MathOlymp.com

Resources for mathematically gifted students

Tutorials in Algebra, Number Theory, Combinatorics and Geometry

The aim of this section is, in the series of tutorials, to cover the material of the unwritten syllabus of the IMO, more precisely that part of it which is not in the school curriculum of most participating countries.

Algebra

- Rearrangement Inequality This article by K. Wu, Andy Liu was first published in "Mathematics Competitions" Vol. 8, No.1 (1995), pp. 53--60. This journal is published by Australian Mathematics Trust. The article is reproduced here thanks to the kind permission of the authors and the Editor of "Mathematics Competitions" Warren Atkins.

Combinatorics

- Interactive Graph Theory Tutorials By Chris K. Caldwell from the University of Tenessee at Martin.
- Permutations.
- Friendship Theorem.

Numbers

- Divisibility and primes
- Euclidean algorithm
- Euler's theorem
- Representation of numbers
- Bertrand's postulate.

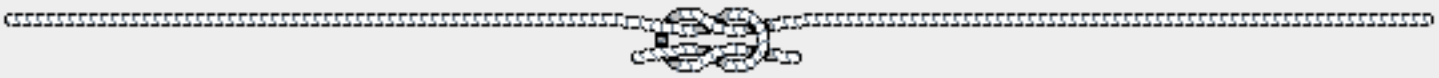
Geometry

- Ptolemy's inequality
- Euler's theorem

Click to go back

MathOlymp.com

Resources for mathematically gifted students



Unwritten Syllabus of the IMO

These thoughts were written in 1997, when I was working on the Problem Selection Committee of the 38th IMO in Argentina and when my impressions about the problems, which were submitted, and the attitude of our Committee to these problems were still fresh. I edited them very little since.

The syllabus of IMO is, of course, unwritten but there are several tendencies which can be clearly observed. It is all ruled by tradition, there is no logic in all this whatsoever. Some topics are included, alhtough they are not in the school curricula for most countries, on the grounds that they are traditional and feature in the training programmes of most countries.

What is not Included

- Any questions where knowledge of Calculus may be an advantage, e.g. most of the inequalities;
- Complex numbers (although they were in the past, when less countries participated);
- Inversion in geometry (the Jury just sick and tired of it for some reason);
- Solid geometry was also present in the past. There are coordinated attempts to return it into the IMO but the resistance is strong;
- After being a darling of the Jury for some time, Pell's equation seems to be strongly out of favour.

What is included

- Fundamental Theorems on Arithmetic and Algebra, factorization of a polynomial into a product of irreducible polynomials;
- Symmetric polynomials of several variables, Vieta's theorem;
- Linear and quadratic Diophantine equations, including the Pell's equation (although see the comment above);
- Arithmetic of residues modulo n, Fermat's and Euler's theorems;
- Properties of the orthocentre, Euler's line, nine-point-circle, Simson line, Ptolemy's inequality, Ceva and Menelaus etc.;
- Interesting situation is with the graph theory. It is sort of considered to be all known and virtually disappeared from submissions to IMO. But watch this space!.

Click to go back

THE REARRANGEMENT INEQUALITY

K. Wu

South China Normal University, China

Andy Liu

University of Alberta, Canada

We will introduce our subject via an example, taken from a Chinese competition in 1978.

"Ten people queue up before a tap to fill their buckets. Each bucket requires a different time to fill. In what order should the people queue up so as to minimize their combined waiting time?"

Common sense suggests that they queue up in ascending order of "bucket-filling time". Let us see if our intuition leads us astray. We will denote by $T_1 < T_2 < \cdots < T_{10}$ the times required to fill the respective buckets.

If the people queue up in the order suggested, their combined waiting time will be given by $T = 10T_1 + 9T_2 + \cdots + T_{10}$. For a different queueing order, the combined waiting time will be $S = 10S_1 + 9S_2 + \cdots + S_{10}$, where $(S_1, S_2, \ldots, S_{10})$ is a permutation of $(T_1, T_2, \ldots, T_{10})$.

The two 10-tuples being different, there is a smallest index i for which $S_i \neq T_i$. Then $S_j = T_i < S_i$ for some $j > i$. Define $S'_i = S_j, S'_j = S_i$ and $S'_k = S_k$ for $k \neq i, j$. Let $S' = 10S'_1 + 9S'_2 + \cdots + S'_{10}$. Then

$$S - S' = (11 - i)(S_i - S'_i) + (11 - j)(S_j - S'_j) = (S_i - S_j)(j - i) > 0.$$

Hence the switching results in a lower combined waiting time.

If $(S'_1, S'_2, \ldots, S'_{10}) \neq (T_1, T_2, \ldots, T_{10})$, this switching process can be repeated again. We will reach $(T_1, T_2, \ldots, T_{10})$ in at most 9 steps. Since the combined waiting time is reduced in each step, T is indeed the minimum combined waiting time.

We can generalize this example to the following result.

The Rearrangement Inequality.
Let $a_1 \leq a_2 \leq \cdots \leq a_n$ and $b_1 \leq b_2 \leq \cdots \leq b_n$ be real numbers. For any permutation $(a'_1, a'_2, \ldots, a'_n)$ of $(a_1, a_2, \ldots, a_n)$, we have

$$\begin{aligned} a_1b_1 + a_2b_2 + \cdots + a_nb_n &\geq a'_1b_1 + a'_2b_2 + \cdots + a'_nb_n \\ &\geq a_nb_1 + a_{n-1}b_2 + \cdots + a_1b_n, \end{aligned}$$

with equality if and only if $(a'_1, a'_2, \ldots, a'_n)$ is equal to $(a_1, a_2, \ldots, a_n)$ or $(a_n, a_{n-1}, \ldots, a_1)$ respectively.

This can be proved by the switching process used in the introductory example. See for instance [1] or [2], which contain more general results. Note that unlike many inequalities, we do not require the numbers involved to be positive.

Corollary 1.
Let $a_1, a_2, \ldots, a_n$ be real numbers and $(a'_1, a'_2, \ldots, a'_n)$ be a permutation of $(a_1, a_2, \ldots, a_n)$. Then

$$a_1^2 + a_2^2 + \cdots + a_n^2 \geq a_1a'_1 + a_2a'_2 + \cdots + a_na'_n.$$

Corollary 2.
Let $a_1, a_2, \ldots, a_n$ be positive numbers and $(a_1', a_2', \ldots, a_n')$ be a permutation of $(a_1, a_2, \ldots, a_n)$. Then

$$\frac{a_1'}{a_1} + \frac{a_2'}{a_2} + \cdots + \frac{a_n'}{a_n} \geq n.$$

A 1935 Kürschák problem in Hungary asked for the proof of Corollary 2, and a 1940 Moscow Olympiad problem asked for the proof of the special case $(a_1', a_2', \ldots, a_n') = (a_2, a_3, \ldots, a_n, a_1)$.

We now illustrate the power of the Rearrangement Inequality by giving simple solutions to a number of competition problems.

Example 1. (International Mathematical Olympiad, 1975)
Let $x_1 \leq x_2 \leq \cdots \leq x_n$ and $y_1 \leq y_2 \leq \cdots \leq y_n$ be real numbers. Let $(z_1, z_2, \cdots, z_n)$ be a permutation of $(y_1, y_2, \ldots, y_n)$. Prove that

$$(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2 \leq (x_1 - z_1)^2 + (x_2 - z_2)^2 + \cdots + (x_n - z_n)^2.$$

Solution:
Note that we have $y_1^2 + y_2^2 + \cdots + y_n^2 = z_1^2 + z_2^2 + \cdots + z_n^2$. After expansion and simplification, the desired inequality is equivalent to

$$x_1y_1 + x_2y_2 + \cdots + x_ny_n \geq x_1z_1 + x_2z_2 + \cdots + x_nz_n,$$

which follows from the Rearrangement Inequality.

Example 2. (International Mathematical Olympiad, 1978)
Let $a_1, a_2, \ldots, a_n$ be distinct positive integers. Prove that

$$\frac{a_1}{1^2} + \frac{a_2}{2^2} + \cdots + \frac{a_n}{n^2} \geq \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}.$$

Solution:
Let $(a_1', a_2', \ldots, a_n')$ be the permutation of $(a_1, a_2, \ldots, a_n)$ such that $a_1' \leq a_2' \leq \cdots \leq a_n'$. Then $a_i' \geq i$ for $1 \leq i \leq n$. By the Rearrangement Inequality,

$$\begin{aligned} \frac{a_1}{1^2} + \frac{a_2}{2^2} + \cdots + \frac{a_n}{n^2} &\geq \frac{a_1'}{1^2} + \frac{a_2'}{2^2} + \cdots + \frac{a_n'}{n^2} \\ &\geq \frac{1}{1^2} + \frac{2}{2^2} + \cdots + \frac{n}{n^2} \\ &\geq \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}. \end{aligned}$$

Example 3. (International Mathematical Olympiad, 1964)
Let a, b and c be the sides of a triangle. Prove that

$$a^2(b + c - a) + b^2(c + a - b) + c^2(a + b - c) \leq 3abc.$$

Solution:
We may assume that $a \geq b \geq c$. We first prove that $c(a+b-c) \geq b(c+a-b) \geq a(b+c-a)$. Note that $c(a+b-c) - b(c+a-b) = (b-c)(b+c-a) \geq 0$. The second inequality can be proved in the same manner. By the Rearrangement Inequality, we have

$$a^2(b+c-a) + b^2(c+a-b) + c^2(a+b-c) \leq ba(b+c-a) + cb(c+a-b) + ac(a+b-c),$$

$$a^2(b+c-a) + b^2(c+a-b) + c^2(a+b-c) \leq ca(b+c-a) + ab(c+a-b) + bc(a+b-c).$$

Adding these two inequalities, the right side simplifies to $6abc$. The desired inequality now follows.

Example 4. (International Mathematical Olympiad, 1983)
Let a, b and c be the sides of a triangle. Prove that $a^2b(a-b) + b^2c(b-c) + c^2a(c-a) \geq 0$.

Solution:
We may assume that $a \geq b, c$. If $a \geq b \geq c$, we have $a(b+c-a) \leq b(c+a-b) \leq c(a+b-c)$ as in Example 3. By the Rearrangement Inequality,

$$\begin{aligned} & \frac{1}{c}a(b+c-a) + \frac{1}{a}b(c+a-b) + \frac{1}{b}c(a+b-c) \\ \leq\ & \frac{1}{a}a(b+c-a) + \frac{1}{b}b(c+a-b) + \frac{1}{c}c(a+b-c) \\ =\ & a+b+c. \end{aligned}$$

This simplifies to $\frac{1}{c}a(b-a) + \frac{1}{a}b(c-b) + \frac{1}{b}c(a-c) \leq 0$, which is equivalent to the desired inequality. If $a \geq c \geq b$, then $a(b+c-a) \leq c(a+b-c) \leq b(c+a-b)$. All we have to do is interchange the second and the third terms of the displayed lines above.

Simple as it sounds, the Rearrangement Inequality is a result of fundamental importance. We shall derive from it many familiar and useful inequalities.

Example 5. The Arithmetic Mean Geometric Mean Inequality.
Let $x_1, x_2, \ldots, x_n$ be positive numbers. Then

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 x_2 \cdots x_n},$$

with equality if and only if $x_1 = x_2 = \cdots = x_n$.

Proof:
Let $G = \sqrt[n]{x_1 x_2 \cdots x_n}$, $a_1 = \dfrac{x_1}{G}, a_2 = \dfrac{x_1 x_2}{G^2}, \ldots, a_n = \dfrac{x_1 x_2 \cdots x_n}{G^n} = 1$. By Corollary 2,

$$n \leq \frac{a_1}{a_n} + \frac{a_2}{a_1} + \cdots + \frac{a_n}{a_{n-1}} = \frac{x_1}{G} + \frac{x_2}{G} + \cdots + \frac{x_n}{G},$$

which is equivalent to $\dfrac{x_1 + x_2 + \cdots + x_n}{n} \geq G$. Equality holds if and only if $a_1 = a_2 = \cdots = a_n$, or $x_1 = x_2 = \cdots = x_n$.

Example 6. The Geometric mean Harmonic Mean Inequality.
Let $x_1, x_2, \ldots, x_n$ be positive numbers. Then

$$\sqrt[n]{x_1 x_2 \cdots x_n} \geq \frac{n}{\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n}},$$

with equality if and only if $x_1 = x_2 = \cdots = x_n$.

