.270.

Ex2: How many 10-letter words use exactly four A's, three B's, two C's, and one D? The DM Book, p.263.

Ex3: Determine the number of distinct permutations of the letters in the word MISSISSIPPI.

Extra material: notes with solved Problem 5.

51 Diagonal summation, Problem 6.

Problem 6: Prove (in **three** different ways!) the following formula:

$$\sum_{k=0}^{n}\binom{m+k}{m}=\binom{m+n+1}{m+1}, \quad n, m\geqslant 0.$$

Extra material: notes with solved Problem 6.

52 Parallel summation, Problem 7.

Problem 7: Prove (in a really **lazy** way) the following formula:

$$\sum_{k=0}^{m}\binom{n+k}{k}=\binom{n+m+1}{m}, \quad n, m\geqslant 0.$$

53 The one with squares, three proofs, Problem 8.

Problem 8: Prove the following formula for $n\in\mathbb{N}$: $\sum_{k=0}^{n}\binom{n}{k}^2=\binom{2n}{n}, \quad n\geqslant 0.$

You get two different solutions from the DM Book on pp.265–266, to read on your own. You will also see another solution, based on the Binomial Theorem. (Some additional explanation will be given in the beginning of V55.)

Note: The last part of this lecture (on a bluish background) contains some explanations (about **polynomials**) that can be helpful for a better understanding of V55 and V56; this part was recorded **after** V55 and V56.

54 Playing with the Binomial Theorem, Problem 9.

Problem 9: Some formulas you just get without any effort:

$$\sum_{k=0}^{n}\binom{n}{k}=\binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{n-1}+\binom{n}{n}=2^n$$

$$\sum_{k=0}^{n}2^k\binom{n}{k}=\binom{n}{0}+2\binom{n}{1}+\ldots+2^{n-1}\binom{n}{n-1}+2^n\binom{n}{n}=3^n$$

$$\sum_{k=0}^{n}(-2)^k\binom{n}{k}=\binom{n}{0}-2\binom{n}{1}+\ldots+(-2)^{n-1}\binom{n}{n-1}+(-2)^n\binom{n}{n}=(-1)^n$$

$$\sum_{k=0}^{n}3^k\binom{n}{k}=\binom{n}{0}+3\binom{n}{1}+\ldots+3^{n-1}\binom{n}{n-1}+3^n\binom{n}{n}=4^n$$

55 Another look at the *diagonal-summation formula* from V51, Problem 10.

Problem 10: Prove the following formula:

$$\binom{m}{m}+\binom{m+1}{m}+\ldots+\binom{n-1}{m}+\binom{n}{m}=\binom{n+1}{m+1}$$

(for $0 \leqslant m \leqslant n$) by using formula S1.6 from our list and the Binomial Theorem. Explain how this formula relates to the *Diagonal-summation* formula from V51.

Extra material: notes with solved Problem 10.

56 Playing with formulas, with a really clean solution from V55, Problem 11.

Problem 11: Find the coefficient at x^2 in $(1+x)^0+(1+x)^1+(1+x)^2+\ldots+(1+x)^{80}$.

Some old formulas will give us another proof for the equality from V55, in a special case (for $n=80$ and $m=2$).

Extra material: notes with solved Problem 11.

57 Two combinatorial proofs: ternary digit strings and pairs of subsets, Problem 12.

Problem 12 (**Exercise 3.6.6.11** on p.270): Let's count *ternary* digit strings, that is, strings in which each digit can be 0, 1, or 2.

- How many ternary digit strings contain exactly n digits?
- How many ternary digit strings contain exactly n digits and n 2s.
- How many ternary digit strings contain exactly n digits and $n-1$ 2s. (Hint: Where can you put the non-2 digit, and then what could it be?)
- How many ternary digit strings contain exactly n digits and $n-2$ 2s. (Hint: See previous hint.)
- How many ternary digit strings contain exactly n digits and $n-k$ 2s.
- How many ternary digit strings contain exactly n digits and no 2s. (Hint: What kind of a string is this?)
- Use the above parts to give a combinatorial proof for the identity (shown in V54).

$$\binom{n}{0}+2\binom{n}{1}+\cdots+2^{n-1}\binom{n}{n-1}+2^n\binom{n}{n}=3^n.$$

Just for fun: another combinatorial proof for the same identity. (BTW, the first solution can be repeated for quaternary, quinary, etc strings.)

58 A combinatorial proof: number of subsets with odd number of elements, Problem 13.

Problem 13 (**Exercise 3.6.6.13** on p.271): Establish the identity below (for all $n \geqslant 2$) using a combinatorial proof.

$$\binom{2}{2}\binom{n}{2}+\binom{3}{2}\binom{n-1}{2}+\binom{4}{2}\binom{n-2}{2}+\ldots+\binom{n}{2}\binom{2}{2}=\binom{n+3}{5}.$$

Try to solve this problem by yourself, after analysing Example 3.6.6 on p.264 in the DM Book.

Extra material: notes with solved Problem 13.

59 Vandermonde identity: choosing a team with members from two groups, Problem 14.

Problem 14: Show (with help of a combinatorial proof) that for each $m, n \in \mathbb{N}^+$ and for each $0 \leqslant r \leqslant m, n$

$$\sum_{i=0}^{r} \binom{n}{i}\binom{m}{r-i} = \binom{n}{0}\binom{m}{r} + \binom{n}{1}\binom{m}{r-1} + \binom{n}{2}\binom{m}{r-2} + \ldots + \binom{n}{r}\binom{m}{0} = \binom{n+m}{r}.$$

This identity will help us in computations somewhere at the end of Section 4, and earlier: in V61.

An observation: The *sum-of-squares* formula from V53 is a special case of the current one, with $m = n = r$.
Extra material: notes with solved Problem 14.

60 Choosing a committee, Problem 15.

Problem 15: Let $n \in \mathbb{N}^+$. Compute the following sum. Hint: use the *Absorption/extraction* formula from V49.

$$\sum_{k=1}^{n} k\binom{n}{k}.$$

I present three solutions:

1. one with help of the formula from V49,
2. one (**optional, advanced**) with help of Calculus,
3. one combinatorial.

Extra material: notes with solved Problem 15.

61 More binomial identities, Problem 16.

Problem 16: Prove the following identity. Hint: use the *Trinomial revision* formula from V50 and *Vandermonde identity* from V59.

$$\sum_{k=m}^{r+m} \binom{k}{m}\binom{m}{r+m-k}\binom{n}{k} = \binom{n}{m}\binom{n}{r}, \qquad (0 \leqslant r \leqslant m \leqslant n;\ \ r+m \leqslant n).$$

62 More binomial identities, Problem 17.

Problem 17: Let $n \in \mathbb{N}^+$. Compute the following sum. Hint: use the *Absorption/extraction* formula from V49. You get additionally a hard-core **optional, advanced** solution involving integrals (Calculus 2).

$$\sum_{k=0}^{n} \binom{n}{k} \cdot \frac{1}{k+1}.$$

Extra material: notes with solved Problem 17.

63 More binomial identities, Problem 18.

Problem 18: Prove the following identity. Hint: use the *Absorption/extraction* formula from V49.

$$\frac{2^1-1}{1}\binom{n}{0} + \frac{2^2-1}{2}\binom{n}{1} + \frac{2^3-1}{3}\binom{n}{2} + \ldots + \frac{2^{n+1}-1}{n+1}\binom{n}{n} = \frac{3^{n+1}-2^{n+1}}{n+1}.$$

Extra material: notes with solved Problem 18.

64 The last one, Problem 19.

Problem 19: Prove the following fact (monotonicity of binomial coefficients):

$$\binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{\lfloor n/2 \rfloor}, \quad n \geqslant 0.$$

Extra material: notes with solved Problem 19.

S4 A very brief introduction to (discrete) probability

You will learn: how Combinatorics can be applied for (discrete) Probability; this is **not** a formal course in Probability, just a demonstration of applications of some combinatorial methods for computing probabilities of events; some concepts (briefly) covered in the lectures: experiment, outcome, sample space, event, favourable event (all these were already covered in V9, here you get more examples involving coin toss, rolling dice, drawing balls from an urn, and playing poker), combining events (union and intersection of events), mutually exclusive events, complementary events, independent and dependent events, conditional probability, random variable and its expected value (just enough about it to fulfil the promise from Videos 49 and 59).

Read along with this section: *DM Book*, Section 3.7: *Applications to Probability*, pp.273–289.

65 A disclaimer.

66 Back to some stuff from V9, two examples.

Write down and depict the sample space Ω and the set of favourable outcomes for the events A_k, where:

a) **Experiment 1**: *rolling a die twice*; events A_k (for $k = 0, 1, \ldots, 13$): *the sum of the two results is* k.

b) **Experiment 2**: *tossing a coin four times*; events A_k (for $k = 0, 1, 2, 3, 4$): *the number of tails is* k.

67 Working with sample spaces and with events is just working with sets.

The following concepts are covered:

- *Sample space* and *simple* (or: *elementary, atomic*) *events* (*sample points*)
- An *event* as any subset of the sample space
- Relation of *inclusion* between events
- Combining events: *or*
- Combining events: *and*
- *Mutually exclusive events*
- *Complementary event*.

Illustrate the concepts on the following experiment (based on an example from V15): draw one number from the set $\{1, 2, \ldots, 50\}$. Describe the sample space Ω and define the following events:

A_2: *the drawn number is divisible by* 2, A_3: *the drawn number is divisible by* 3,

A_5: *the drawn number is divisible by* 5, A_6: *the drawn number is divisible by* 6,

A_{10}: *the drawn number is divisible by* 10, A_{15}: *the drawn number is divisible by* 15,

A_{30}: *the drawn number is divisible by* 30, B: *the drawn number is prime*, C: *the drawn number is* > 5.