Proof:
Let $G, a_1, a_2, \ldots, a_n$ be as in Example 5. By Corollary 2,

$$n \leq \frac{a_1}{a_2} + \frac{a_2}{a_3} + \cdots + \frac{a_n}{a_1} = \frac{G}{x_1} + \frac{G}{x_2} + \cdots + \frac{G}{x_n},$$

which is equivalent to

$$G \geq \frac{n}{\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n}}.$$

Equality holds if and only if $x_1 = x_2 = \cdots = x_n$.

Example 7. The Root Mean Square Arithmetic Mean Inequality.
Let $x_1, x_2, \ldots, x_n$ be real numbers. Then

$$\sqrt{\frac{x_1^2 + x_2^2 + \cdots + x_n^2}{n}} \geq \frac{x_1 + x_2 + \cdots + x_n}{n},$$

with equality if and only if $x_1 = x_2 = \cdots = x_n$.

Proof:
By Corollary 1, we have

$$\begin{aligned} x_1^2 + x_2^2 + \cdots + x_n^2 &\geq x_1x_2 + x_2x_3 + \cdots + x_nx_1, \\ x_1^2 + x_2^2 + \cdots + x_n^2 &\geq x_1x_3 + x_2x_4 + \cdots + x_nx_2, \\ \cdots &\geq \cdots \\ x_1^2 + x_2^2 + \cdots + x_n^2 &\geq x_1x_n + x_2x_1 + \cdots + x_nx_{n-1}. \end{aligned}$$

Adding these and $x_1^2 + x_2^2 + \cdots + x_n^2 = x_1^2 + x_2^2 + \cdots + x_n^2$, we have

$$n(x_1^2 + x_2^2 + \cdots + x_n^2) \geq (x_1 + x_2 + \cdots + x_n^2)^2,$$

which is equivalent to the desired result. Equality holds if and only if $x_1 = x_2 = \cdots = x_n$.

Example 8. Cauchy's Inequality.
Let $a_1, a_2, \ldots a_n, b_1, b_2, \ldots, b_n$ be real numbers. Then

$$(a_1b_1 + a_2b_2 + \cdots + a_nb_n)^2 \leq (a_1^2 + a_2^2 + \cdots + a_n^2)(b_1^2 + b_2^2 + \cdots + b_n^2),$$

with equality if and only if for some constant $k, a_i = kb_i$ for $1 \leq i \leq n$ or $b_i = ka_i$ for $1 \leq i \leq n$.

Proof:
If $a_1 = a_2 = \cdots = a_n = 0$ or $b_1 = b_2 = \cdots = b_n = 0$, the result is trivial. Otherwise, define $S = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}$ and $T = \sqrt{b_1^2 + b_2^2 + \cdots + b_n^2}$. Since both are non-zero, we may let $x_i = \frac{a_i}{S}$ and $x_{n+i} = \frac{b_i}{T}$ for $1 \leq i \leq n$. By Corollary 1,

$$\begin{aligned} 2 &= \frac{a_1^2 + a_2^2 + \cdots + a_n^2}{S^2} + \frac{b_1^2 + b_2^2 + \cdots + b_n^2}{T^2} \\ &= x_1^2 + x_2^2 + \cdots + x_{2n}^2 \\ &\geq x_1x_{n+1} + x_2x_{n+2} + \cdots + x_nx_{2n} + x_{n+1}x_1 + x_{n+2}x_2 + \cdots + x_{2n}x_n \\ &= \frac{2(a_1b_1 + a_2b_2 + \cdots + a_nb_n)}{ST}, \end{aligned}$$

which is equivalent to the desired result. Equality holds if and only if $x_i = x_{n+i}$ for $1 \leq i \leq n$, or $a_iT = b_iS$ for $1 \leq i \leq n$.

We shall conclude this paper with two more examples whose solutions are left as exercises.

Example 9. (Chinese competition, 1984) Prove that

$$\frac{x_1^2}{x_2} + \frac{x_2^2}{x_3} + \cdots + \frac{x_n^2}{x_1} \geq x_1 + x_2 + \cdots + x_n$$

for all positive numbers $x_1, x_2, \ldots, x_n$.

Example 10. (Moscow Olympiad, 1963) Prove that

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geq \frac{3}{2}$$

for all positive numbers a, b and c.

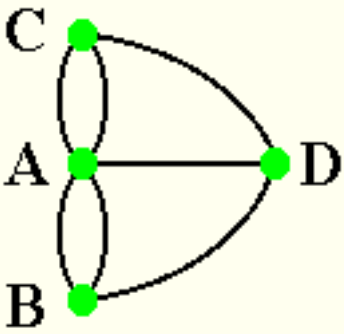
References:

1. G. Hardy, J. Littlewood and G. Polya, "Inequalities", Cambridge University Press, Cambridge, paperback edition, (1988) 260-299.

2. K. Wu, The Rearrangement Inequality, Chapter 8 in "Lecture Notes in Mathematics Competitions and Enrichment for High Schools" (in Chinese), ed. K. Wu et al., (1989) 8:1-8:25.

AUSTRALIAN MATHEMATICS TRUST

What's New . Events . Information for Parents . AMT Publishing . People
Activity . Links . Email Us . About the Trust . Privacy Policy



Graph Theory Tutorials

Chris K. Caldwell

This is the home page for a series of short interactive tutorials introducing the basic concepts of graph theory. There is not a great deal of theory here, we will just teach you enough to wet your appetite for more!

Most of the pages of this tutorial require that you pass a quiz before continuing to the next page. So the system can keep track of your progress you will need to register for *each* of these courses by pressing the [REGISTER] button on the bottom of the first page of *each* tutorial. (You can use the same username and password for each tutorial, but you will need to register separately for each course.)

Introduction to Graph Theory (6 pages)

Starting with three motivating problems, this tutorial introduces the definition of graph along with the related terms: vertex (or node), edge (or arc), loop, degree, adjacent, path, circuit, planar, connected and component. [*Suggested prerequisites: none*]

Euler Circuits and Paths

Beginning with the Königsberg bridge problem we introduce the Euler paths. After presenting Euler's theorem on when such paths and circuits exist, we then apply them to related problems including pencil drawing and road inspection. [*Suggested prerequisites: Introduction to Graph Theory*]

Coloring Problems (6 pages)

How many colors does it take to color a map so that no two countries that share a common border have the same color? This question can be changed to "how many colors does it take to color a planar graph?" In this tutorial we explain how to change the map to a graph and then how to answer the question for a graph. [*Suggested prerequisites: Introduction to Graph Theory*]

Adjacency Matrices (Not yet available.)

How do we represent a graph on a computer? The most common solution to this question, adjacency matrices, is presented along with several algorithms to find a shortest path... [*Suggested prerequisites: Introduction to Graph Theory*]

Related Resources for these Tutorials:

- Glossary of Graph Theory Terms
- Partially Annotated Bibliography

Similar Systems

- Online Exercises

Other Graph Theory Resources on the Internet:

- Graph drawing
- J. Graph Algorithms & Applications
- David Eppstein's graph theory publications
- J. Spinrad research and problems on graph classes

Chris Caldwell *caldwell@utm.edu*

Combinatorics. Tutorial 1: Permutations

As of late, permutations find their way into math olympiads more and more often. The latest example is the Balkan Mathematics Olympiad 2001 where the following problem was suggested.

> A cube of dimensions $3\times3\times3$ is divided into 27 unit cells, each of dimensions $1\times1\times1$. One of the cells is empty, and all others are filled with unit cubes which are, at random, labelled 1,2,...,26. A legal move consists of a move of any of the unit cubes to its neighbouring empty cell. Does there exist a finite sequence of legal moves after which the unit cubes labelled k and $27-k$ exchange their positions for all $k=1,2,...,13$? (Two cells are said to be neighbours if they share a common face.)

This tutorial was written in responce to this event.

1 Definitions and Notation

We assume here that the reader is familiar with the concept of composition of functions f and g, which is denoted here as $f\circ g$. It is a well-known fact that if $f\colon A\to B$ is a function which is both one-to-one and onto then f is *invertible*, i.e. there exists a function $g\colon B\to A$ such that $g\circ f=\mathrm{id}_A$ and $f\circ g=\mathrm{id}_B$, where id_A and id_B are the identity mappings of A and B, respectively. Note that we assume that in the composition $f\circ g$ the function g acts first and f acts second: e.g., $(f\circ g)(b)=f(g(b))$. There are, however, many good books using the alternative convention, so it is always necessary to check whether a particular author uses one or the other convention.

In what follows we will be concerned with invertible functions from a finite set to itself. For convenience, we assume that the elements of the set are the numbers $1,2,\ldots,n$ (the elements of any finite set can be labelled with the first few integers, so this does not restrict generality).

Definition 1. Let n be a positive integer. A *permutation of degree n* is a function $f\colon\{1,2,\ldots,n\}\to\{1,2,\ldots,n\}$ which is one-to-one and onto.

Since a function is specified if we indicate what the image of each element is, we can specify a permutation π by listing each element together with its image as follows:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots\cdots & n-1 & n \\ \pi(1) & \pi(2) & \pi(3) & \cdots\cdots & \pi(n-1) & \pi(n) \end{pmatrix}.$$

For example $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 3 & 1 & 7 & 6 & 4 \end{pmatrix}$ is the permutation of degree 7 which maps 1 to 2, 2 to 5, 3 to 3, 4 to 1, 5 to 7, 6 to 6, and 7 to 4. It is clear that in the second row of such an array all the numbers of the top row must appear exactly once, i.e. the second row is just a rearrangement of the top row.

It is also clear that there are exactly $n!$ permutations of degree n (if you want to fill the bottom row of such an array, there are n ways to fill the first position, $n-1$ ways to fill the second position (since we must not repeat the first entry), etc., leading to a total of $n(n-1)\cdot\ldots\cdot 2\cdot 1 = n!$ different possibilities).

2 Calculations with Permutations

The composition of two permutations of degree n is again a permutation of degree n (exercise: prove that if $f\colon A \to A$ and $g\colon A \to A$ are one-to-one then $f \circ g$ is one-to-one; prove that if $f\colon A \to A$ and $g\colon A \to A$ are onto then $f \circ g$ is onto).

First of all we practice the use of our symbolism for the calculation of the composition of two permutations. This is best done with a few examples. In the sequel, we omit the symbol for function composition ($\circ$), and speak of the *product $\pi\sigma$ of two permutations π and σ*, meaning the composition $\pi \circ \sigma$.

Example 1. Let

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 1 & 3 & 8 & 5 & 7 & 2 \end{pmatrix}, \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 5 & 6 & 1 & 8 & 3 & 7 \end{pmatrix}.$$

Then

$$\pi\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 1 & 3 & 8 & 5 & 7 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 5 & 6 & 1 & 8 & 3 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 3 & 8 & 5 & 4 & 2 & 1 & 7 \end{pmatrix},$$

$$\sigma\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 5 & 6 & 1 & 8 & 3 & 7 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 1 & 3 & 8 & 5 & 7 & 2 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 8 & 2 & 5 & 7 & 1 & 3 & 4 \end{pmatrix}.$$

Explanation: the calculation of $\pi\sigma$ requires us to find

- the image of 1 when we apply *first* σ, *then* π, ($1 \overset{\sigma}{\mapsto} 2 \overset{\pi}{\mapsto} 6$, so write the 6 under the 1),
- the image of 2 when we apply *first* σ, *then* π, ($2 \overset{\sigma}{\mapsto} 4 \overset{\pi}{\mapsto} 3$, so write the 3 under the 2),
- etc.

The calculation of $\sigma\pi$ requires us to find

- the image of 1 when we apply *first* π, *then* σ, ($1 \overset{\pi}{\mapsto} 4 \overset{\sigma}{\mapsto} 6$, so write the 6 under the 1)
- the image of 1 when we apply *first* π, *then* σ, ($2 \overset{\pi}{\to} 6 \overset{\sigma}{\to} 8$, so write the 8 under the 2)
- etc.

⋮ All this is easily done at a glance and can be written down immediately; BUT be careful to start with the right hand factor again!

Important note 1: the example shows clearly that $\pi\sigma \neq \sigma\pi$; so we have to be very careful about the order of the factors in a product of permutations.

Important note 2: But the good news is that the composition of permutations is associative, i.e., $(\pi\sigma)\tau = \pi(\sigma\tau)$ for all permutations π, σ, τ.

To prove this we have to compute:

$$[(\pi\sigma)\tau](i) = (\pi\sigma)(\tau(i)) = \pi(\sigma(\tau(i))),$$
$$[\pi(\sigma\tau)](i) = \pi((\sigma\tau)(i)) = \pi(\sigma(\tau(i))).$$

We see that the right hand sides are the same in both cases, thus the left hand sides are the same too.

We can also calculate the inverse of a permutation; for example, using the same π as above, we find

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 4 & 1 & 6 & 2 & 7 & 5 \end{pmatrix}.$$

Explanation: just read the array for π from the bottom up: since $\pi(1) = 4$, we must have $\pi^{-1}(4) = 1$, hence write 1 under the 4 in the array for π^{-1}, since $\pi(2) = 6$, we must have $\pi^{-1}(6) = 2$, hence write 2 under the 6 in the array for π^{-1}, etc.

Similarly, we calculate

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 2 & 3 & 4 & 8 & 6 \end{pmatrix}.$$

Simple algebra shows that the inverse of a product can be calculated from the product of the inverses (but note how the order is reversed!):

$$(\pi\sigma)^{-1} = \sigma^{-1}\pi^{-1}.$$

(To justify this, we need only check if the product of $\pi\sigma$ and $\sigma^{-1}\pi^{-1}$ equals the identity, and this is pure algebra: it follows from the associative law that $(\pi\sigma)(\sigma^{-1}\pi^{-1}) = ((\pi\sigma)\sigma^{-1})\pi^{-1} = \pi(\sigma\sigma^{-1})\pi^{-1} = \pi\pi^{-1} = \mathrm{id}$.)

Definition 2. The set of all permutations of degree n, with the composition as the multiplication, is called the *symmetric group of degree n*, and is denoted by S_n.

3 Cycles

A permutation $\pi \in S_n$ which "cyclically permutes" some of the numbers $1, \ldots, n$ (and leaves all others fixed) is called a *cycle*.

For example, the permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 3 & 7 & 4 & 6 & 2 \end{pmatrix}$ is a cycle, because we have $5 \xrightarrow{\pi} 4 \xrightarrow{\pi} 7 \xrightarrow{\pi} 2 \xrightarrow{\pi} 5$, and each of the other elements of $\{1, 2, 3, 4, 5, 6, 7\}$ stays unchanged, namely $3 \xrightarrow{\pi} 3$, $6 \xrightarrow{\pi} 6$. To see that, we must of course chase an element around, the nice cyclic structure is not immediately evident from our notation. We write $\pi = (5\ 4\ 7\ 2)$, meaning that all numbers not on the list are mapped to themselves, whilst the ones in the bracket are mapped to the one listed to the right, the rightmost one going back to the leftmost on the list.

Note: cycle notation is not unique, since there is no beginning or end to a circle. We can write $\pi = (5\ 4\ 7\ 2)$ and $\pi = (2\ 5\ 4\ 7)$, as well as $\pi = (4\ 7\ 2\ 5)$ and $\pi = (7\ 2\ 5\ 4)$—they all denote one and the same cycle.

We say that a cycle is of length k (or a k-cycle) if it involves k numbers. For example, $(3\ 6\ 4\ 9\ 2)$ is a 5-cycle, $(3\ 6)$ is a 2-cycle, $(1\ 3\ 2)$ is a 3-cycle. We note also that the inverse of a cycle is again a cycle. For example

$(1\ 2\ 3)^{-1} = (1\ 3\ 2)$ (or $(3\ 2\ 1)$ if you prefer this). Similarly, $(1\ 2\ 3\ 4\ 5)^{-1} = (1\ 5\ 4\ 3\ 2)$. Finding the inverse of a cycle one has to reverse the arrows.

Not all permutations are cycles; for example, the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 3 & 2 & 11 & 8 & 9 & 5 & 6 & 7 & 10 & 1 & 12 \end{pmatrix}$$

is not a cycle (we have $1 \overset{\sigma}{\mapsto} 4 \overset{\sigma}{\mapsto} 11 \overset{\sigma}{\mapsto} 1$, but *the other elements are not all fixed* (2 goes to 3, for example). However, this permutation σ —and any other permutation — can be written as a product of *disjoint cycles*, simply by chasing each of the elements. The obvious approach is to visualise what the permutation σ does: (draw your picture here!)

From this it is evident that every permutation can be written as a product of disjoint cycles. Moreover, any such representation is unique up to the order of the factors. We also note that *disjoint* cycles commute; e.g.

$$(1\ 2\ 3\ 4)(5\ 6\ 7) = (5\ 6\ 7)(1\ 2\ 3\ 4).$$

But we recall that in general multiplication of permutations is *not commutative*; in particular, if we multiply cycles which are not disjoint, we have to watch their order; for example: $(1\ 2)(1\ 3) = (1\ 3\ 2)$, whilst $(1\ 3)(1\ 2) = (1\ 2\ 3)$, and $(1\ 3\ 2) \neq (1\ 2\ 3)$.

It is clear that if τ is a cycle of length k, then $\tau^k = \mathrm{id}$, i.e. if this permutation is repeated k times, we have the identity permutation. More generally, we will now define the order of a permutation, and the decomposition into a product of disjoint cycles will allow us to calculate the order of any permutation.

Definition 3. Let π be a permutation. The smallest positive integer i such that $\pi^i = \mathrm{id}$ is called the *order* of π.

Example 2. The order of the cycle $(3\ 2\ 6\ 4\ 1)$ is 5, as we noted before.

Example 3. The order of the permutation $\pi = (1\ 2)(3\ 4\ 5)$ is $2 \cdot 3 = 6$.

Indeed,

$$\begin{aligned}
\pi &= (1\ 2)(3\ 4\ 5),\\
\pi^2 &= (1\ 2)^2(3\ 4\ 5)^2 = (3\ 5\ 4),\\
\pi^3 &= (1\ 2)^3(3\ 4\ 5)^3 = (1\ 2),\\
\pi^4 &= (1\ 2)^4(3\ 4\ 5)^4 = (3\ 4\ 5),\\
\pi^5 &= (1\ 2)^5(3\ 4\ 5)^5 = (1\ 2)(3\ 5\ 4),\\
\pi^6 &= \mathrm{id}.
\end{aligned}$$

Example 4. The order of the cycle (3 2 6 4 1) is 5, as we noted before.

Example 5. The order of the permutation $\varphi = (1\ 2)(3\ 4\ 5\ 6)$ is 4. Indeed,

$$\begin{aligned}
\varphi &= (1\ 2)(3\ 4\ 5\ 6),\\
\varphi^2 &= (1\ 2)^2(3\ 4\ 5\ 6)^2 = (3\ 5)(4\ 6),\\
\varphi^3 &= (1\ 2)^3(3\ 4\ 5\ 6)^3 = (1\ 2)(3\ 6\ 5\ 4),\\
\varphi^4 &= \mathrm{id}.
\end{aligned}$$

This suggests that the order of a product of *disjoint* cycles equals the lcm of the lengths of these cycles. This can be formalised in the following

Theorem 1. *Let σ be a permutation and $\sigma = \tau_1\tau_2\cdots\tau_r$ be the decomposition of σ into a product of disjoint cycles. Let k be the order of σ and $k_1, k_2, \ldots, k_r$ be the orders (lengths) of $\tau_1, \tau_2, \ldots, \tau_r$, respectively. Then*

$$k = lcm\,(k_1, k_2, \ldots, k_r).$$

Proof. We first notice that $\tau_i^m = \mathrm{id}$ iff m is a multiple of k_i. Then, since the cycles τ_i are disjoint, we know that they commute and hence

$$\sigma^m = \tau_1^m\tau_2^m\ldots\tau_r^m.$$

The powers $\tau_1^m, \tau_2^m, \ldots, \tau_r^m$ act on disjoint sets of indices and, if $\sigma^m = \mathrm{id}$, it must be $\tau_1^m = \tau_2^m = \ldots = \tau_r^m = \mathrm{id}$. Indeed, if say $\tau_s^m(i) = j$ with $i \neq j$, then the product $\tau_1^m\tau_2^m\ldots\tau_r^m$ cannot be equal to id because all permutations $\tau_1^m, \ldots, \tau_{s-1}^m, \tau_{s+1}^m, \ldots, \tau_r^m$ leave i and j invariant. Thus the order of σ is a multiple of each of the $k_1, k_2, \ldots, k_r$ and hence the multiple of the least common multiple of them. On the other hand, it is clear that $\sigma^{\mathrm{lcm}\,(k_1,k_2,\ldots,k_r)} = \mathrm{id}$, which proves the theorem. □

Example 6. The order of $\sigma = (1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9)(10\ 11\ 12)(13\ 14\ 15\ 16\ 17)$ is 60.

Example 7. To determine the order of an arbitrary permutation, first write it as product of disjoint cycles. For example,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 3 & 2 & 11 & 8 & 9 & 5 & 6 & 7 & 10 & 1 & 12 \end{pmatrix} = (1\ 4\ 11)(2\ 3)(5\ 8\ 6\ 9\ 7)$$

and therefore the order of σ is 30.

4 Transpositions. Even and Odd

Cycles of length 2 are the simplest permutations, as they involve only 2 objects. We define

Definition 4. A cycle of length 2 is called a *transposition*.

It is intuitively plausible that any permutation is a product of transpositions (every arrangement of n objects can be obtained from a given starting position by making a sequence of swaps). Once we observe how a cycle of arbitrary length can be expressed as a product of transpositions, we can express any permutation as product of transpositions. Here are some examples:

Example 8. $(1\ 2\ 3\ 4\ 5) = (1\ 5)(1\ 4)(1\ 3)(1\ 2)$ (just check that the left hand side equals the right hand side!).

Exactly in the same way we can express an arbitrary cycle as a product of transpositions:

$$(i_1\ i_2\ \ldots\ i_r) = (i_1\ i_r)\ldots(i_1\ i_3)(i_1\ i_2). \tag{1}$$

Example 9. To express any permutation σ as product of transpositions, first decompose σ into a product of disjoint cycles, then write each cycle as product of transpositions as shown above. For example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 4 & 3 & 2 & 11 & 8 & 9 & 5 & 6 & 7 & 10 & 1 \end{pmatrix} = (1\ 4\ 11)(2\ 3)(5\ 8\ 6\ 9\ 7) =$$

$$(1\ 11)(1\ 4)(2\ 3)(5\ 7)(5\ 9)(5\ 6)(5\ 8).$$

Example 10. Note that there are many different ways to write a permutation as product of transpositions; for example

$$(1\ 2\ 3\ 4\ 5) = (1\ 5)(1\ 4)(1\ 3)(1\ 2) = (3\ 2)(3\ 1)(3\ 5)(3\ 4) =$$

$$(3\ 2)(3\ 1)(2\ 1)(2\ 3)(1\ 3)(2\ 3)(3\ 5)(3\ 4).$$

(Don't ask how these products were found! The point is to check that all these products are equal, and to note that there is nothing unique about how one can write a permutation as product of transpositions.)

Definition 5. A permutation is called *even* if it can be written as a product of an even number of transpositions. A permutation is called *odd* if it can be written as a product of an odd number of transpositions.

An important point is that there is no permutation that is at the same time even and odd—this justifies the use of the terminology.[1] We will establish that by looking at the polynomial

$$f(x_1, x_2, \ldots, x_n) = \prod_{i<j}(x_i - x_j). \tag{2}$$

Example 11. For $n = 3$, the polynomial (2) will look like

$$f(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3).$$

If $\sigma = (1\ 3)$, we may compute

$$f(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}) = (x_3 - x_2)(x_3 - x_1)(x_2 - x_1) = -f(x_1, x_2, x_3).$$

This leads us to

Proposition 2. *For any permutation σ from S_n*

$$f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = \pm f(x_1, x_2, \ldots, x_n). \tag{3}$$

Proof. In the left-hand-side of (3), for any pair of indices i and j, we have either $x_i - x_j$ or $x_j - x_i$ (but not both) wil be a factor. Thus the left-hand-side can differ from the right-hand-side by its sign only. This proves (3). □

We will write $\mathrm{sign}(\sigma) = 1$, if we have "+" in (3) and $\mathrm{sign}(\sigma) = -1$ otherwise. We notice that

$$\mathrm{sign}(\sigma\tau) = \mathrm{sign}(\sigma)\mathrm{sign}(\tau). \tag{4}$$

Indeed,

$$f(x_{\sigma\tau(1)}, x_{\sigma\tau(2)}, \ldots, x_{\sigma\tau(n)}) = \mathrm{sign}(\sigma) f(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}) =$$

$$\mathrm{sign}(\sigma)\mathrm{sign}(\tau) f(x_1, x_2, \ldots, x_n),$$

[1] You may skip this proof for the first reading and go straight to Example 12.

which shows that sign($\sigma\tau$) =sign(σ)sign(τ) holds.