68 Working with sample spaces and with events is just working with sets, Exercise.

Exercise: Let A, B, and C be three events in the sample space Ω. Write down (with help of set-theoretical symbols) events defined in the following ways:

(a) Only event A occurs, not the other two.

(b) Only events A and B occur, but not C.

(c) All the three events occur.

(d) At least one of these events occurs.

(e) At least two of these events occur.

(f) Exactly two of these events occur.

(g) Exactly one of these events occur.

(h) Not more than two of these events occur (but at least one does).

(i) None of these events occur.

Illustrate each of these situations with help of Venn diagram, where Ω is the entire universe, and A, B, and C are its subsets.

69 More formally about probability: Kolmogorov's axiomatic definition.

70 Some important properties of probabilities.

The following properties (theorems) of probability functions follow from the axiomatic definition:

T1 *Generalised additivity property (Sum Principle) for events that are mutually exclusive, pairwise*: If $A_1, \dots, A_n$ are such events that $A_i \cap A_j = \emptyset$ if $i \neq j$ (i.e., are mutually exclusive pairwise) then

$$P(A_1 \cup A_2 \cup \ldots \cup A_n) = P(A_1) + P(A_2) + \ldots + P(A_n).$$

T2 *Probability of the empty event*: $P(\emptyset) = 0$.

T3 *Monotonicity of probability functions*: $(A \subset B) \quad \Rightarrow \quad P(A) \leqslant P(B)$.

T4 *Upper bound*: $(A \subset \Omega) \quad \Rightarrow \quad P(A) \leqslant 1$.

T5 *The Subtraction Principle*: $(A \subset B) \quad \Rightarrow \quad P(B \setminus A) = P(B) - P(A)$.

T6 *Probability of the complementary event*: $P(A^c) = 1 - P(A)$.

T7 *PIE for probabilities*: $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.

T8 *Probability of the union is less than or equal to the sum of probabilities*:

$$P(A_1 \cup A_2 \cup \ldots \cup A_n) \leqslant P(A_1) + P(A_2) + \ldots + P(A_n).$$

T9 *PIE3 for probabilities*: $P(A \cup B \cup C) = P(A) + P(B) + P(C) - P(A \cap B) - P(A \cap C) - P(B \cap C) + P(A \cap B \cap C)$.

T10 *PIEn for probabilities*: A similar formula as in V38 (the same, but with $P(A)$ etc instead of $|A|$ etc).

71 A finite sample space and uniform distribution of probability.

Exercise: Use the examples from V67 (divisibility) for testing the properties formulated and proved in V70.

72 Computing probabilities, Example 1.

Example 1: Compute the probabilities of all the events defined in V66, for both experiments.

73 Computing probabilities, Example 2.

Example 2: Compute the probabilities of the events defined in part (b) in V23 and V24.

74 Computing probabilities, Example 3.

Example 3: Compute the probabilities of the events defined in V29 (the optional one), both cases.

75 Computing probabilities, Example 4.

Example 4: Compute the probabilities of the events defined in (b) and (c) in V21.

76 Computing probabilities, Example 5.

Example 5: A train has k compartments and n passengers enter the (empty) train, randomly taking places. What is the probability that they will get distributed so that no compartment is empty?

77 Studying together, Problem 1.

Problem 1: Two girls and three boys from high school Lycée 4 study for their finals. Each day they go to the park and sit on a bench there reading, studying, and solving problems together. The way they pick places on the bench is random. What is more probable: that the two girls will sit next to each other or that they will be separated?

Extra material: notes with solved Problem 1.

78 Taking the train, Problem 2.

Problem 2: An empty train has 3 compartments. Nine people enter and take places randomly. How probable is

a) that there are three persons in the first compartment,

b) that there are three persons in each compartment,

c) that there are four passengers in one compartment, three in another one, and two in the remaining one.

Extra material: notes with solved Problem 2.

79 Picking random numbers, Problem 3.

Problem 3: We pick (randomly) one number from the set $\{1, 2, 3, \ldots, 50 \cdot 10^9\}$ (up to 50 billion). What is the probability of picking a number whose digits (in the decimal system) form a non-decreasing sequence (from the left to the right).

Extra material: notes with solved Problem 3.

80 Arranging people in pairs, Problem 4.

Problem 4: We have a group of 20 people: ten boys and ten girls. We are supposed to arrange them in groups of two, in a random way. What is the probability of the event where each pair contains people of different genders?

Extra material: notes with solved Problem 4.

81 Looking for shoes, Problem 5.

Problem 5: We have m (different, distinguishable) pairs of shoes. We pick (randomly, without looking) $2r$ shoes, where $2r < m$. Compute the probability that among the chosen shoes:

a) there is not even one pair (i.e., matching shoes)
b) there is exactly one pair
c) there are exactly two pairs.

Extra material: notes with solved Problem 5.

82 The One with All the Poker, Problem 6.

Problem 6: Compute the probability of the following hands in poker:

a) Royal flush
b) Straight flush
c) Four of a kind
d) Full house
e) Flush
f) Straight
g) Three of a kind
h) Two pair
i) One pair
j) High card.

(The meaning of these names is explained in the video.)

83 Weird poker, continuation from V26, Problem 7.

Problem 7: In poker, one defines *full house* as hand with three cards of one rank and two of a second rank.

∗ In how many ways can one pick five cards from a deck of 46?
∗ There are five cards missing in your deck; they are all hearts (ranks: 2, 5, 10, jack, and king). If you had to lose one more card, what type should it be to get the largest probability of getting full house using the 46-card deck?

84 The Sum and the Product Rules in diagrams, Example 6.

Example 6: We have a non-transparent sack with five balls: two black and three white. Our experiment is drawing (randomly, without looking) one ball, and then another one.

∗ Case 1: with replacement,
∗ Case 2: without replacement.

Illustrate the space of all the possible outcomes. We define three events: A: both balls are black, B: both balls are white, C: the balls are of different colours. In both cases, show the favourable outcomes in your illustrations, and determine their number. Determine $P(A)$, $P(B)$, and $P(C)$.

85 Repeated experiments and Cartesian products of multiple sets, Example 7.

Example 7 (back to Experiment 2 from V66, one with [naturally] the same set of outcomes at each time): Tossing a coin four times, compute (and illustrate) the probabilities of the following events:

- ⋆ A: The result of the second toss is heads (0)
- ⋆ B: The result of the third toss is tails (1)
- ⋆ $A \cap B$: The result of the second toss is heads (0) **and** the result of the third toss is tails (1).

86 Some examples from the DM Book.

Example 3.7.7. Suppose you flip a coin 10 times. What is the probability that you will get at least one heads?

Examples 3.7.8. What is the probability that you will roll at least one 6 in four rolls of a fair 6-sided die?

87 A word about independent events.

Example 3.7.11 from the DM Book: What is the probability of getting an even number when rolling a 6-sided die and a heads when flipping a coin?

Back to the examples from V85 (illustrating the intuition around the concept) and from V67 (formally correct but not contributing to our understanding).

88 A word about conditional probability, Example 8.

Example 8: In a group of w women and m men, w_1 women and m_1 men play football and $w_2 = w - w_1$ women and $m_2 = m - m_1$ men don't. We pick (without looking and randomly; for example from a list) one person. What is the probability that this person doesn't play football if we know that it is a woman?

89 Random variable and its distribution.

Each event can be described in terms of a random variable: we look back at the example from V66.

90 Random variable and its distribution, Example 9.

Example 9 (back to Experiment 1 from V66): in the experiment of rolling a die twice, our random variable is the sum of the two results. Describe the distribution of this variable.

91 Random variable and its distribution, Example 10.

Example 10: We pick 5 cards from a regular deck of 52 cards. Our random variable is the number of Spades ♠ among the chosen cards. Describe the distribution of this variable.

Extra material: notes with solved Example 10.

92 Expected value of a random variable.

We look back at the example from V66 and V89: expected value there is simply the probability of the event.

93 Expected value of a random variable, Example 11.

Example 11: We roll a die once. The random variable is the number that we got. Compute its expected value.

Extra material: notes with solved Example 11.

94 Expected value of a random variable, Example 12.

Example 12: Compute expected value of the random variable described in V90.

95 Expected value of a random variable, Example 13.

Example 13: We toss a coin 6 times. Our random variable is defined as the number of tails. Find its distribution and expected value. Generalize for the experiment of tossing the coin n times.

Extra material: notes with solved Example 13.

96 Expected value of a random variable, Problem 8.

Problem 8: Compute the expected value of the variable from V91.

Extra material: notes with solved Problem 8.

97 Back to the absent-minded secretary, Problem 9.

Problem 9 (back to the problem from V43): Using the formulas derived in Videos 42 and 43, it is very easy to compute the probability of the event that our secretary sends at least one letter to the right recipient (do it). What number is this probability approaching when n (the number of all letters) tends to infinity? (This type of questions are usually answered in a Calculus class, but you will get a nice MANIM-based visual.)

S5 An introduction to Number Theory

You will learn: divisibility, prime factorisation, finding primes (sieve of Eratosthenes), Euclid's algorithm for multiple purposes (finding the gcd [*greatest common divisor*] and lcm [*least common multiple*] of two natural numbers, solving Diophantine equations, and solving linear equations in modular arithmetic [in Section 6]), Euler's totient function, the sum-of-all-divisors formula, number representation in different position systems (decimal, binary, etc), converting numbers from decimal to other bases (and back). This is **not** a complete course in Number Theory (which is a huge branch of Maths!), just a basic introduction to some of its topics, the ones that are usually a part of DM courses.