It is clear that for $\pi = (i\ i{+}1)$ we have

$$f(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}) = -f(x_1, x_2, \ldots, x_n) \tag{5}$$

(only one factor changes its sign), hence sign($(i\ i{+}1)$) $= -1$. Since

$$(i\ k{+}1) = (k\ k{+}1)(i\ k)(k\ k{+}1),$$

and due to (4), we see that sign($(i\ k)$) $= -1$ implies sign($(i\ k{+}1)$) $= -1$. This means that by induction (5) can be extended to an arbitrary transposition π. Hence (5) will be true for any odd permutation π, i.e sign(π) $= -1$. At the same time, it is clear that for every even permutation π we will have sign(π) $= +1$. This implies that there is no permutation which is both even and odd.

Example 12. (1 2 3 4) is an odd permutation, because (1 2 3 4) = (1 4)(1 3)(1 2).

(1 2 3 4 5) is an even permutation, because (1 2 3 4 5) = (1 5)(1 4)(1 3)(1 2).

Example 13. Since id = (1 2)(1 2), the identity is even.

Theorem 3. *A k-cycle is even if k is odd; a k-cycle is odd if k is even.*

Proof. Immediately follows from (1). □

Example 14. Let $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 2 & 5 & 1 & 6 & 9 & 8 & 7 \end{pmatrix}$. Is π even or odd?

First decompose π into a product of cycles, then use the result above:

$$\pi = (1\ 4\ 5)(2\ 3)(7\ 9) \quad (= (1\ 5)(1\ 4)(2\ 3)(7\ 9)).$$

We have an even number (two) of odd cycles, it shows that π is even.

Definition 6. We say that two permutations have the same parity, if they are both odd or both even, and different parities, if one of them is odd and another is even.

Theorem 4. *In any symmetric grooup S_n*

1. *The product of two even permutations is even.*
2. *The product of two odd permutations is even.*
3. *The product of an even permutation and an odd one is odd.*
4. *A permutation and its inverse are of the same parities.*

Proof. Only the statements 4 needs a comment. It follows from 1 and 2. Indeed, since the identity permutation id is even, we cannot have a permutation and its inverse being of different parities. □

Theorem 5. *Exactly half of the elements of S_n are even and half of them are odd.*

Proof. Denote by E the set of even permutations in S_n, and by O the set of odd permutations in S_n. If τ is any fixed transposition from S_n, we can establish a one-to-one correspondence between E and O as follows: for π in E we know that $\tau\pi$ belongs to O. Therefore we have a mapping $f\colon E \to O$ defined by $f(\pi) = \tau\pi$. f is one-to-one since $\tau\pi = \tau\sigma$ implies that $\pi = \sigma$; f is onto, because if κ is an odd permutation then $\tau\kappa$ is even, and $f(\tau\kappa) = \tau\tau\kappa = \kappa$. □

Corollary 6. *The number of even permutations in S_n is $\frac{n!}{2}$. The number of odd permutations in S_n is also $\frac{n!}{2}$.*

Definition 7. The set of all even permutations of degree n is called the *alternating group of degree n*. It is denoted by A_n.

Example 15. We can have a look at the elements of S_4, listing all of them, and checking which of them are even, which of them are odd.

$$\begin{aligned} S_4 = \{&\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (2\ 3\ 4), (2\ 4\ 3),\\ &(1\ 3\ 4), (1\ 4\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3),\\ &(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4), (1\ 2\ 3\ 4), (1\ 4\ 3\ 2),\\ &(1\ 3\ 2\ 4), (1\ 4\ 2\ 3), (1\ 2\ 4\ 3), (1\ 3\ 4\ 2)\} \end{aligned}$$

The elements in the first 2 lines are even permutations, and the remaining elements are odd. We have

$$\begin{aligned} A_4 = \{&\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (2\ 3\ 4), (2\ 4\ 3),\\ &(1\ 3\ 4), (1\ 4\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}. \end{aligned}$$

5 The interlacing shuffle. Puzzle 15

In this section we consider two applications of permutations.

We have a deck of $2n$ cards (normally 52), we split it into 2 halves and then interlace them as follows. Suppose that our cards were numbered from 1 to $2n$ and the original order of cards was

$$a_1 a_2 a_3 \dots a_{2n-1} a_{2n}$$

Then the two halves will contain the cards $a_1, a_2, \dots, a_n$ and $a_{n+1} a_{n+2}, \dots, a_{2n}$, respectively. The interlacing shuffle will put the first card of the second pile first, then the first card of the first pile, then the second card of the second pile, then the second card of the first pile etc. After the shuffle the order of cards will be:

$$a_{n+1} a_1 a_{n+2} a_2 \dots a_{2n} a_n$$

We put the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n & n+1 & n+2 & \dots & 2n \\ 2 & 4 & 6 & \dots & 2n & 1 & 3 & \dots & 2n-1 \end{pmatrix}$$

in correspondence to this shuffle. We see that

$$\sigma(i) = 2i \bmod 2n+1$$

where $\sigma(i)$ is the position of the ith card after the shuffle.

Example 16. $n = 5$

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 4 & 6 & 8 & 10 & 1 & 3 & 5 & 7 & 9 \end{pmatrix} = \\ &= \begin{pmatrix} 1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \end{pmatrix}. \end{aligned}$$

What will happen after $2, 3, 4, \dots$ shuffles? The resulting change will be characterised by the permutations $\sigma^2, \sigma^3, \sigma^4, \dots$, respectively.

In the example above

$$\begin{aligned} \sigma^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 8 & 1 & 5 & 9 & 2 & 6 & 10 & 3 & 7 \end{pmatrix} = \\ &= \begin{pmatrix} 1 & 4 & 5 & 9 & 3 \end{pmatrix} \begin{pmatrix} 2 & 8 & 10 & 7 & 6 \end{pmatrix} \end{aligned}$$

Also $\sigma^{10} = \mathrm{id}$ and 10 is the order of σ. Hence all cards will be back to their initial positions after 10 shuffles but not before.

Example 17. $n = 4$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 8 & 7 & 5 \end{pmatrix} \begin{pmatrix} 3 & 6 \end{pmatrix}$$

The order of σ is 6.

We close this section with a few words about a game played with a simple toy. This game seems to have been invented in the 1870s by the famous puzzle-maker Sam Loyd. It caught on and became the rage in the United States in the 1870s, and finally led to a discussion by W. Johnson in the scholarly journal, the *American Journal of Mathematics*, in 1879. It is often called the "fifteen puzzle". Our discussion will be without full proofs.

Consider a toy made up of 16 squares, numbered from 1 to 15 inclusive and with the lower right-hand corner blank.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

The toy is constructed so that squares can be slid vertically and horizontally, such moves being possible because of the presence of the blank square.

Start with the position shown and perform a sequence of slides in such a way that, at the end, the lower right-hand square is again blank. Call the new position "realisable." Question: What are all possible realisable positions?

What do we have here? After such a sequence of slides we have shuffled about the numbers from 1 to 15; that is, we have effected a permutation of the numbers from 1 to 15. To ask what positions are realisable is merely to ask what permutations can be carried out. In other words, in S_{15}, the symmetric group of degree 15, what elements can be reached via the toy? For instance, can we get

13	4	12	15
1	14	9	6
8	3	2	7
10	5	11	

To answer, we will characterise every position of this game by a permutation. We will denote the empty square by the number 16. The position

a_1	a_2	a_3	a_4
a_5	a_6	a_7	a_8
a_9	a_{10}	a_{11}	a_{12}
a_{13}	a_{14}	a_{15}	a_{16}

will be characterised by the transposition

$$\begin{pmatrix} 1 & 2 & \dots & 16 \\ a_1 & a_2 & \dots & a_{16} \end{pmatrix}.$$

Example 18. The position

1	3	5	7
9	11	13	15
2	4		6
8	10	12	14

will correspond to the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 3 & 5 & 7 & 9 & 11 & 13 & 15 & 2 & 4 & 16 & 6 & 8 & 10 & 12 & 14 \end{pmatrix}.$$

If we make a move pulling down the square 13, then the new position will be

1	3	5	7
9	11		15
2	4	13	6
8	10	12	14

and the new permutation is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 3 & 5 & 7 & 9 & 11 & 16 & 15 & 2 & 4 & 13 & 6 & 8 & 10 & 12 & 14 \end{pmatrix} = \begin{pmatrix} 13 & 16 \end{pmatrix} \sigma.$$

Theorem 7. *If a position characterised by the permutation σ can be transformed by legal moves to the initial position, then there exist permutations $\tau_1, \tau_2, \ldots, \tau_m$ such that*

$$id = \tau_1 \tau_2 \ldots \tau_m \sigma. \tag{6}$$

If the empty square was in the right bottom corner, then m is even and τ is even.

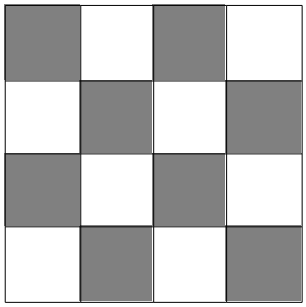
Proof. As we have seen every legal move is equivalent to multiplying the permutation corresponding to the existing position by a transposition $(i\ 16)$.

Then (6) follows. In this case:

$$\sigma = \tau_m \tau_{m-1} \ldots \tau_2 \tau_1$$

hence the parity of σ is the same as that of m.

Let us colour the board in the chessboard pattern



Every move changes the colour of the empty square. Thus, if at the beginning and at the end the empty square was black, then there was an even number of moves made. Therefore, if initially the right bottom corner was empty and we could transform this position to the initial position, then an even number of moves was made, m is even, and σ is also even. □

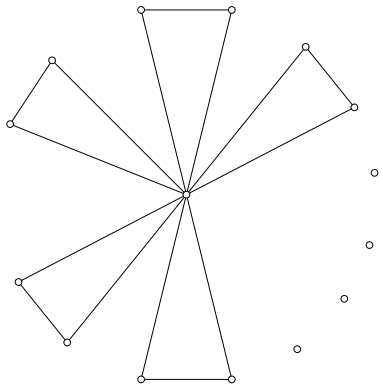
It can be shown that every position, with an even permutation σ can be transformed to the initial positon but no easy proof is known.

Combinatorics. Tutorial 2: Friendship Theorem

This wonderful theorem has a very simple commonsense formulation. Namely, given a society in which any two people have exactly one friend in common, there must be a "host," who is everybody's friend. Of course, this is a graph-theoretic theorem and in order to prove it we must express it in graph-theoretic terms.

Theorem 1 (Friendship Theorem). *Suppose that G is a graph such that, if x and y are any two distinct vertices of G, then there is a unique vetex z adjacent in G to both x and y. Then there is a vertex adjacent to all other vertices.*

From this, it immediately follows that the graph G is a "windmill" like the one below:



We will prove this theorem in several steps.[1] We will assume that a counterexample G to the Friendship theorem does exist and will be working with this counterexample until we get a contradiction. Then the theorem will be established.

[1] following largely J.Q. Longyear and T.D Parsons (1972)

Definition 1. *A sequence of vertices $x_0, x_1, \ldots, x_n$ will be called a path of length n, if x_{i-1} is adjacent to x_i for all $i = 1, 2, \ldots, n$. These vertices need not be all different, i.e. going along this path we may visit a certain vertex several times. Any path $x_0, x_1, \ldots, x_{n-1}, x_0$ is called a cycle of length n.*

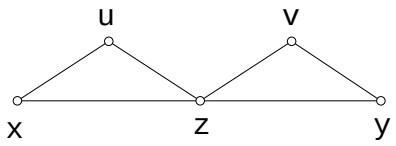
Lemma 1. *G does not have any cycles of length 4.*

Proof. If we had a cycle $x_0, x_1, x_2, x_3, x_4, x_0$ of length 4, then x_0 and x_2 would have at least two neighbors in common, namely x_1 and x_3, which is not possible. □

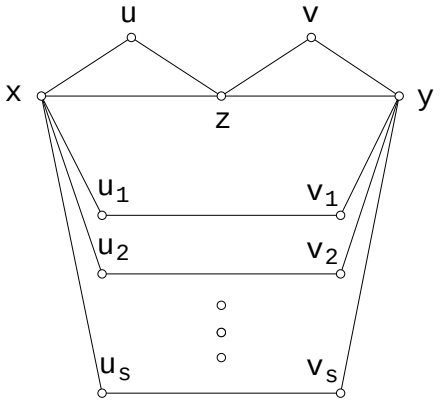
Definition 2. *The degree of a vertex is the number of other vertices adjacent to it. The graph is called regular, if all its vertices have the same degree.*

Lemma 2. *Any two nonadjacent vertices of G have the same degree.*

Proof. Let x and y be two nonadjacent vertices and let z be their unique common neighbor. Then x and z will have a unique common neighbor u and y and z will have a unique common neighbor v.