Read along with this section: *DM Book*, Section 6.2: *Introduction to Number Theory*, pp.432–448.

Mathematics for CS, Chapter 9: *Number Theory*, pp.341–420 (some chosen parts).

98 Number Theory in DM1 (listed in V3) and later in DM2.

The following concepts: divisor, prime number, relatively prime numbers.

99 A current-years problem, Problem 2025–2029.

Problem 2025–2029: How many zeros are there at the end of 2025!? These are often called *trailing zeros*. The same answer holds for 2026!, 2027!, 2028!, and 2029!.

100 Every second, every third, etc, Problem 1.

Problem 1: Show that the number $n^2(n^2-1)(n^2-4)$ is divisible by 360 for all integers n.

Extra material: notes with solved Problem 1.

101 Every second, every third, etc, Problem 2.

Problem 2: Let $n \in \mathbb{N}$ be such that $n > 2$. Show that if one of the numbers $2^n - 1$ or $2^n + 1$ is prime, then the other one is composite.

Extra material: notes with solved Problem 2.

102 Divisibility and induction, Problem 3.

Problem 3: Show that for each natural number n we have $7|(2^{n+2} + 3^{2n+1})$.

Extra material: notes with solved Problem 3.

103 Divisibility and factoring, Problem 4.

Problem 4: Show that the number $n^4 + 2n^3 - n^2 - 2n$ is divisible by 12 for all integers n.

Extra material: notes with solved Problem 4.

104 Divisibility and Binomial Theorem, Problem 5.

Problem 5: Show that for each natural number n we have $74|(6^{4n} + 38^n - 2)$.

Extra material: notes with solved Problem 5.

105 Remainders in division by three of the squares of natural numbers, Problem 6.

Problem 6: Show that if both p and $p^2 + 8$ are prime, then also $p^3 + 4$ is prime.

Extra material: notes with solved Problem 6.

106 A really cool divisibility problem with factorial, Problem 7.

Problem 7: Find all the pairs of positive integers (n, k) such that $n! + 8 = 2^k$.

Extra material: notes with solved Problem 7.

107 Finding prime numbers: sieve of Eratosthenes, Example 1.

Example 1: Find all the prime numbers that are less than or equal to 200, using sieve of Eratosthenes.

Extra material: notes with solved Example 1.

108 Sieve of Eratosthenes: why it works.

109 Some basic properties of divisibility.

Theorem: Suppose a, b, c are integers.

1. Here $a, b \neq 0$. If $a|b$ and $b|c$, then $a|c$ (transitivity)
2. Here $a \neq 0$. If $a|b$ then, for any integer x, $a|bx$
3. Here $a \neq 0$. If $a|b$ and $a|c$, then $a|(b+c)$ and $a|(b-c)$
4. Here $a \neq 0$. If $a|b$ and $b \neq 0$, then $a = \pm b$ or $|a| < |b|$
5. Here $a, b \neq 0$. If $a|b$ and $b|a$, then $|a| = |b|$, i.e., $a = \pm b$
6. Here $a \neq 0$. If $a|1$, then $a = \pm 1$.

Extra material: notes from the iPad, with a proof of the Theorem.

110 Gcd (*greatest common divisor*) and lcm (*least common multiple*), Example 2.

Example 2: Motivate the usefulness of gcd and lcm on the examples of simplifying and adding fractions.

111 How to get gcd and lcm from the prime factorisation of a number.

Show how to localise the gcd and lcm of the numbers 15 and 6 in Hasse's diagram for 60 (from V27).

Answer the question posed in the subject of this video.

Show that $a \cdot b = \operatorname{lcm}(a, b) \cdot \gcd(a, b)$.

112 A word about linear combinations.

Lemma: If d is a common divisor of integers a and b, then d is also a common divisor of all their linear combinations with integer coefficients.

Conclusion (from Lemma and Property (6) from V109): If some linear combination (with integer coefficients) of integers a and b is equal to 1, then a and b are relatively prime.

Note: The Conclusion is actually an IFF statement! (See V114 and V115.)

113 Division with remainder.

Theorem: If a and b are positive integers, then there exist q (*quotient*) and r (*remainder*) in $\mathbb{N}$ such that

$$a = bq + r \qquad \text{and} \qquad 0 \leqslant r < b.$$

114 One of the most important tools in Number Theory: Euclid's algorithm, Example 3.

Example showing that prime factorisation can be really, really hard: factor $2^{67} - 1$.

Example 3: Euclid's algorithm performed for 4734 and 1914.

115 One of the most important tools in Number Theory: Euclid's algorithm, continued.

Theorem: Let a and b be positive integers, and let $d = \gcd(a, b)$. Then there are integers m and n such that

$$d = ma + nb \qquad \text{(Bézout's identity).}$$

Corollary: Let a and b be positive integers that are relatively prime, i.e., $\gcd(a, b) = 1$. Then there are integers m and n such that (**Note**: This is an **if-and-only-if** condition for a and b being relatively prime!)

$$ma + nb = 1.$$

Fact: Euclid's algorithm gives us both gcd and lcm.

Question: Can we get a similar result if some of the numbers (a, b, or both) are **negative**?

116 Plenty of exercises for Euclid's algorithm, Example 4.

Ex 4: Compute the gcd and lcm for $a = 29$ and $b = 24$, and represent the gcd as a linear combination of a&b.

Extra material: notes with solved Example 4.

Extra material: an article with more solved problems on Euclid's algorithm. In all problems beneath, compute the gcd and lcm for a and b, and represent the gcd as a linear combination of a and b:

- ⋆ **Extra problem 1**: $a = 69, b = 49$
- ⋆ **Extra problem 2**: $a = 69, b = 48$
- ⋆ **Extra problem 3**: $a = 67, b = 29$
- ⋆ **Extra problem 4**: $a = 75, b = 64$
- ⋆ **Extra problem 5**: $a = 15, b = 13$
- ⋆ **Extra problem 6**: $a = 132, b = 77$
- ⋆ **Extra problem 7**: $a = 133, b = 56$
- ⋆ **Extra problem 8**: $a = 315, b = 305$.

We will revisit these examples later, in the context of solving Diophantine equations (Video 129).

117 Finally, a proof promised in V43 of DM1.

Theorem: If $n \in \mathbb{Z}$, two (non-zero) integers p and q are relatively prime and both divide n, then also their product divides n. (Illustrate with an example that the theorem is not true if p and q are **not** relatively prime.) Sketch the proof (by induction) that the statement can be generalised for any number of relatively prime divisors of n: $p_1, p_2, \ldots, p_k$.

Extra material: notes from the iPad.

118 Two lemmas for the next lecture.

Lemma 1 (divisibility of a product): If a prime number p divides the product mk then in must divide at least one of the factors m or k.

Lemma 2 (generalisation): If a prime number p divides the product $k_1 k_2 \cdot \ldots \cdot k_n$ then in must divide at least one of the factors k_i.

Exercise: Show that the lemma is not true if p is **not** a prime number.

Extra material: notes from the iPad.

119 Back to the factorisation theorem (V17 and V234 in DM1).

Fundamental Theorem of Arithmetic: Every integer $n \geqslant 2$ can be factored as

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdot \ldots \cdot p_N^{\alpha_N},$$

where all p_i are prime numbers and all α_i are positive natural numbers (proven in DM1, V234).

If $p_1 < p_2 < \ldots < p_N$ then the factorisation is **unique**.

120 The sum-of-all-divisors formula.

Sum of all natural divisors of a natural number $n \geqslant 2$ decomposed as in V119:

$$\sigma_1(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_N^{\alpha_N+1} - 1}{p_N - 1} = \prod_{i=1}^{N} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1},$$

where the p_i and α_i are as in the formula from V119.

121 A really cool formula, good to have for V123.

If $x_1, x_2, ..., x_n$ are any real numbers, then

$$\prod_{i=1}^{n}(1 - x_i) = 1 - \sum_{i=1}^{n} x_i + \sum_{1 \leqslant i < j \leqslant n} x_i x_j - \sum_{1 \leqslant i < j < k \leqslant n} x_i x_j x_k + \ldots + (-1)^n \prod_{i=1}^{n} x_i.$$

This formula can be proven by induction, but I will only write it for $n = 2$ and $n = 3$, so that one can see what would happen in the induction step.

Extra material: notes from the iPad.

122 A prelude to V123, Example 5.

Example 5: How many numbers from the set [60] are relatively prime with 60?

Confirm the result with help of the formula from V123.

Extra material: notes with solved Example 5.

123 Euler's totient function.

Theorem: Let $n \geqslant 2$ be a natural number. The number $\varphi(n)$ of positive integers up to n that are *relatively prime* with n is:

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_N}\right) = n\prod_{i=1}^{N}\left(1-\frac{1}{p_i}\right) = n\prod_{p|n}\left(1-\frac{1}{p}\right),$$

where the p_i are as in the decomposition formula from V119.

124 Diophantine equations: what, why, and how.

Theorem: If $a, b, c \in \mathbb{Z} \setminus \{0\}$, then the equation $ax + by = c$ has an integer-number solution (x, y) iff $d|c$, where $d = \gcd(|a|, |b|)$. If the equation has one solution (x_0, y_0), then it has infinitely many solutions expressed by:

$$(x, y) = \left(x_0 + k\cdot\frac{b}{d},\ \ y_0 - k\cdot\frac{a}{d}\right) \qquad (\text{for all } k \in \mathbb{Z}).$$

The solutions given above are forming the *entire* solution set (i.e., these are *all* the solution the equation has). The solution set is empty if $d \not| c$.

125 Diophantine equations, a word problem, Example 6.

Example 6: You have \$20 and you want to buy 12-cent and 16-cent stamps, **using exactly \$20**. Is it possible? If so, how many of each type can you buy (with the restriction that there must be at least one of each kind)?

Extra material: notes with solved Example 6.

126 Diophantine equations, negative coefficients and additional conditions, Example 7.

Example 7: Find all the integer-number solutions to the equation $10x - 22y = 2$ that satisfy the condition $0 \leqslant x \leqslant 21$.

Extra material: notes with solved Example 7.

127 A word about straight lines in the plane and their equations.

Some examples of equations of straight lines in the plane (slope-intercept equations, standard equations).

128 Diophantine equations with a geometric interpretation, Example 8.

Example 8: Solve the equations $2x + 4y = 3$, $2x + 4y = -2$, and $5x + 3y = 4$ in integer numbers. Give a geometric illustration in terms of straight lines and integer-coordinate points belonging to them.

129 Diophantine equations, a lot of practice, Example 9.

Example 9: Solve the equation $24x + 29y = 2$ in integer numbers.

Extra material: notes with solved Example 9.

Extra material: an article with more solved problems on Diophantine equations. In all problems beneath, solve the equations in integer numbers:

- ⋆ **Extra problem 1**: $69x + 49y = 5$
- ⋆ **Extra problem 2**: $69x + 48y = 5$, $\quad 69x + 48y = 6$
- ⋆ **Extra problem 3**: $67x + 29y = 2569$
- ⋆ **Extra problem 4**: $64x + 75y = 1$
- ⋆ **Extra problem 5**: $13x + 15y = 1$

- ⋆ **Extra problem 6**: $132x + 77y = 66$
- ⋆ **Extra problem 7**: $133x + 56y = 98$
- ⋆ **Extra problem 8**: $315x + 305y = 15$
- ⋆ **Extra problem 9** (another word problem): You are given an unlimited supply of water, a large container, and two jugs whose capacities are 7 litres and 9 litres. How would you put one litre of water in the container?

130 Positional number systems: Decimal system.

Number representation in decimal system; some examples of addition ($758 + 4\,366 = 5\,124$), multiplication ($247 \cdot 65 = 16\,055$), and subtraction. The result of $10^n - 1$ computed formally (as support for the next video).

131 Positional number systems: Binary system.

Converting from binary to decimal: Express the binary number 11011100001_2 in the decimal system.

Converting from decimal to binary: Express the number 777_{10} in the binary system.

Subtracting 1 from the least binary number with $n+1$ digits: We revisit the example from the previous lecture, computing $2^n - 1$.

132 Positional number systems: any base works fine.

Converting from binary to bases 4, 8, and 16: Express the number 11011100001_2 in bases 4, 8, and 16.

Converting from decimal to bases 4, 8, and 16: Express the number 777_{10} in bases 4, 8, and 16, using its binary representation, as in the previous exercise. Repeat the method from V131 to number 777_{10} (in bases 4, 8, and 16) and compare the results with the previous ones.

Subtracting 1 from the least number with $n + 1$ digits in some base: We revisit the example from the previous lecture, computing $b^n - 1$ for $b = 3, 4, 8, 16$.

133 Comparing numbers, Exercise 1.

Exercise 1: Order the following numbers from the least to the greatest:

$$2655_8, \quad 112231_4, \quad 1001010110_2, \quad 1238_{10}.$$

Extra material: notes with solved Exercise 1.

134 Arithmetic in various positional number systems, Exercise 2.

Exercise 2: Solve the following problems in two ways, given that we know from V131 that $11011100001_2 = 1761_{10}$ and $1100001001_2 = 777_{10}$:

$$11011100001_2 + 1100001001_2, \quad 11011100001_2 \cdot 1100001001_2, \quad 11011100001_2 - 1100001001_2.$$

Extra material: notes with solved Exercise 2.

135 Arithmetic in various positional number systems, Exercise 3.

Exercise 3: Multiply 1032_4 by 131_4. Represent the result as a binary number, and then as a number in positional systems with bases 4, 8, and 16.

Extra material: notes with solved Exercise 3.

136 Where can you learn more advanced stuff about different kinds of numbers.

137 **Optional**: Some really, really cool stuff for the last one.

First I show that $0.999\ldots = 1$ in the decimal system. In the same way: $0.111\ldots = 1$ in the binary system and $0.(b-1)(b-1)(b-1)\ldots = 1$ in the system with base b (where $b \geqslant 2$ is a natural number). I show the explanation with help of a well-known formula (S1.6 from our list) and with help of a picture (for $b = 2$). At the end I show a very nice derivation of the formula for $1 + q + q^2 + \ldots + q^n$ (that is the special case of the formula S1.6 that we need for this lecture).

S6 Modular arithmetic

You will learn: the basics of modular arithmetic: addition, subtraction, multiplication, raising to a power; properties of modular arithmetic; relation modulo n as an equivalence relation, equivalence classes and their representatives; tests for divisibility (by 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16); solving congruences, systems of congruences (with a reference to Chinese Remainder Theorem), linear equations, and systems of linear equations in $\mathbb{Z}_n$ for different numbers n; Fermat's Little Theorem with several proofs, one of them really exciting (combinatorial); Euler's Totient Theorem; some earlier problems are revisited and solved with new methods.

Read along with this section: *DM Book*, Section 6.2: *Introduction to Number Theory*, pp.432–448.

Mathematics for CS, Chapter 9: *Number Theory*, pp.341–420 (some chosen parts).

138 What is *modular arithmetic.*

Two examples that show computations modulo 12 when working with an analogue watch.

139 Back to the (equivalence) relation of congruence modulo n.

Terminology and notation, with examples for $n = 5$:

- equivalence classes under such relation are called *residue classes modulo n*,
- *representative of a class*,
- *complete residue system modulo n*,
- $\mathbb{Z}_n$ (that will be one of the celebrities of Section 7).

Examples: Compute $57 \pmod 3$, $58 \pmod 3$, $40 \pmod{19}$, $17 \pmod{30}$, $14 + 15 \pmod{30}$, $14 + 15 \pmod{13}$.

140 Basic properties of modular arithmetic, with proofs and examples.

Properties: We know from DM1 (V170) that the congruence relation modulo n for each fixed natural number $n \geqslant 2$ is *reflexive*, *symmetric*, and *transitive*. Now we establish more properties; they are easy to prove, but very practical to have, as will be illustrated in later lectures. In all the properties beneath, we assume that $n \geqslant 2$ is a fixed natural number, that $a_1 \equiv b_1 \pmod n$ and $a_2 \equiv b_2 \pmod n$ (or, in some cases, $a \equiv b \pmod n$). Then:

P1 for all integers k we have $a + k \equiv b + k \pmod n$; this property of the congruence relation is called *compatibility with translation*,

P2 for all integers k we have $a \cdot k \equiv b \cdot k \pmod n$; *compatibility with scaling*,

P3 $a_1 + a_2 \equiv b_1 + b_2 \pmod n$; *compatibility with addition*,

P4 $a_1 - a_2 \equiv b_1 - b_2 \pmod n$; *compatibility with subtraction*,

P5 $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod n$; *compatibility with multiplication*,

P6 for all integers $k \geqslant 0$ we have $a^k \equiv b^k \pmod n$; *compatibility with exponentiation*,

P7 for all polynomials p with integer coefficients $p(a) \equiv p(b) \pmod n$; *compatibility with polynomial evaluation*.

141 Addition and multiplication in $\mathbb{Z}_n$ and their properties.

Operations $\oplus$ and $\odot$ satisfy the following rules, where x, y, z denote *any* members of $\mathbb{Z}_n$, and $0 = [0]_n$, $1 = [1]_n$:

A1 $x \oplus y \in \mathbb{Z}_n$ ($\mathbb{Z}_n$ is closed under addition)

A2 $x \oplus y = y \oplus x$ (commutativity)

A3 $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ (associativity)

A4 $x \oplus 0 = x = 0 \oplus x$ for all $x \in \mathbb{Z}_n$ (neutral element of addition, zero)

A5 For each $x \in \mathbb{Z}_n$ there exists an element $x' \in \mathbb{Z}_n$ s.t. $x \oplus x' = x' \oplus x = 0$. This element x' is denoted $-x$ (additive inverse, the negative/opposite of x)

M1 $x \odot y \in \mathbb{Z}_n$ ($\mathbb{Z}_n$ is closed under multiplication)

M2 $x \odot y = y \odot x$ (commutativity)

M3 $x \odot (y \odot z) = (x \odot y) \odot z$ (associativity)

M4 $1 \odot x = x = x \odot 1$ for all $x \in \mathbb{Z}_n$ (neutral element of multiplication, identity, one)

D $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$ (distributivity).

Illustrations showing addition and multiplication modulo 5 and modulo 6.

142 Divisibility tests: by 2, 4, 8, 16, 5, and 10.

Examples: Show that the following numbers are divisible by 16: $1\,012\,064,\ 5\,132\,704,\ 1\,011\,276\,720$.

Extra material: notes from the iPad (the test and some examples).

143 Divisibility tests: by 3, 6, 9, 12, and 15.

Extra material: notes from the iPad (derivations of the tests).

144 Divisibility by 12, an example.

Example: Show that a standard circular watch (see illustration in the presentation) will be showing exactly the same time as now in 748 212 hours, assuming that it will always be working perfectly correctly.

Extra material: notes from the iPad (derivations of the tests, and some examples).