Now let $u_1, u_2, \ldots, u_s$ be all other vertices adjacent to x. For each $i = 1, 2, \ldots, s$, let v_i be the unique common neighbor of u_i and y. By inspection we check that v_i is different from any of the x, z, y, u, v, u_i (every such assumption lead to the existence of a 4-cycle). Also, no two vertices v_i and v_j can coincide for $i \neq j$, according to the same reason.



Thus, we see that the degree of x is not greater than the degree of y. But the situation is symmetric, i.e. we can also prove that the degree of y is not greater than the degree of x. Hence, these two degrees coincide. □

Lemma 3. *G is regular.*

Proof. Let $d(x)$ denote the degree of the vertex x. Suppose that G is not regular and that there exist two vertices a and b such that $d(a) \neq d(b)$. Then a and b must be adjacent by Lemma 2. There is a unique common neighbor c of a and b. Since either $d(c) \neq d(a)$ or $d(c) \neq d(b)$, or both, we may assume that the former is true and $d(c) \neq d(a)$. Now let x be any other vertex. Then x is adjacent to one of a or b, for otherwise by Lemma 2 $d(a) = d(x) = d(b)$, contrary to the assumption that $d(a) \neq d(b)$. Similarly, x is adjacent to either a or c. But x cannot be adjacent to both b and c, as a is their unique common neighbor, hence x must be adjacent to a. This now shows that all vertices of G are adjacent to a and G is not a counterexample. Hence G is regular. □

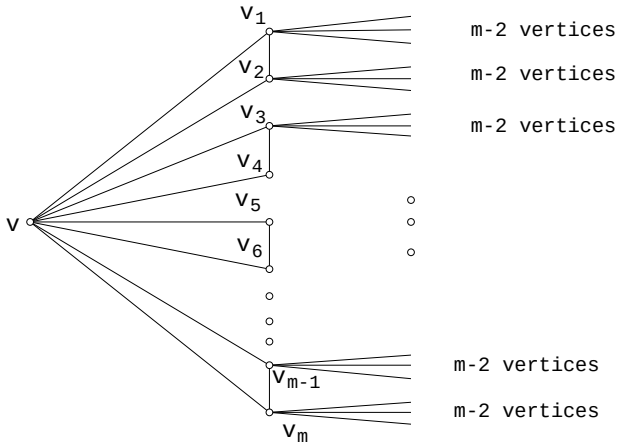
Let m be the degree of G.

Lemma 4. *m is an even number.*

Proof. Let $v_1, v_2, \ldots, v_m$ be the vertices adjacent to v. Let us consider v_1. Together with v it must have a vertex which is adjacent to both. Since $v_1, v_2, \ldots, v_m$ are all vertices adjacent to v, this third vertex must be among $v_1, v_2, \ldots, v_m$. Let it be v_2. No other vertex among $v_1, v_2, \ldots, v_m$ can be adjacent to v_1 or to v_2. Thus v_1 and v_2 form a pair. This way we can pair off the vertices adjacent to v which implies that m is even. We show that the neighborhood of every vertex v looks like a "windmill." □

Lemma 5. *Let N be the number of vertices of G. Then $N = m(m-1)+1$.*

Proof. Let v be any vertex and $v_1, v_2, \ldots, v_m$ be the vertices adjacent to v. We know that the neighborhood of v looks like a "windmill." Without loss of generality we assume that the vertices are paired off so that v_1 is adjacent to v_2, v_3 is adjacent to v_4 and finally v_{m-1} is adjacent to v_m. Every vertex different from v and $v_1, v_2, \ldots, v_m$ must be adjacent to one of the v_i since it must have a common neighbor with v. Each v_i will have exactly $m-2$ neighbors of this kind. In total we then have $N = 1 + m + m(m-2) = m(m-1)+1$ vertices. □



Let us now note that $m > 2$, or else G is just a triangle which is not a counterexample. Let p be any prime which divides $m - 1$. Since $m - 1$ is odd, p is also odd. In the following two lemmas we will consider the set S of all cycles $v_0, v_1, \ldots, v_{p-1}, v_0$ of length p with the fixed initial point v_0. This means that the same cycle with two different initial vertices will be considered as two different elements of S. Let us agree that if the cycle is written as $v_0, v_1, \ldots, v_{p-1}, v_0$, then v_0 is chosen as its initial point. Note that we again do not require that all vertices in the cycle are different.

We shall compute the cardinality $|S|$ of S in two ways.

Lemma 6. *$|S|$ is a multiple of p.*

Proof. Every cycle of length p with the fixed initial point

$$v_0, v_1, \ldots, v_{p-1}$$

gives us $p - 1$ other cycles by changing the initial point of it: $v_1, v_2, \ldots, v_0$, and $v_2, v_3, \ldots, v_1$, and so on. No two of such sequences are the same, assuming the opposite will contradict to the primeness of p (see the solution to Exercise 9 of the assignment "Many faces of mathematical Induction"). Since in every cycle of length p we can choose p initial points, and hence get p different elements of S, it is clear that $|S|$ is divisible by p. □

Proof of the Friendship Theorem. Now we will prove that $|S|$ is NOT divisible by p which will give us a contradiction and the proof will be therefore complete.

First, we will count the number of vertex sequences $v_0, v_1, \ldots, v_{p-2}$, such that v_i is adjacent to v_{i+1} for all $i = 0, 1, \ldots, p - 2$. There are two types

of such sequences: 1) those for which $v_0 = v_{p-2}$ and 2) those for which $v_0 \neq v_{p-2}$. Let K_1 and K_2 be the number of sequences of the first and the second type, respectively. Then $K_1 + K_2 = Nm^{p-2}$. Indeed, we can choose v_0 in N different ways, and having chosen $v_0, v_1, \ldots, v_i$, we can choose v_{i+1} in m different ways. Now we will return to cycles with fixed initial vertices from S. Each of them can be obtained from a sequence of one of the above types by adding a vertex v_{p-1} which is adjacent to v_0 and v_{p-2} and considering v_0 as the initial vertex of this cycle. If $v_0 = v_{p-2}$, then we can choose v_{p-1} in m different ways, while if $v_0 \neq v_{p-2}$, then such v_{p-1} will be unique. Thus $|S| = mK_1 + K_2$. But now

$$|S| = (m-1)K_1 + (K_1 + K_2) = (m-1)K_1 + Nm^{p-2} \equiv Nm^{p-2} \pmod{p}$$

But $N \equiv 1 \pmod{p}$, and $m = (m-1) + 1 \equiv 1 \pmod{p}$, thus $|S| \equiv 1 \pmod{p}$ which is a contradiction.

Therefore the Friendship theorem is proved. □

Number Theory. Tutorial 1: Divisibility and Primes

1 Introduction

The theory of numbers is devoted to studying the set $\mathbb{N} = \{1, 2, 3, 4, 5, 6, \ldots\}$ of positive integers, also called the *natural numbers*. The most important property of $\mathbb{N}$ is the following axiom (which means that it cannot be proved):

Axiom 1 (The Least-integer Principle) *A non-empty set $S \subseteq \mathbb{N}$ of positive integers contains a smallest element.*

The set of all integers

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

is denoted by $\mathbb{Z}$. In this section we use letters of the roman alphabet

$$a, b, c, \ldots, k, l, m, n, \ldots, x, y, z$$

to designate integers unless otherwise specified.

Theorem 1 (The division algorithm) *Given any integers a, b, with $a > 0$, there exist unique integers q, r such that*

$$b = qa + r, \qquad 0 \leq r < a.$$

The number q is called the *quotient* and the number r is called the *remainder*. The notation $r = b \pmod{a}$ is often used.

Example 1 $35 = 3 \cdot 11 + 2$, $-51 = (-8) \cdot 7 + 5$*; so that* $2 = 35 \pmod{11}$ *and* $5 = -51 \pmod{7}$.

Definition 1 *An integer b is divisible by an integer $a \neq 0$, if there exists an integer c such that $b = ac$ or else it can be written as $0 = b \pmod{a}$. We also say that a is a* divisor *of b and write $a|b$.*

Let n be a positive integer. Let us denote by $d(n)$ the number of divisors of n. It is clear that 1 and n are always divisors of a number n which is greater than 1. Thus we have $d(1) = 1$ and $d(n) \geq 2$ for $n > 1$.

Definition 2 *An integer n is called a* prime *if $d(n) = 2$. An integer $n > 1$, which is not prime is called a* composite *number.*

Example 2 $2, 3, 5, 7, 11, 13$ *are primes;* $1, 4, 6, 8, 9, 10$ *are not primes;* $4, 6, 8, 9, 10$ *are composite numbers.*

Theorem 2 (The Fundamental Theorem of Arithmetic) *Every positive integer $n > 1$ can be expressed as a product of primes (with perhaps only one factor), that is*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},$$

where $p_1, p_2, \dots, p_n$ are distinct primes and $\alpha_1, \alpha_2, \dots, \alpha_n$ are positive integers. This factoring is unique apart from the order of the prime factors.

Proof: Let us prove first that any number $n > 1$ can be decomposed into a product of primes. If $n = 2$, the decomposition is trivial and we have only one factor, i.e., 2 itself. Let us assume that for all positive integers, which are less than n, a decomposition exists. If n is a prime, then $n = n$ is the decomposition required. If n is composite, then $n = n_1 n_2$, where $n > n_1 > 1$ and $n > n_2 > 1$ and by the induction hypothesis there are prime decompositions $n_1 = p_1 \dots p_r$ and $n_2 = q_1 \dots q_s$ for n_1 and n_2. Then we may combine them

$$n = n_1 n_2 = p_1 \dots p_r q_1 \dots q_s$$

and get the decomposition for n and prove the first statement.

To prove that the decomposition is unique, we shall assume the existence of an integer capable of two essentially different prime decompositions, and from this assumption derive a contradiction. This will show that the hypothesis that there exists an integer with two essentially different prime decompositions is untenable, and hence the prime decomposition of every integer is unique. We will use the Least-integer Principle.

Suppose that there exists an integer with two essentially different prime decompositions, then there will be a smallest such integer

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s, \tag{1}$$

where p_i and q_j are primes. By rearranging the order of the p's and the q's, if necessary, we may assume that

$$p_1 \le p_2 \le \dots \le p_r, \qquad q_1 \le q_2 \le \dots \le q_s.$$

It is impossible that $p_1 = q_1$, for if it were we could cancel the first factor from each side of equation (1) and to obtain two essentially different prime decompositions for a number smaller than n, contradicting the choice of n. Hence either $p_1 < q_1$ or $q_1 < p_1$. Without loss of generality we suppose that $p_1 < q_1$.

We now form the integer

$$n' = n - p_1 q_2 q_3 \dots q_s. \tag{2}$$

Then two decompositions of n give the following two decompositions of n':

$$n' = (p_1 p_2 \dots p_r) - (p_1 q_2 \dots q_s) = p_1(p_2 \dots p_r - q_2 \dots q_s), \tag{3}$$

$$n' = (q_1 q_2 \dots q_s) - (p_1 q_2 \dots q_s) = (q_1 - p_1)(q_2 \dots q_s). \tag{4}$$

Since $p_1 < q_1$, it follows from (4) that n' is a positive integer, which is smaller than n. Hence the prime decomposition for n' must be unique and, apart from the order of the factors, (3) and (4) coincide. From (3) we learn that p_1 is a factor of n' and must appear as a factor in decomposition (4). Since $p_1 < q_1 \le q_i$, we see that $p_1 \ne q_i$, $i = 2, 3, \dots, s$. Hence, it is a factor of $q_1 - p_1$, i.e., $q_1 - p_1 = p_1 m$ or $q_1 = p_1(m+1)$, which is impossible as q_1 is prime and $q_1 \ne p_1$. This contradiction completes the proof of the Fundamental Theorem of Arithmetic.

Let x be a real number. Then it can be written in a unique way as $z + e$, where $z \in \mathbb{Z}$ and $0 \le e < 1$. Then, the following notation is used: $z = \lfloor x \rfloor$, $z + 1 = \lceil x \rceil$, $e = \{x\}$. We will use here only the first function $\lfloor x \rfloor$, which is called *the integral part* of x. Examples: $\lfloor -2.5 \rfloor = -3$, $\lfloor \pi \rfloor = 3$, $\lfloor 5 \rfloor = 5$.

Theorem 3 *The smallest prime divisor of a composite number n is less than or equal to $\lfloor \sqrt{n} \rfloor$.*

Proof: We prove first that n has a divisor which is greater than 1 but less than $\sqrt{n}$. As n is composite, then $n = d_1 d_2$, $d_1 > 1$ and $d_2 > 1$. If $d_1 > \sqrt{n}$ and $d_2 > \sqrt{n}$, then

$$n = d_1 d_2 > (\sqrt{n})^2 = n,$$

a contradiction. Suppose, $d_1 \leq \sqrt{n}$. Then any of the prime divisors of d_1 will be less than or equal to $\sqrt{n}$. But every divisor of d_1 is also a divisor of n, thus the smallest prime divisor p of n will satisfy the inequality $p \leq \sqrt{n}$. Snce p is an integer, $p \leq \lfloor \sqrt{n} \rfloor$. The theorem is proved.

Theorem 4 (Euclid) *The number of primes is infinite.*

Proof: Suppose there were only finite number of primes $p_1, p_2, \ldots, p_r$. Then form the integer

$$n = 1 + p_1 p_2 \ldots p_r.$$

Since $n > p_i$ for all i, it must be composite. Let q be the smallest prime factor of n. As $p_1, p_2, \ldots, p_r$ represent all existing primes, then q is one of them, say $q = p_1$ and $n = p_1 m$. Now we can write

$$1 = n - p_1 p_2 \ldots p_r = p_1 m - p_1 p_2 \ldots p_r = p_1 (m - p_2 \ldots p_r).$$

We have got that $p_1 > 1$ is a factor of 1, which is a contradiction.

The following three theorems are far from being elementary. Of course, no one jury assumes that students are familiar with these theorems. Nevertheless, some students use them and sometimes a difficult math olympiad problem can be trivialised by doing so. The attitude of the Jury of the International Mathematics Olympiad is to believe that students know what they use. Therefore it pays to understand these results even without a proof.

Let $\pi(x)$ denote the number of primes which do not exceed x. Because of the irregular occurence of the primes, we cannot expect a simple formula for $\pi(x)$. However one of the most impressive results in advanced number theory gives an asymptotic approximation for $\pi(x)$.

Theorem 5 (The Prime Number Theorem)

$$\lim_{x \to \infty} \pi(x) \frac{\ln x}{x} = 1,$$

where $\ln x$ *is the natural logarithm, to base* e.

Theorem 6 (Dirichlet's Theorem) *If a and b are relatively prime positive integers (which means that they don't have common prime factors in their prime factorisations), then there are infinitely many primes of the form $an + b$, where $n = 1, 2, \ldots$.*

Theorem 7 (Bertrand's Postulate, proved by Chebyschef) *For every positive integer $n > 1$ there is a prime p such that $n < p < 2n$.*

Number Theory. Tutorial 2:

The Euclidean algorithm

1 The number of divisors of n

Let n be a positive integer with the prime factorisation

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}, \tag{1}$$

where p_i are distinct primes and α_i are positive integers. How can we find all divisors of n? Let d be a divisor of n. Then $n = dm$, for some m, thus

$$n = dm = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},$$

Since the prime factorisation of n is unique, d cannot have in its prime factorisation a prime which is not among the primes $p_1, p_2, \dots, p_r$. Also, a prime p_i in the prime factorisation of d cannot have an exponent greater than α_i. Therefore

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}, \qquad 0 \le \beta_i \le \alpha_i, \qquad i = 1, 2, \dots, r. \tag{2}$$

Theorem 1. *The number of positive divisors of n is*

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1). \tag{3}$$

Proof. Indeed, we have exactly $\alpha_i + 1$ possibilities to choose β_i in (2), namely $0, 1, 2, \dots, \alpha_i$. Thus the total number of divisors will be exactly the product $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1)$. □

Definition 1. *The numbers kn, where $k = 0, \pm 1, \pm 2, \dots$, are called* multiples of n.

It is clear that any multiple of n given by (1) has the form

$$m = k p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r}, \qquad \gamma_i \ge \alpha_i, \qquad i = 1, 2, \dots, r,$$

where k has no primes $p_1, p_2, \dots, p_r$ in its prime factorisation. The number of multiples of n is infinite.

2 Greatest common divisor and least common multiple

Let a and b be two positive integers. If d is a divisor of a and also a divisor of b, then we say that d is a common divisor of a and b. As there are only a finite number of common divisors, there is a *greatest common divisor*, denoted by $\gcd(a,b)$. The number m is said to be a common multiple of a and b if m is a multiple of a and also a multiple of b. Among all common multiples there is a minimal one (Least-integer principle!). It is called the *least common multiple* and it is denoted by $\operatorname{lcm}(a,b)$.

In the decomposition (1) we had all exponents positive. However, sometimes it is convenient to allow some exponents to be 0. This is especially convenient, when we consider prime factorisations of two numbers a and b, looking for $\gcd(a,b)$ and $\operatorname{lcm}(a,b)$, since we may assume that both a and b have the same set of primes in their prime factorisations.

Theorem 2. *Let*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}, \qquad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r},$$

where $\alpha_i \geq 0$ and $\beta_i \geq 0$, be two arbitrary positive integers. Then

$$\gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \dots p_r^{\min(\alpha_r,\beta_r)}, \tag{4}$$

and

$$\operatorname{lcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \dots p_r^{\max(\alpha_r,\beta_r)}. \tag{5}$$

Moreover,

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = a \cdot b. \tag{6}$$

Proof. Formulas (4) and (5) follow from our description of common divisors and common multiples. To prove (6) we have to notice that $\min(\alpha_i,\beta_i) + \max(\alpha_i,\beta_i) = \alpha_i + \beta_i$. □

We suspect (in fact it is an open question) that prime factorisation is computationally difficult and we don't know easy algorithms for that but fortunately the greatest common divisor $\gcd(a,b)$ of numbers a and b can be found without knowing the prime factorisations for a and b. This algorithm was known to Euclid and maybe even was discovered by him.

Theorem 3 (The Euclidean Algorithm). *Let a and b be positive integers. We use the division algorithm several times to find:*

$$\begin{aligned}
a &= q_1 b \ + r_1, && 0 < r_1 < b,\\
b &= q_2 r_1 + r_2, && 0 < r_2 < r_1,\\
r_1 &= q_3 r_2 + r_3, && 0 < r_3 < r_2,\\
&\vdots\\
r_{s-2} &= q_s r_{s-1} + r_s, && 0 < r_s < r_{s-1},\\
r_{s-1} &= q_{s+1} r_s.
\end{aligned}$$

Then $r_s = \gcd(a, b)$.

Proof. Is based on the observation that if $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$. Indeed, if d is a common divisor of a and b, then $a = a'd$ and $b = b'd$ and then $r = a - qb = a'd - qb'd = (a' - qb')d$ and d is also a common divisor of b and r. Also if d is a common divisor of b and r, then $b = b'd$, $r = r'd$ and $a = qb + r = qb'd + r'd = (qb' + r')d$, whence d is a common divisor of a and b.

It is clear now that $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{s-1}, r_s) = r_s$. □

Theorem 4 (The Extended Euclidean Algorithm). *Let us write the following table with two rows R_1, R_2, and three columns:*

$$\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}.$$

In accordance with the Euclidean Algorithm above, we perform the following operations with rows of this table. First we will create the third row R_3 by subtracting from the first row the second row times q_1, we denote this as $R_3 := R_1 - q_1 R_2$. Then similarly we create the fourth row: $R_4 := R_2 - q_2 R_3$. We will continue this process as follows: when creating R_k we will obtain it taking R_{k-2} and subtracting R_{k-1} times q_{k-2}, which can be written symbolically as

$R_k := R_{k-2} - q_{k-2}R_{k-1}$. *Eventually we will obtain the table:*

$$\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \\ r_1 & 1 & -q_1 \\ r_2 & -q_2 & 1+q_1q_2 \\ & \vdots & \\ r_s & m & n \end{pmatrix}.$$

Then $\gcd(a,b) = r_s = am + bn$.

Proof. We will prove this by induction. Let the kth row of the table be

$$R_k = (u_k, v_k, w_k).$$

We assume that $u_i = av_i + bw_i$ for all $i < k$. This is certainly true for $i = 1, 2$. Then by induction hypothesis

$$u_k = u_{k-2} - q_k u_{k-1} = av_{k-2} + bw_{k-2} - q_k(av_{k-1} + bw_{k-1}) =$$

$$a(v_{k-2} - q_k v_{k-1}) + b(w_{k-2} - q_k w_{k-1}) = av_k + bw_k.$$

Thus the statement $u_i = av_i + bw_i$ is true for all i. In particular, this is true for the last row, which gives us $r_s = am + bn$. □

Example 1. *Let* $a = 321$, $b = 843$. *Find the greatest common divisor* $\gcd(a,b)$, *the least common multiple* $\operatorname{lcm}(a,b)$, *and a linear presentation of the greatest common divisor in the form* $\gcd(a,b) = ka + mb$.

The Euclidean algorithm:

$$\begin{aligned} 321 &= 0 \cdot 843 + 321 \\ 843 &= 2 \cdot 321 + 201 \\ 321 &= 1 \cdot 201 + 120 \\ 201 &= 1 \cdot 120 + 81 \\ 120 &= 1 \cdot 81 + 39 \\ 81 &= 2 \cdot 39 + 3 \\ 39 &= 13 \cdot 3 + 0, \end{aligned}$$

and therefore $\gcd(321, 843) = 3$ *and* $\operatorname{lcm}(321, 843) = \dfrac{321 \cdot 843}{3} = 107 \cdot 843 = 90201$. *The Extended Euclidean algorithm:*

321	1	0
843	0	1
321	1	0
201	−2	1
120	3	−1
81	−5	2
39	8	−3
3	−21	8

obtaining the linear presentation $\gcd(321, 843) = 3 = (-21) \cdot 321 + 8 \cdot 843$.

3 Relatively prime numbers

Definition 2. *If* $\gcd(a, b) = 1$*, the numbers* a *and* b *are said to be* relatively prime *(or* coprime*).*

The following properties of relatively prime numbers are often used.

Lemma 1. *Let* $\gcd(a, b) = 1$*, i.e.,* a *and* b *are relatively prime. Then*

1. *a and b do not have common primes in their prime factorisations;*
2. *If c is a multiple of a and also a multiple of b, then c is a multiple of ab;*
3. *If ac is a multiple of b, then c is a multiple of b;*
4. *There exist integers m, n such that $ma + nb = 1$.*

Proof. Part 1 follows from equation (4), parts 2 and 3 follow from part 1, and part 4 follows from Theorem 4. □

Theorem 5 (The Chinese remainder theorem). *Let a and b be two relatively prime numbers, $0 \le r < a$ and $0 \le s < b$. Then there exists a unique number N such that $0 \le N < ab$ and*

$$r = N \pmod{a} \quad \textit{and} \quad s = N \pmod{b}, \tag{7}$$

i.e., N has remainder r on dividing by a and remainder s on dividing by b.

Proof. Let us prove first, that there exists at most one integer N with the conditions required. Assume, on the contrary, that for two integers N_1 and N_2 we have $0 \leq N_1 < ab$, $0 \leq N_2 < ab$ and

$$r = N_1 \pmod a = N_2 \pmod a \quad \text{and} \quad s = N_1 \pmod b = N_2 \pmod b.$$

Let us assume that $N_1 > N_2$. Then the number $M = N_1 - N_2$ satisfies $0 \leq M < ab$ and

$$0 = M \pmod a \quad \text{and} \quad 0 = M \pmod b. \tag{8}$$

By Lemma 1 part 3, condition (8) implies that M is divisible by ab, whence $M = 0$ and $N_1 = N_2$.