145 Divisibility by 9, an example of application.

Example: Use the result from V143 to show (without performing the multiplication) that the following computation is not correct:

$$54\,321 \cdot 98\,765 = 5\,363\,013\,565.$$

Extra material: notes with solved Example.

146 Divisibility test by 11.

Examples: Show that the following numbers are divisible by 11: $718\,608,\ 69\,582\,579$.

Extra material: notes from the iPad (derivations of the tests, and some examples).

147 Divisibility tests: by 7, 13, and 14.

Example: Show that $2\,279\,668\,846$ is divisible by 7, 13, and 14.

Extra material: notes with solved Example.

148 Solving congruences: looking for ones or minus ones.

Example: Determine $49^{3857} \pmod{25}$.

Extra material: notes with solved Example.

149 Solving congruences: looking for ones or minus ones, Exercise 1.

Exercise 1: Determine $3^{31} \pmod 7$. (Will be revisited in V156.)

Extra material: notes with solved Exercise 1.

150 Solving congruences: looking for ones or minus ones, Exercise 2.

Exercise 2: Determine $17^{64} \pmod 7$. (Will be revisited in V156.)

Extra material: notes with solved Exercise 2.

151 Solving congruences: looking for ones or minus ones, Exercise 3.

Exercise 3: Determine $47^{109} \pmod{15}$.

Extra material: notes with solved Exercise 3.

152 Solving congruences: looking for ones or minus ones, Exercise 4.

Exercise 4: Determine $32^{19} \pmod 5$.

Extra material: notes with solved Exercise 4.

153 Three earlier divisibility problems revisited, Exercise 5.

Exercise 5: Show that the following statements are true for all $n \in \mathbb{N}$:

- $\ast$ Proven in V102 in this course (by induction): $7|(2^{n+2} + 3^{2n+1})$.
- $\ast$ Proven in V236 in DM1 (by induction): $11|(2^{6n+1} + 3^{2n+2})$.
- $\ast$ Proven in V236 in DM1 (by induction): $133|(11^{n+2} + 12^{2n+1})$.

Extra material: notes with solved Exercise 5.

154 Three earlier divisibility problems revisited, Exercise 6.

Exercise 6: Show that the following statements are true for all $n \in \mathbb{N}$:

- Proven in V104 in this course (with help of the Binomial Theorem): $74 | (6^{4n} + 38^n - 2)$.
- Proven in V235 in DM1 (by induction): $9 | (2^{2n+1} + 3n + 7)$.
- Proven in V235 in DM1 (by induction): $9 | (4^n + 15n - 1)$.

Extra material: notes with solved Exercise 6.

155 Two cancellation properties.

Let n be a fixed natural number $n \geqslant 2$. Then:

C1 for all integers k we have $a + k \equiv b + k \pmod{n} \;\Rightarrow\; a \equiv b \pmod{n}$ (see P1 from V140).

C2 If $ca \equiv cb \pmod{n}$ and $\gcd(c, n) = 1$ then $a \equiv b \pmod{n}$.

L Lemma (for C2): If $n | cd$ and $\gcd(c, n) = 1$ then $n | d$. (This lemma was used at the very end of V124.)

Example: Show that the second cancellation property doesn't work if n and c are *not* relatively prime.

Extra material: notes from the iPad.

156 Fermat's Little Theorem: a formulation and an example of application.

Fermat's Little Theorem: If p is a *prime number*, then for every integer a the number $a^p - a$ is a multiple of p:

$$a^p \equiv a \pmod{p}.$$

Corollary: If p is a *prime number* and a is an integer such that $\gcd(a, p) = 1$ then $a^{p-1} - 1$ is a multiple of p:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Examples: Determine $3^{31} \pmod{7}$ (revisited from V149), $17^{64} \pmod{7}$ (revisited from V150), and $53^{100} \pmod{101}$.

157 Fermat's Little Theorem: proof 1 (by induction and Binomial Theorem).

158 Fermat's Little Theorem: proof 2 (beautiful combinatorics).

159 Fermat's Little Theorem and Euler's Totient Theorem: proof 3.

Lemma: If p is a prime number and $S = \{1, 2, 3, \dots, p-1\}$, then we define for each $a \in S$ the set $a \cdot S$ consisting of the products of the elements in S with a, taken modulo p. The set $a \cdot S$ is, for each $a \in S$, equal to S [i.e., $(1a, 2a, 3a, \dots, (p-1)a)$ is a **permutation** of $(1, 2, 3, \dots, p-1)$]. Moreover, none of these permutations have any fixed points (i.e., they are **derangements**), except for the permutation corresponding to $a = 1$, which has all its points fixed.

Euler's Totient Theorem: If a and n are *relatively prime* positive integers, then

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

where φ is Euler's totient function introduced in V123.

160 Playing with Fermat's Little Theorem and various patterns, Exercise 7.

Exercise 7: Show that $n^7 - n$ is divisible by 42 for any $n \in \mathbb{N}$.

(The same method can be used for V43 and V45 in DM1, to show that $n^3 - n$ is divisible by 6 and $n^5 - n$ is divisible by 30 for each $n \in \mathbb{N}$. We look together at $n^k \pmod{m}$ for $2 \leqslant m \leqslant 9$ and $1 \leqslant k \leqslant 5$ that help us formulate many divisibility statements [see the slides].)

161 Solving linear equations in real numbers, and what is different in $\mathbb{Z}_n$.

Example: Solve (using the picture from V141) the equation $3x = 3$ in $\mathbb{Z}_6$. Strange result? What about $3x = 4$?

Example: Rewrite the equations: $33x = 15$ in $\mathbb{Z}_6$, $34x = -14$ in $\mathbb{Z}_{31}$, $50x = -1$ in $\mathbb{Z}_{27}$, $12x - 10 = 20$ in $\mathbb{Z}_5$.

162 Linear equations in $\mathbb{Z}_n$, Exercise 8.

Exercise 8: Solve the equation $4x = 1$ in $\mathbb{Z}_5$. Do it in two ways: graphically (using the pictures from V141), and by plugging in all the elements of $\mathbb{Z}_5$ and verifying.

163 Linear equations in $\mathbb{Z}_n$, Exercise 9.

Exercise 9: Solve the equation $3x + 5 = 7$ in $\mathbb{Z}_8$ by plugging in all the elements of $\mathbb{Z}_8$ and verifying.

Extra material: notes with solved Exercise 9.

164 Linear equations in $\mathbb{Z}_n$, Exercise 10.

Exercise 10: Determine the number of all such elements x from $\mathbb{Z}_{120}$ that $72x \equiv 0 \pmod{120}$.

Extra material: notes with solved Exercise 10.

165 Zero-product property in $\mathbb{Z}_n$

Zero-product property for *real* numbers: If x and y are real numbers such that $xy = 0$ and $x \neq 0$ then $y = 0$.

Show by counterexamples that this property is not satisfied in $\mathbb{Z}_6$, $\mathbb{Z}_8$, and $\mathbb{Z}_{15}$. What about $\mathbb{Z}_5$?

166 Invertible elements in $\mathbb{Z}_n$

Theorem 1: An element $a \in \mathbb{Z}_n$ is *invertible* in $\mathbb{Z}_n$ [i.e., $ab \equiv 1 \pmod{n}$ for some $b \in \mathbb{Z}_n$] iff $\gcd(a, n) = 1$.

Fact: If p is a prime number, then all non-zero $a \in \mathbb{Z}_p$ are *invertible* in $\mathbb{Z}_p$, and their inverses can be computed using the following consequence of FLT: $a^{-1} \equiv a^{p-2} \pmod{p}$.

(Even though the formula exists, it is not too practical to use; a more practical way of finding inverses is by solving appropriate Diophantine equations; For small p this formula works fine, as shown with the example of $p = 5$; for large p it is much harder: for example, 25^{29} is the inverse to 25 in $\mathbb{Z}_{31}$, but it doesn't tell us which number from $\{1, 2, \ldots, 31\}$ it is. [For answer and for a better computation: see Extra problem 4 in V170.])

Theorem 2: If $a \in \mathbb{Z}_n$ is *invertible* in $\mathbb{Z}_n$ then all equations $ax = c$ have exactly one solution in $\mathbb{Z}_n$.

Example: Illustrate the Theorems for $n = 5$ and $n = 6$, using illustrations from V141.

Back to old examples: Solve the equations $3x + 5 = 7$ in $\mathbb{Z}_8$ (V163) and $50x = -1$ in $\mathbb{Z}_{27}$ (V161).

Extra material: notes with solved old examples.

167 Invertible elements in $\mathbb{Z}_n$, Exercise 11.

Exercise 11: Make a list of all the (multiplicatively) invertible elements of $\mathbb{Z}_9$ and in $\mathbb{Z}_{20}$. Explain. Make a multiplication table for $\mathbb{Z}_9$ to confirm your first result.

Extra material: notes with solved Exercise 11.

168 Invertible elements in $\mathbb{Z}_n$, Exercise 12.

Exercise 12: Motivate why 89 is invertible in $\mathbb{Z}_{210}$ and determine its inverse.

Extra material: notes with solved Exercise 12.

169 Invertible elements in $\mathbb{Z}_n$, Exercise 13.

Exercise 13: Solve the equation $10x + 3 = 5$ in $\mathbb{Z}_{22}$. Compare to Example 7 in V126.

170 Reformulating extra problems from V116 and V129.

We look together at the equations from V129 and translate them into our current context.