Now we will find an integer N, such that $r = N \pmod a$ and $s = N \pmod b$, ignoring the condition $0 \leq N < ab$. By Theorem 4 there are integers m, n such that $\gcd(a, b) = 1 = ma + nb$. Multiplying this equation by $r - s$ we get the equation

$$r - s = (r - s)ma + (r - s)nb = m'a + n'b.$$

Now it is clear that the number

$$N = r - m'a = s + n'b$$

satisfies the condition (7). If N does not satisfy $0 \leq N < ab$, we divide N by ab with remainder $N = q \cdot ab + N_1$. Now $0 \leq N_1 < ab$ and N_1 satisfies (7). Theorem is proved. □

This is a constructive proof of the Chinese remainder theorem, which gives also an algorithm of calculating such N with property (7). A shorter but nonconsructive proof, which uses Pigeonhole principle can be found in the training material "Pigeonhole Principle." It is used there to prove Fermat's theorem that any prime of the type $4n + 1$ can be represented as a sum of two squares.

Number Theory. Tutorial 3:

Euler's function and Euler's Theorem

1 Euler's ϕ-function

Definition 1. *Let n be a positive integer. The number of positive integers less than or equal to n that are relatively prime to n, is denoted by $\phi(n)$. This function is called Euler's ϕ-function or Euler's totient function.*

Let us denote $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ and by $\mathbb{Z}_n^*$ the set of those nonzero numbers from $\mathbb{Z}_n$ that are relatively prime to n. Then $\phi(n)$ is the number of elements of $\mathbb{Z}_n^*$, i.e., $\phi(n) = |\mathbb{Z}_n^*|$.

Example 1. *Let $n = 20$. Then $\mathbb{Z}_{20}^* = \{1, 3, 7, 9, 11, 13, 17, 19\}$ and $\phi(20) = 8$.*

Lemma 1. *If $n = p^k$, where p is prime, then $\phi(n) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$.*

Proof. It is easy to list all integers that are less than or equal to p^k and not relatively prime to p^k. They are $p, 2p, 3p, \ldots, p^{k-1} \cdot p$. We have exactly p^{k-1} of them. Therefore $p^k - p^{k-1}$ nonzero integers from $\mathbb{Z}_n$ will be relatively prime to n. Hence $\phi(n) = p^k - p^{k-1}$. □

An important consequence of the Chinese remainder theorem is that the function $\phi(n)$ is multiplicative in the following sense:

Theorem 1. *Let m and n be any two relatively prime positive integers. Then*

$$\phi(mn) = \phi(m)\phi(n).$$

Proof. Let $\mathbb{Z}_m^* = \{r_1, r_2, \ldots, r_{\phi(m)}\}$ and $\mathbb{Z}_n^* = \{s_1, s_2, \ldots, s_{\phi(n)}\}$. By the Chinese remainder theorem there exists a unique positive integer N_{ij} such that $0 \leq N_{ij} < mn$ and

$$r_i = N_{ij} \pmod{m}, \qquad s_j = N_{ij} \pmod{n},$$

that is N_{ij} has remainder r_i on dividing by m, and remainder s_j on dividing by n, in particular for some integers a and b

$$N_{ij} = am + r_i, \qquad N_{ij} = bn + s_j. \tag{1}$$

As in Tutorial 2, in the proof of the Euclidean algorithm, we notice that $\gcd(N_{ij}, m) = \gcd(m, r_i) = 1$ and $\gcd(N_{ij}, n) = \gcd(n, s_j) = 1$, that is N_{ij} is relatively prime to m and also relatively prime to n. Since m and n are relatively prime, N_{ij} is relatively prime to mn, hence $N_{ij} \in \mathbb{Z}^*_{mn}$. Clearly, different pairs $(i, j) \neq (k, l)$ yield different numbers, that is $N_{ij} \neq N_{kl}$ for $(i, j) \neq (k, l)$.

Suppose now that a number $N \neq N_{ij}$ for all i and j. Then

$$r = N \pmod{m}, \qquad s = N \pmod{n},$$

where either r does not belong to $\mathbb{Z}^*_m$ or s does not belong to $\mathbb{Z}^*_n$. Assuming the former, we get $\gcd(r, m) > 1$. But then $\gcd(N, m) = \gcd(m, r) > 1$ and N does not belong to $\mathbb{Z}^*_{mn}$. It shows that the numbers N_{ij} and only they form $\mathbb{Z}^*_{mn}$. But there are exactly $\phi(m)\phi(n)$ of the numbers N_{ij}, exactly as many as the pairs (r_i, s_j). Therefore $\phi(mn) = \phi(m)\phi(n)$. □

Theorem 2. *Let n be a positive integer with the prime factorisation*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},$$

where p_i are distinct primes and α_i are positive integers. Then

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right).$$

Proof. We use Lemma 1 and Theorem 1 to compute $\phi(n)$:

$$\begin{aligned} \phi(n) &= \phi\left(p_1^{\alpha_1}\right) \phi\left(p_2^{\alpha_2}\right) \dots \phi\left(p_r^{\alpha_r}\right) \\ &= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \dots p_r^{\alpha_r} \left(1 - \frac{1}{p_r}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right). \end{aligned}$$

□

Example 2. $\phi(264) = \phi(2^3 \cdot 3 \cdot 11) = 264 \left(\frac{1}{2}\right) \left(\frac{2}{3}\right) \left(\frac{10}{11}\right) = 80.$

2 Congruences. Euler's Theorem

If a and b are intgers we write $a \equiv b \pmod{m}$ and say that a is congruent to b if a and b have the same remainder on dividing by m. For example, $41 \equiv 80 \pmod{1}3$, $41 \equiv -37 \pmod{1}3$, $41 \not\equiv 7 \pmod{1}3$.

Lemma 2. *Let a and b be two integers and m is a positive integer. Then*

(a) $a \equiv b \pmod{m}$ if and only if $a - b$ is divisible by m;

(b) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$;

(c) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$;

(d) If $a \equiv b \pmod{m}$ and n is a positive integer, then $a^n \equiv b^n \pmod{m}$;

(e) If $ac \equiv bc \pmod{m}$ and c is relatively prime to m, then $a \equiv b \pmod{m}$.

Proof. (a) By the division algorithm

$$a = q_1 m + r_1, \quad 0 \le r_1 < m, \text{ and } \quad b = q_2 m + r_2, \quad 0 \le r_2 < m.$$

Thus $a - b = (q_1 - q_2)m + (r_1 - r_2)$, where $-m < r_1 - r_2 < m$. We see that $a - b$ is divisible by m if and only if $r_1 - r_2$ is divisible by m but this can happen if and only if $r_1 - r_2 = 0$, i.e., $r_1 = r_2$.

(b) is an exercise.

(c) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $m|(a - b)$ and $m|(c - d)$, i.e., $a - b = im$ and $c - d = jm$ for some integers i, j. Then

$$ac - bd = (ac - bc) + (bc - bd) = (a - b)c + b(c - d) = icm + jbm = (ic + jb)m,$$

whence $ac \equiv bd \pmod{m}$;

(d) Follows immediately from (c)

(e) Suppose that $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$. Then there exist integers u, v such that $cu + mv = 1$ or $cu \equiv 1 \pmod{m}$. Then by (c)

$$a \equiv acu \equiv bcu \equiv b \pmod{m}.$$

and $a \equiv b \pmod{m}$ as required. □

The property in Lemma 2 (e) is called the *cancellation property.*

Theorem 3 (Fermat's Little Theorem). *Let p be a prime. If an integer a is not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$. Also $a^p \equiv a \pmod{p}$ for all a.*

Proof. Let a, be relatively prime to p. Consider the numbers a, $2a$, ..., $(p-1)a$. All of them have different remainders on dividing by p. Indeed, suppose that for some $1 \leq i < j \leq p-1$ we have $ia \equiv ja \pmod{p}$. Then by the cancellation property a can be cancelled and $i \equiv j \pmod{p}$, which is impossible. Therefore these remainders are 1, 2, ..., $p-1$ and

$$a \cdot 2a \cdot \cdots \cdot (p-1)a \equiv (p-1)! \pmod{p},$$

which is

$$(p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod{p}.$$

Since $(p-1)!$ is relatively prime to p, by the cancellation property $a^{p-1} \equiv 1 \pmod{p}$. When a is relatively prime to p, the last statement follows from the first one. If a is a multiple of p the last statement is also clear. □

Theorem 4 (Euler's Theorem). *) Let n be a positive integer. Then*

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

for all a relatively prime to n.

Proof. Let $\mathbb{Z}_n^* = \{z_1, z_2, \ldots, z_{\phi(n)}\}$. Consider the numbers z_1a, z_2a, ..., $z_{\phi(n)}a$. Both z_i and a are relatively prime to n, therefore z_ia is also relatively prime to n. Suppose that $r_i = z_ia \pmod{n}$, i.e., r_i is the remainder on dividing z_ia by n. Since $\gcd(z_ia, n) = \gcd(r_i, n)$, yielding $r_i \in \mathbb{Z}_n^*$. These remainders are all different. Indeed, suppose that $r_i = r_j$ for some $1 \leq i < j \leq n$. Then $z_ia \equiv z_ja \pmod{n}$. By the cancellation property a can be cancelled and we get $z_i \equiv z_j \pmod{n}$, which is impossible. Therefore the remainders $r_1, r_2, ..., r_{\phi(n)}$ coincide with $z_1, z_2, \ldots, z_{\phi(n)}$, apart from the order in which they are listed. Thus

$$z_1a \cdot z_2a \cdot \ldots \cdot z_{\phi(n)}a \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)} \equiv z_1 \cdot z_2 \cdot \ldots \cdot z_{\phi(n)} \pmod{n},$$

which is

$$Z \cdot a^{\phi(n)} \equiv Z \pmod{n},$$

where $Z = z_1 \cdot z_2 \cdot \ldots \cdot z_{\phi(n)}$. Since Z is relatively prime to n it can be cancelled and we get $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Number Theory. Tutorial 4: Representation of Numbers

1 Classical Decimal Positional System

There is an important distinction between numbers and their representations. In the decimal system the zero and the first nine positive integers are denoted by symbols $0, 1, 2, \ldots, 9$, respectively. These symbols are called *digits*. The same symbols are used to represent all the integers. The tenth integer is denoted as 10 and an arbitrary integer N can now be represented in the form

$$N = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10 + a_0, \tag{1}$$

where $a_0, a_1, \ldots, a_n$ are integers that can be represented by a single digit $0, 1, 2, \ldots, 9$. For example, the year, when I started to think about setting up this website, can be written as

$$1 \cdot 10^3 + 9 \cdot 10^2 + 9 \cdot 10 + 8.$$

We shorten this expression to $(1998)_{(10)}$ or simply 1998, having the decimal system in mind. In this notation the meaning of a digit depends on its position. Thus two digit symbols "9" are situated in the tens and the hundreds places and their meaning is different. In general for the number N given by (1) we write

$$N = (a_n a_{n-1} \ldots a_1 a_0)_{(10)}$$

to emphasise the exceptional role of 10. This notation is called *positional*. Its invention, attributed to Sumerians or Babylonians and its further development by Hindus, was of enormous significance for civilisation. In Roman symbolism, for example, one wrote

$$\text{MCMXCVIII} = (\text{thousand}) + (\text{nine hundreds}) + (\text{ninety}) +$$
$$(\text{five}) + (\text{one}) + (\text{one}) + (\text{one}),$$

It is clear that more and more new symbols such as I, V, X, C, M are needed as numbers get larger while with the Hindu positional system now in use we need only ten "Arabic numerals" $0, 1, 2, \ldots, 9$, no matter how large is the number. The positional system was introduced into medieval Europe by merchants, who learned it from the Arabs. It is exactly this system which is to blame that the ancient art of computation, once confined to a few adepts, became a routine algorithmic skill that can be done automatically by a machine, and is now taught in elementary school.

2 Other Positional Systems

Mathematically, there is nothing special in the decimal system. The use of ten, as the base, goes back to the dawn of civilisation, and is attributed to the fact that we have ten fingers on which to count. Other number could be used as the base, and undoubtedly some of them were used. The number words in many languages show remnants of other bases, mainly twelve, fifteen and twenty. For example, in English the words for 11 and 12 and in Spanish the words for 11, 12, 13, 14 and 15, are not constructed on the decimal principle. In French a special role of the word for 20 is clearly observed. The Babylonian astronomers had a system of notation with the base 60. This is believed to be the reason for the customary division of the hour and the angular degree into 60 minutes. In the theorem that follows we show that an arbitrary positive integer $b > 1$ can be used as the base.