Extra material: an article with more solved problems on solving equations in $\mathbb{Z}_n$ for various n:

- ⋆ **Extra problem 1**: Solve the equation $72x = 0$ in $\mathbb{Z}_{120}$.
- ⋆ **Extra problem 2**: Solve the equation $8x + 2 = 4$ in $\mathbb{Z}_{18}$.
- ⋆ **Extra problem 3**: Solve the equation $2x + 9 = 4$ in $\mathbb{Z}_{19}$.
- ⋆ **Extra problem 4**: Solve the equation $25x + 17 = 10$ in $\mathbb{Z}_{31}$.
- ⋆ **Extra problem 5**: Solve the equation $15x + 33 = 0$ in $\mathbb{Z}_{36}$.
- ⋆ **Extra problem 6**: Solve the equation $43x + 12 = 53$ in $\mathbb{Z}_{97}$.
- ⋆ **Extra problem 7**: Solve the equation $43x + 37 = 50$ in $\mathbb{Z}_{102}$.

171 Solving systems of linear equations in real numbers.

172 Systems of linear equations in $\mathbb{Z}_n$, Exercise 14.

Exercise 14: Solve the following system of equations in $\mathbb{Z}_7$: $\begin{cases} 2x + 4y = 4 \\ 3x + 5y = 2 \end{cases}$

Extra material: notes with solved Exercise 14.

173 Systems of linear equations in $\mathbb{Z}_n$, Exercise 15.

Exercise 15: Solve the following system of equations in $\mathbb{Z}_{25}$:

$$\begin{cases} x + 4y = 10 \\ 2x + 21y = 5 \end{cases}$$

Extra material: notes with solved Exercise 15.

174 An example of a system of congruences (Chinese Remainder Theorem), Exercise 16.

Exercise 16: Solve the following system of congruences:

$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{6} \\ x \equiv 3 \pmod{7} \end{cases}$$

This example comes back in DM3, in the context of so called *Chinese Remainder Theorem*; then I will motivate that we in this video have solved the same problem as in V168, i.e., we have found the inverse to 89 in $\mathbb{Z}_{210}$.

Extra material: notes with solved Exercise 16.

175 Some really simple quadratic equations.

Examples: Solve the following equations: $x^2 = 2$ (in $\mathbb{Z}_3$), $x^2 = 1$ (in $\mathbb{Z}_3$), $x^2 = 0$ (in $\mathbb{Z}_6$), $x^2 = 0$ (in $\mathbb{Z}_{18}$).

Extra material: notes with solved Examples.

176 A quadratic equation in $\mathbb{Z}_{11}$, Exercise 17.

Exercise 17: Solve the quadratic equation $x^2 + 3x + 4 = 0$ in $\mathbb{Z}_{11}$.

Extra material: notes with solved Exercise 17.

177 Fun divisibility problems, Problem 1.

Problem 1: How many natural numbers less than 10 000 and divisible by 6 can be written with help of digits 0, 1, and 2?

Extra material: notes with solved Problem 1.

178 Fun divisibility problems, Problem 2.

Problem 2: Find all positive natural numbers n for which

$$S_n = 1! + 2! + 3! + \ldots + n!$$

is the square of a natural number. (Hint: Examine last digits of involved numbers.)

Extra material: notes with solved Problem 2.

179 Fun divisibility problems, Problem 3.

Problem 3: Show that no number in the sequence

$$11, \quad 111, \quad 1111, \quad 11111, \ \ldots$$

is the square of a natural number. (Hint: Examine divisibility by 4.)

Extra material: notes with solved Problem 3.

180 Fun divisibility problems, Problem 4.

Problem 4: Show that the number $123^{123} - 57^{57}$ is divisible by 10.

Extra material: notes with solved Problem 4.

181 Fun divisibility problems: Problem 5.

Problem 5: Suppose n is such that the number 2^n has exactly 1000 digits in its decimal representation. Since there are 10 possible digits (0—9), it seems plausible that each digit might appear exactly 100 times. Explain why it is impossible. (Hint: Examine divisibility by 3.)

Extra material: notes with solved Problem 5.

182 Fun divisibility problems, Problem 6.

Problem 6: Find all the triples of consecutive prime numbers p, q, r for which $p^2 + q^2 + r^2$ is a prime number. (Hint: Examine divisibility by 3.)

Extra material: notes with solved Problem 6.

183 Fun divisibility problems: Problem 7.

Problem 7: Determine the remainder of 10^{100} in division by 7.

Extra material: notes with solved Problem 7.

184 Fun divisibility problems, Problem 8.

Problem 8: Solve the following equation in positive natural numbers:

$$837 = 3^k + 3^m + 3^n$$

(Hint: use the ternary number system; see V132.)

Extra material: notes with solved Problem 8.

185 Fun divisibility problems, Problem 9.

Problem 9: Suppose a_n denotes the two-digit number we get from the last two digits of 7^n, i.e., $a_1 = 07$, $a_2 = 49$, and so on. Find the value of

$$\sum_{k=1}^{2026} a_k = a_1 + a_2 + a_3 + \ldots + a_{2026}.$$

(Hint: Try to find a pattern in the sequence (a_n).)

Extra material: notes with solved Problem 9.

186 Fun divisibility problems, Problem 10.

Problem 10: Find all the positive integers n satisfying the following two conditions:

- n is less than or equal to 400,
- n has exactly 9 positive divisors.

(Hint: Use the formula from V27.)

Extra material: notes with solved Problem 10.

187 Fun divisibility problems, Problem 11.

Problem 11: Find the number of positive integers $n < 2026$ such that $25^n + 9^n$ is divisible by 13.

Extra material: notes with solved Problem 11.

188 Fun divisibility problems, Problem 12.

Problem 12: Prove that if n is an integer greater than 1 then $n^{n-1} - 1$ is divisible by $(n-1)^2$. (Hint: Put $m = n - 1$ and apply Binomial Theorem.)

Extra material: notes with solved Problem 12.

189 Fun divisibility problems, Problem 13.

Problem 13: What is the remainder when the following number is divided by 11?

$$\underbrace{999\,999\ldots999^{2024}}_{\text{2025 digits 9 in the base}} - \underbrace{333\,333\ldots333^{2024}}_{\text{2025 digits 3 in the base}}$$

Extra material: notes with solved Problem 13.

S7 An introduction to algebraic structures

You will learn: you will get a glimpse into the wonderful world of Abstract Algebra, the domain of mathematics that studies structures such as groups, rings, fields, vector spaces, etc, their properties and relations between them; basic concepts such like binary operations on sets, their associativity and commutativity, neutral elements and inverse elements with respect to the operations; sets with two operations (rings, fields) and the property that binds these operations (distributivity), additive and multiplicative inverses; the concept of a subgroup; cyclic groups; direct (Cartesian) product of structures; groups of permutations and the geometrical interpretation of some of their subgroups; homomorphisms and isomorphisms between structures; Lagrange's Theorem; various examples and illustrations.

Read along with this section: *Abstract Algebra*, chosen parts (the basics) about groups, rings, fields, etc. Chapter 3: *Groups*, pp.56–106, Chapter 5: *Permutation Groups*, pp.107–127 (pages in the pdf).

190 Abstract Algebra in this course.

191 Our most important models and examples.

192 The definition of a group, order, and subgroup; multiplicative and additive notation.

193 Our first natural examples of groups.

Example 1: Determine whether the following structures are groups:

Ex1.1 $(\mathbb{R}, +, 0)$

Ex1.2 $(\mathbb{R}, \cdot, 1)$

Ex1.3 $(\mathbb{R} \setminus \{0\}, \cdot, 1)$

Ex1.4 $(\mathbb{N}, +, 0)$

Ex1.5 $(\mathbb{N}, \cdot, 1)$

Ex1.6 $(\mathbb{Z}, +, 0)$

Ex1.7 $(\mathbb{Z}, \cdot, 1)$

Ex1.8 $(\mathbb{Z} \setminus \{0\}, \cdot, 1)$

Ex1.9 $(\mathbb{Q}, +, 0)$

Ex1.10 $(\mathbb{Q}, \cdot, 1)$

Ex1.11 $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$

Ex1.12 $(\mathbb{Q}^+, \cdot, 1)$

Ex1.13 $(\mathbb{Q}^- \cup \{1\}, \cdot, 1)$.

Moreover:

- $(\mathbb{Z}, +, 0)$ is a subgroup of $(\mathbb{Q}, +, 0)$; $(\mathbb{Q}, +, 0)$ is a subgroup of $(\mathbb{R}, +, 0)$; $(\mathbb{Z}, +, 0)$ is a subgroup of $(\mathbb{R}, +, 0)$; $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$ and $(\mathbb{Q}^+, \cdot, 1)$ are subgroups of $(\mathbb{R} \setminus \{0\}, \cdot, 1)$; $(\mathbb{Q}^+, \cdot, 1)$ is a subgroup of $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$.
- $(\mathbb{E}, +, 0)$ is a subgroup of $(\mathbb{Z}, +, 0)$ (where $\mathbb{E}$ denotes the set of all *even* integers).

Extra material: notes from the iPad.

194 Our new friends from DM2.

Example 2: Determine whether the following structures are groups:

Ex2.1 $(\mathbb{Z}_n, \oplus, [0]_n)$, for a fixed $n \geqslant 2$. Notation: $(\mathbb{Z}/n\mathbb{Z}, +)$ or $\mathbb{Z}/n\mathbb{Z}$.

Ex2.2 $(\mathbb{Z}_n, \odot, [1]_n)$, for a fixed $n \geqslant 2$, not prime

Ex2.3 $(\mathbb{Z}_n \setminus \{[0]_n\}, \odot, [1]_n)$, for a fixed $n \geqslant 2$, not prime

Ex2.4 $(\mathbb{Z}_p, \odot, [1]_p)$ for a fixed prime number $p \geqslant 2$

Ex2.5 $(\mathbb{Z}_p \setminus \{[0]_p\}, \odot, [1]_p)$ for a fixed prime number $p \geqslant 2$. Notation: $(\mathbb{Z}/p\mathbb{Z})^\times$.

195 Some important properties of groups, illustrated with our earlier examples.

In each group:

- (Uniqueness of the neutral element) the neutral element is unique (proven in V224 of DM1),
- (Uniqueness of the inverse) the inverse to each element is unique (proven in V224 of DM1),
- (Inverse of the inverse) the inverse to the inverse of x is equal to x for each element from the group (compare to V188 of DM1),
- (Inverse of the product) the inverse to a product is equal to the product of the inverses in reverse order (compare to V188 of DM1),
- (Cancellation) each equation $xg_1 = g_2$ (or $g_1y = g_2$), where g_1 and g_2 are some fixed elements from the group, have exactly one solution in the group: $x = g_2g_1^{-1}$ (or $y = g_1^{-1}g_2$); in commutative groups, these equations are equivalent.

196 Operations without nice properties, an exercise.

Exercise: Consider the following operations and prove the statements about them:

1. Given the operation $\diamond : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined as $x \diamond y = \dfrac{x+y}{2}$. Show that this operation is **not** associative. It is obviously commutative (motivate it).
2. Given the operation $\boxplus : \mathbb{N}^+ \times \mathbb{N}^+ \to \mathbb{N}^+$ defined as $m \boxplus n = m^n$. Show that this operation is **neither** associative **nor** commutative, but it has the following interesting property:
$$\forall\, m, n, k \in \mathbb{N}^+ \quad (m \boxplus n) \boxplus k = (m \boxplus k) \boxplus n.$$
3. Given the operation $\circledast : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined as $m \circledast n = m(n-1)$. Show that this operation is **neither** associative **nor** commutative, but it has the following interesting property:
$$\forall\, m, n \in \mathbb{Z} \quad n \circledast m = (m-1) \circledast (n+1).$$

Extra material: notes from the iPad.

197 Alon Amit's wonderful example with a neat trick.

Problem: Prove that the operation (defined for all real x and y such that $x + y \neq 90$)
$$x \circ y = \frac{xy - 2025}{x + y - 90}$$
is commutative and associative.

198 A strange group.

Exercise: We define the following binary operation $\circ$ on $\mathbb{R}$:
$$\circ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \qquad x \circ y = x + y - xy.$$

Show that this operation is associative and commutative. Determine its neutral element and the inverse to each $x \in \mathbb{R}$; you will discover that the latter is not entirely possible. Which numbers do you need to exclude in order to get an abelian group with the operation $\circ$? (Don't forget to analyse the *closedness* of the operation on the restricted set!)

Extra material: notes from the iPad.

199 Klein's four-group, a small but exciting group.

Klein's four-group can be defined in many ways (see V216). For example like this: $(G, \circ, e)$ is an abelian group such that $G = \{e, a, b, ab\}$, and each element is its own inverse. Draw the *Cayley table* for the group.

200 A preparation for The Grand Finale: line symmetries and rotations.

Extra material: notes from the iPad.

201 Groups of permutations: the symmetric groups S_n.

202 Order of an element in a group, cyclic groups and their subgroups.

A geometric example: Given a regular polygon with n vertices (where $n \geqslant 3$ is fixed). The set of n (counterclockwise) rotations of this polygon around its centre, by the angles $\alpha_k = \frac{2k\pi}{n}$ for $k = 1, 2, 3, \ldots, n$ (the last one is the identity transformation, as the rotation by the full/complete angle doesn't change anything) form a group (called C_n) with the composition of isometries as the group operation.

- This group is generated by the rotation by α_1 (generally: by each rotation by α_k such that $\gcd(k, n) = 1$).
- All the subgroups of this group are also cyclic, and their orders are expressed by the divisors of n.

You will learn in any course about complex numbers that such a group can be described as the group of nth roots of 1, with the operation being multiplication of complex numbers.

203 Cyclic groups, more examples.

All groups $(\mathbb{Z}_n, \oplus_n, [0]_n)$ are cyclic; even more: they have the same *construction* as the (*multiplicative*) groups C_n discussed in the previous lecture. (Such pairs of groups, like the additive $\mathbb{Z}_n$ and *multiplicative* C_n, are called *isomorphic*; the concept is discussed in V211.)

Show (using the tables from V160) that the multiplicative groups $\mathbb{Z}_3 \setminus \{0\}$, $\mathbb{Z}_5 \setminus \{0\}$, and $\mathbb{Z}_7 \setminus \{0\}$ are cyclic with generators 2 for the first one, 2 or 3 for the second one, and 3 or 5 for the third one. In V212 you will learn that $(\mathbb{Z}_6, \oplus_6, [0]_6)$ is *isomorphic* to $(\mathbb{Z}_7 \setminus \{0\}, \odot_7, [1]_7)$.

204 The group of units U_n, an example.

We look back at $\mathbb{Z}_9$ with multiplication modulo 9 (which is not a group, we know this from V194). The set S that we determined in V167, together with multiplication modulo 9 forms the group of units U_9 (another common notation: $(\mathbb{Z}/9\mathbb{Z})^\times$). This group has six elements and it is cyclic $U_9 = \langle 2 \rangle$. Another cyclic group, $\langle 4 \rangle$, is a subgroup of $U_9 = \langle 2 \rangle$.

205 The group of units U_n, another example.

We analyse $\mathbb{Z}_{18}$ with multiplication modulo 18 (which is not a group, we know this from V194). We analyse the group of units U_{18} (another common notation: $(\mathbb{Z}/18\mathbb{Z})^\times$) and we discover that $\langle 7 \rangle$ is its subgroup.

Extra material: notes from the iPad.

206 Fields, a definition with some non-surprising examples.

The following structures are examples of rings:

- $(\mathbb{R}, +, \cdot, 0, 1)$ (an **ordered** field, by the order relation $<$),
- $(\mathbb{Q}, +, \cdot, 0, 1)$ (an **ordered** field, by the order relation $<$),
- $(\mathbb{Z}_p, \oplus, \odot, [0]_p, [1]_p)$, where p is prime. (These fields are **not** ordered.)

207 Plenty of number fields containing $\mathbb{Q}$ and contained in $\mathbb{R}$.

Example: Choose a positive natural number d which is **not** the square of a natural number (like for example: 2, 3, 5, 6, 7, 8, 10,11,12,13,14,15,17,...). The following set

$$\{\alpha + \beta\sqrt{d};\ \alpha, \beta \in \mathbb{Q}\}$$

with addition and multiplication as in $\mathbb{R}$ is an ordered number field $\mathbb{F}_d$ such that $\mathbb{Q} \subset \mathbb{F}_d \subset \mathbb{R}$. I prove this for $d = 2$, because we know (DM1, V221) that $\sqrt{2}$ is an irrational number. Later I also prove that each $\sqrt{d}$ (for $d \in \mathbb{N}^+$ as described above) is irrational. This (together with the fact that we get different fields for different choices of d) will show that we have plenty of number fields strictly between $\mathbb{Q}$ and $\mathbb{R}$.

Extra material: notes with solved Example.

208 A mysterious and complex field.

Consider $\mathbb{R} \times \mathbb{R}$ with the following two operations defined on pairs of pairs of real numbers:

$$\oplus, \odot :\ (\mathbb{R} \times \mathbb{R}) \times (\mathbb{R} \times \mathbb{R}) \to (\mathbb{R} \times \mathbb{R})$$

defined as:

$$(a, b) \oplus (c, d) = (a + c, b + d), \qquad (a, b) \odot (c, d) = (ac - bd, ad + bc).$$

Show that $(\mathbb{R} \times \mathbb{R}, \oplus, \odot, (0, 0), (1, 0))$ is a field (**unordered**). If we define $i = (0, 1)$, then $i^2 =$?

209 Rings, a definition with some non-surprising examples.

The following structures are examples of number fields:

- $(\mathbb{R}, +, \cdot, 0, 1)$ (each field is a ring),
- $(\mathbb{Q}, +, \cdot, 0, 1)$ (each field is a ring),
- $(\mathbb{Z}_p, \oplus, \odot, [0]_p, [1]_p)$, where p is prime (each field is a ring),
- $(\mathbb{Z}, +, \cdot, 0, 1)$,
- $(\mathbb{Z}_n, \oplus, \odot, [0]_n, [1]_n)$, where $n \geqslant 2$ is any fixed positive composite integer.

You will also see an example of a **non-commutative** ring $\mathcal{M}_{n\times n}$ of $n \times n$ matrices with addition and multiplication of matrices (with references to Linear Algebra and Geometry).

210 Creating new structures from old structures: direct product of groups.

We look together at two examples:

E1 Given two groups: $(G, \circ, e)$ and $(H, \diamond, e')$, we define the *direct product* $(G \times H, \times, (e, e'))$, which is also a group (with coordinate-wise operations and neutral elements).

E2 Direct product of the ring of real numbers by itself is a ring, but not a field, even though $\mathbb{R}$ is a field.

The second example shows why it was necessary to come up with another definition of multiplication of pairs of real numbers in order to get the field of complex numbers (like in V208).

Extra material: notes from the iPad.

211 Homomorphisms and isomorphisms of structures.

Some important facts about homomorphisms. If $f : (G, \circ) \to (H, \diamond)$ is a homomorphism, then

- $f(e) = e'$, where e and e' are neutral elements in G and H respectively.
- The definition of homomorphism can be expanded (by induction) to any number $(n \geqslant 3)$ of factors/terms:

$$f(x_1 \circ x_2 \circ \ldots \circ x_n) = f(x_1) \diamond f(x_2) \diamond \ldots \diamond f(x_n).$$

- In particular, for all $n \in \mathbb{N}^+$ and for all $x \in G$ we have $f(x^n) = (f(x))^n$, where the power at the LHS denotes repeated operation $\circ$ in G, while the power at the RHS denotes repeated operation $\diamond$ in H.

212 Two isomorphic groups of order 6.

The groups $(\mathbb{Z}_6, \oplus_6, [0]_6)$ and $(\mathbb{Z}_7 \setminus \{[0]_7\}, \odot_7, [1]_7)$ are both cyclic. Determine an isomorphism between them.

213 Some preparations for the Chinese Remainder Theorem (see V174).

Let $n_1, n_2, \ldots, n_k$ be natural numbers greater than 1, pairwise co-prime, and $N = n_1 \cdot n_2 \cdot \ldots \cdot n_k$. We have the following isomorphic pair of rings (that we will use in DM3 to discuss the Chinese Remainder Theorem and *quick arithmetic*):

$$(\mathbb{Z}_N, +, \cdot) \cong (\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}, \oplus, \odot).$$

The structure at the RHS is the direct product of rings $\mathbb{Z}_{n_i}$ (for $i = 1, 2, \ldots, k$) as discussed in V210.

214 Vector spaces and linear transformations.

The most important examples of vector spaces:

Ex0 **our prototype**: geometric vectors in the plane $\mathbb{R}^2$ or in the 3-space $\mathbb{R}^3$,

Ex1 a generalisation to $\mathbb{R}^n$ for any number $n \in \mathbb{N}^+$, with coordinate-wise addition and scaling,

- some examples of linear transformations from $\mathbb{R}^2$ to $\mathbb{R}^2$ (just some animations with MANIM).

215 Some more unusual examples of vector spaces.

After Example 1 from the previous lecture, we look at three more examples:

Ex2 the set $\mathcal{M}_{m\times n}(\mathbb{R})$ of $m \times n$ matrices with real entries, with matrix addition and scaling,

Ex3 the set $F[a, b]$ of all functions $f : [a, b] \to \mathbb{R}$, with function addition and scaling (both argument-wise),

Ex4 the set of all complex numbers, with the addition as defined in V208, and with scaling by real numbers.

216 A fun problem about isomorphic groups.

The following three groups are isomorphic:

- Klein's four-group (see V199),
- $\mathbb{Z}_2 \times \mathbb{Z}_2$ with coordinate-wise addition modulo 2 (like in V210),
- the group of own isometries of a non-square rectangle.

217 **Optional, difficult**: A really tricky problem about isomorphic groups.

A difficult (optional) problem about groups. We define the following binary operation $*$ on $\mathbb{R}$:

$$*: \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \qquad x * y = x\sqrt{y^2+1} + y\sqrt{x^2+1}.$$

Show that this operation is commutative. Proving **associativity** of the operation is very hard without a special trick that at the same time shows that the group $(\mathbb{R}, *, 0)$ is isomorphic to $(\mathbb{R}, +, 0)$:

- We use the following *hyperbolic* functions (defined with help of Euler's number $e \approx 2.718$):

$$\sinh(t) = \frac{e^t - e^{-t}}{2} \quad \text{and} \quad \cosh(t) = \frac{e^t + e^{-t}}{2}.$$

- Both hyperbolic sine and hyperbolic cosine are defined for all $t \in \mathbb{R}$; moreover, hyperbolic sine attains all the real values (less obvious, but you will get some references), so we can substitute $x = \sinh(a)$ and $y = \sinh(b)$ (and this is the trick I meant!); the hyperbolic sine is strictly increasing on the entire $\mathbb{R}$, and thus invertible; its inverse is called arsinh and is a 1-to-1 function $f : \mathbb{R} \to \mathbb{R}$. This is the key to our method.
- We show the identity that resembles Pythagorean identity: $\cosh^2(t) - \sinh^2(t) = 1$ for all $t \in \mathbb{R}$.
- We show the identity that resembles the sine-of-the-sum identity: $\sinh(a+b) = \sinh(a)\cosh(b) + \sinh(b)\cosh(a)$ for all $a, b \in \mathbb{R}$.
- Function $\operatorname{arsinh} : \mathbb{R} \to \mathbb{R}$ is an isomorphism from $(\mathbb{R}, *)$ to $(\mathbb{R}, +)$, which helps us prove associativity of $*$, determine its neutral element and the inverse to each $x \in \mathbb{R}$.

Extra material: notes from the iPad.

218 Group or no group? An exercise.

Exercise: Which of the following binary-operation tables on the set $G = \{a, b, c, d\}$ define a group? Motivate your answers.

$\circ$	a	b	c	d
a	a	c	d	a
b	b	b	c	d
c	c	d	a	b
d	d	a	b	c

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	b	a	d
d	d	d	b	c

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

We get two groups and two structures that are **not** groups. The two groups have the same order, but they are not isomorphic. Explain why.

219 Dihedral group D_3: the isometries of an equilateral triangle (cont. from V138 in DM1).

We analyse the *dihedral group* D_3 (group of the isometries of an equilateral triangle)

$$D_3 = \{I, S_1, S_2, S_3, R_1, R_2\}.$$

- The group consists of the identity transformation, three line symmetries (reflections), and two rotations, with the operation being the composition of isometries (or, equivalently, multiplication of permutations).
- It is (isomorphic to) the *symmetric group* $S_{[3]}$ of all 6 permutations of a set with three elements. (The symbol denoting this group is actually S_3, but I used this symbol for one of the symmetries...)

- The identity is the **neutral** element in the group.
- Each element has exactly one **inverse** element in the group.
- The group is **non-abelian** (for example: $S_1 \circ S_2 \neq S_2 \circ S_1$).
- **Associativity** was proven (generally, for functions) in V137 of DM1.
- All the equations $g_1 \circ x = g_2$ have **exactly one solution** for each g_1, g_2 from D_3.
- The set of all the rotations $R = \{I, R_1, R_2\} = \{I, R_1, R_1^2\}$ forms a **cyclic subgroup** of D_3.
- The set D_3 is **closed** for the operation of composition, as shown in the table. We confirm with computations the values of chosen compositions: $R_1 \circ R_2,\ S_2 \circ S_1,\ S_3 \circ R_2,\ R_1 \circ R_1$.

Extra material: notes from the iPad.

220 Dihedral group D_4: the isometries of a square.

We analyse the *dihedral group* D_4 (group of the isometries of a square)

$$D_4 = \{I, S_1, S_2, S_3, S_4, R_1, R_2, R_3\}.$$

- The group consists of the identity transformation, four line symmetries (reflections), and three rotations, with the operation being the composition of isometries (or, equivalently, multiplication of permutations).
- It is (isomorphic to) a subgroup of the *symmetric group* $S_{[4]}$ of all 24 permutations of a set with four elements. (The symbol denoting this group is actually S_4, but I used this symbol for one of the symmetries...)
- The identity is the **neutral** element in the group.
- Each element has exactly one **inverse** element in the group.
- The group is **non-abelian** (for example: $S_1 \circ S_3 \neq S_3 \circ S_1$).
- **Associativity** was proven (generally, for functions) in V137 of DM1.
- All the equations $g_1 \circ x = g_2$ have **exactly one solution** for each g_1, g_2 from D_4.
- The set of all the rotations $R = \{I, R_1, R_2, R_3\} = \{I, R_1, R_1^2, R_1^3\}$ forms a **cyclic subgroup** of D_4.
- The set D_4 is **closed** for the operation of composition, as shown in the table. We confirm with computations the values of chosen compositions: $S_3 \circ S_4,\ S_4 \circ S_3,\ S_1 \circ S_3,\ S_3 \circ S_1,\ R_1 \circ R_3,\ S_3 \circ S_3,\ R_3 \circ R_3$.

Extra material: notes from the iPad.

221 Subgroups, cosets, and Lagrange's Theorem.

- Left and right *cosets* (gH and Hg) of a subgroup H with respect to an element g in a group G.
- **Theorem**: Let H be a subgroup of a group G. If g_1 and g_2 are any elements of G, the left cosets g_1H and g_2H are either identical or they have no elements in common.
- We look at this theorem from the perspective of equivalence relations and partitions by equivalence classes.
- **Theorem (Lagrange)**: If G is a finite group of order n and H is a subgroup of order m, then $m|n$.
- One more proof (proof 4) of Fermat's Little Theorem (Videos 156–160).
- Some examples: earlier in the course and in the next lecture.

222 The last one: something for the soul.

We revisit the topic of V219 and V220 and we look together at a beautiful picture from Wikipedia created by Tilman Piesk (*Watchduck*): the dihedral group D_4 as a subgroup of the symmetric group $S_{[4]}$, even and odd permutations, and 4-cycles; a similar picture for the dihedral group D_3 (by the same creator).
We also look at the subgroups of D_3 in the light of Lagrange's Theorem; we determine left and right cosets for the subgroup $G = \{I, S_1\}$.

S8 Extras

You will learn: about all the courses we offer, and where to find discount coupons. You will also get a glimpse into our plans for future courses, with approximate (very hypothetical!) release dates.

B Bonus lecture.

Extra material 1: a pdf with all the links to our courses, and coupon codes.

Extra material 2: a pdf with an advice about optimal order of studying our courses.

Extra material 3: a pdf with information about course books, and how to get more practice.