Theorem 1. *Let $b > 1$ be a positive integer. Then every positive integer N can be uniquely represented in the form*

$$N = d_0 + d_1 b + d_2 b^2 + \cdots + d_n b^n, \tag{2}$$

where "the digits" $d_0, d_1, \ldots, d_n$ lie in the range $0 \le d_i \le b-1$, for all i.

Proof. The proof is by induction on N, the number being represented. Clearly, the representation $1 = 1$ for 1 is unique. Suppose, inductively, that every integer $1, 2, \ldots, N-1$ is uniquely representable. Now consider the integer N. Let $d_0 = N \pmod b$. Then $N - d_0$ is divisible by b and let $N_1 = (N - d_0)/b$. Since $N_1 < N$, by the induction hypothesis N_1 is uniquely representable in the form

$$N_1 = \frac{N - d_0}{b} = d_1 + d_2 b + d_3 b^2 + \cdots + d_n b^{n-1},$$

Then clearly,

$$N = d_0 + N_1 b = d_0 + d_1 b + d_2 b^2 + \cdots + d_n b^n,$$

is the representation required.

Finally, suppose that N has some other representation in this form also, i.e.,

$$N = d_0 + d_1 b + d_2 b^2 + \cdots + d_n b^n = e_0 + e_1 b + e_2 b^2 + \cdots + e_n b^n.$$

Then $d_0 = e_0 = r$ as they are equal to the remainder of N on dividing by b. Now the number

$$N_1 = \frac{N - r}{b} = d_1 + d_2 b + d_3 b^2 + \cdots + d_n b^{n-1} = e_1 + e_2 b + e_3 b^2 + \cdots + e_n b^{n-1}$$

has two different representations which contradicts the inductive assumption, since we have assumed the truth of the result for all $N_1 < N$. □

Corollary 1. *We use the notation*

$$N = (d_n d_{n-1} \ldots d_1 d_0)_{(b)} \tag{3}$$

to express (2). The digits d_i can be found by the repeated application of the division algorithm as follows:

$$\begin{aligned} N &= q_1 b + d_0, && (0 \le d_0 < b) \\ q_1 &= q_2 b + d_1, && (0 \le d_1 < b) \\ &\vdots \\ q_n &= 0 \cdot b + d_n && (0 \le d_n < b) \end{aligned}$$

For example, the positional system with base 5 employ the digits $0, 1, 2, 3, 4$ and we can write

$$1998_{(10)} = 3 \cdot 5^4 + 0 \cdot 5^3 + 4 \cdot 5^2 + 4 \cdot 5 + 3 = 30443_{(5)}.$$

But in the computers' era it is the binary (or dyadic) system (base 2) that emerged as the most important one. We have only two digits here 0 and 1 and a very simple multiplication table for them. But under the binary system, the representations of numbers get longer. For example,

$$86_{(10)} = 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 0 = 1010110_{(2)}. \tag{4}$$

Leibniz (1646–1716) was one of the proponents of the binary system. According to Laplace: "Leibniz saw in his binary arithmetic the image of creation. He imagined that Unity represented God, and zero the void; that the Supreme Being drew all beings from the void, just as unity and zero express all numbers in his system of numeration."

Let us look at the binary representation of a number from the information point of view. Information is measured in bits. One *bit* is a unit of information expressed as a choice between two possibilities 0 and 1. The number of binary digits in the binary representation of a number N is therefore the number of bits we need to transmit N through an information channel (or input into a computer). For example, the equation (4) shows that we need 7 bits to transmit or input the number 86.

Theorem 2. *To input a number N by converting it into its binary representation we need $\lfloor \log_2 N \rfloor + 1$ bits of information, where $\lfloor x \rfloor$ denotes the integer part of x.*

Proof. Suppose that N has n binary digits in its binary representation. That is

$$N = 2^{n-1} + a_{n-2}2^{n-2} + \cdots + a_1 2^1 + a_0 2^0, \qquad a_i \in \{0, 1\}.$$

Then $2^n > N \geq 2^{n-1}$ or $n > log_2 N \geq n - 1$, i.e., $\lfloor \log_2 N \rfloor = n - 1$ and thus $n = \lfloor \log_2 N \rfloor + 1$. □

3 Representations for real numbers

The negative powers of 10 are used to express those real numbers which are not integers. The other bases can be also used. For example,

$$\frac{1}{8} = 0.125_{(10)} = \frac{1}{10} + \frac{2}{10^2} + \frac{5}{10^3} = \frac{0}{2} + \frac{0}{2^2} + \frac{1}{2^3} = 0.001_{(2)}$$

$$\frac{1}{7} = 0.142857142857\ldots_{(10)} = 0.(142857)_{(10)} = 0.001001\ldots_{(2)} = 0.(001)_{(2)}$$

The binary expansions of irrational numbers, such as

$$\sqrt{5} = 10.001111000110111\ldots_{(2)},$$

are used sometimes in cryptography for simulating a random sequence of bits. But this method is considered to be insecure. The number, $\sqrt{5}$ in the example above, can be guessed after knowing the initial segment which will reveal the whole sequence.

Number Theory. Tutorial 5: Bertrand's Postulate

1 Introduction

In this tutorial we are going to prove:

Theorem 1 (Bertrand's Postulate). *For each positive integer $n > 1$ there is a prime p such that $n < p < 2n$.*

This theorem was verified for all numbers less than three million for Joseph Bertrand (1822-1900) and was proved by Pafnutii Chebyshev (1821-1894).

2 The floor function

Definition 1. *Let x be a real number such that $n \leq x < n + 1$. Then we define $\lfloor x \rfloor = n$. This is called the floor function. $\lfloor x \rfloor$ is also called the integer part of x with $x - \lfloor x \rfloor$ being called the fractional part of x. If $m - 1 < x \leq m$, we define $\lceil x \rceil = m$. This is called the ceiling function.*

In this tutorial we will make use of the floor function. Two useful properties are listed in the following propositions.

Proposition 1. $2\lfloor x \rfloor \leq \lfloor 2x \rfloor \leq 2\lfloor x \rfloor + 1$.

Proof. Proving such inequalities is easy (and it resembles problems with the absolute value function). You have to represent x in the form $x = \lfloor x \rfloor + a$, where $0 \leq a < 1$ is the fractional part of x. Then $2x = 2\lfloor x \rfloor + 2a$ and we get two cases: $a < 1/2$ and $a \geq 1/2$. In the first case we have

$$2\lfloor x \rfloor = \lfloor 2x \rfloor < 2\lfloor x \rfloor + 1$$

and in the second

$$2\lfloor x \rfloor < \lfloor 2x \rfloor = 2\lfloor x \rfloor + 1.$$

□

Proposition 2. *let a, b be positive integers and let us divide a by b with remainder*

$$a = qb + r \qquad 0 \leq r < b.$$

Then $q = \lfloor a/b \rfloor$ and $r = a - b\lfloor a/b \rfloor$.

Proof. We simply write

$$\frac{a}{b} = q + \frac{r}{b}$$

and since q is an integer and $0 \leq r/b < 1$ we see that q is the integer part of a/b and r/b is the fractional part. □

Exercise 1. $\lfloor x \rfloor + \lfloor x + 1/2 \rfloor = \lfloor 2x \rfloor$.

3 Prime divisors of factorials and binomial coefficients

We start with the following

Lemma 1. *Let n and b be positive integers. Then the number of integers in the set $\{1, 2, 3, \ldots, n\}$ that are multiples of b is equal to $\lfloor n/b \rfloor$.*

Proof. Indeed, by Proposition 2 the integers that are divisible by b will be $b, 2b, \ldots, \lfloor m/b \rfloor \cdot b$. □

Theorem 2. *Let n and p be positive integers and p be prime. Then the largest exponent s such that $p^s \mid n!$ is*

$$s = \sum_{j \geq 1} \left\lfloor \frac{n}{p^j} \right\rfloor. \tag{1}$$

Proof. Let m_i be the number of multiples of p^i in the set $\{1, 2, 3, \ldots, n\}$. Let

$$t = m_1 + m_2 + \ldots + m_k + \ldots \tag{2}$$

(the sum is finite of course). Suppose that a belongs to $\{1, 2, 3, \ldots, n\}$, and such that $p^j \mid a$ but $p^{j+1} \nmid a$. Then in the sum (2) a will be counted j times and will contribute i towards t. This shows that $t = s$. Now (1) follows from Lemma 1 since $m_j = \lfloor n/p^j \rfloor$. □

Theorem 3. *Let n and p be positive integers and p be prime. Then the largest exponent s such that $p^s \mid \binom{2n}{n}$ is*

$$s = \sum_{j \geq 1} \left(\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \left\lfloor \frac{n}{p^j} \right\rfloor \right). \tag{3}$$

Proof. Follows from Theorem 2. □

Note that, due to Proposition 1, in (3) every summand is either 0 or 1.

Corollary 1. *Let $n \geq 3$ and p be positive integers and p be prime. Let s be the largest exponent such that $p^s \mid \binom{2n}{n}$. Then*

(a) $p^s \leq 2n$.

(b) If $\sqrt{2n} < p$, then $s \leq 1$.

(c) If $2n/3 < p \leq n$, then $s = 0$.

Proof. (a) Let t be the largest integer such that $p^t \leq 2n$. Then for $j > t$

$$\left(\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \left\lfloor \frac{n}{p^j} \right\rfloor \right) = 0.$$

Hence

$$s = \sum_{j=1}^{t} \left(\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \left\lfloor \frac{n}{p^j} \right\rfloor \right) \leq t.$$

since each summand does not exceed 1 by Proposition 1. Hence $p^s \leq 2n$.

(b) If $\sqrt{2n} < p$, then $p^2 > 2n$ and from (a) we know that $s \leq 1$.

(c) If $2n/3 < p \leq n$, then $p^2 > 2n$ and

$$s = \left(\left\lfloor \frac{2n}{p} \right\rfloor - 2 \left\lfloor \frac{n}{p} \right\rfloor \right)$$

As $1 \leq n/p < 3/2$, we se that $s = 2 - 2 \cdot 1 = 0$.

□

4 Two inequalities involving binomial coefficients

We all know the Binomial Theorem:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k. \tag{4}$$

Let us derive some consequences from it. Substituting $a = b = 1$ we get:

$$2^n = \sum_{k=0}^{n} \binom{n}{k}. \tag{5}$$

Lemma 2. *(a) If n is odd, then*

$$\binom{n}{(n+1)/2} \leq 2^{n-1}.$$

(b) If n is even, then

$$\binom{n}{n/2} \geq \frac{2^n}{n}.$$

Proof. (a) From (5), deleting all terms except the two middle ones, we get

$$\binom{n}{(n-1)/2} + \binom{n}{(n+1)/2} \leq 2^n.$$

The two binomial coefficients on the left are equal and we get (a).

(b) If n is even, then it is pretty easy to prove that the middle binomial coefficient is the largest one. In (5) we have $n+1$ summand but we group the two ones together and we get n summands among which the middle binomial coefficient is the largest. Hence

$$n\binom{n}{n/2} \geq \sum_{k=0}^{n} \binom{n}{k} = 2^n,$$

which proves (b).

□

5 Proof of Bertrand's Postulate

Finally we can pay attention to primes.

Theorem 4. *Let $n \geq 2$ be an integer, then*

$$\prod_{p \leq n} p < 4^n,$$

where the product on the left has one factor for each prime $p \leq n$.

Proof. The proof is by induction over n. For $n = 2$ we have $2 < 4^2$, which is true. This provides a basis for the induction. Let us assume that the statement is proved for all integers smaller than n. If n is even, then it is not prime, hence by induction hypothesis

$$\prod_{p \leq n} p = \prod_{p \leq n-1} p < 4^{n-1} < 4^n,$$

so the induction step is trivial in this case. Suppose $n = 2s + 1$ is odd, i.e $s = (n-1)/2$. Since $\prod_{s+1<p\leq n} p$ is a divisor of $\binom{n}{s+1}$, we obtain

$$\prod_{p \leq n} p = \prod_{p \leq s+1} p \cdot \prod_{s+1<p\leq n} p < 4^{s+1} \cdot \binom{n}{s+1} < 4^{s+1} 2^{n-1}$$

using the induction hypothesis for $n = s + 1$ and Lemma 2(a). Now the right-hand-side can be presented as

$$4^{s+1} 2^{n-1} = 2^{2s+2} 2^{n-1} = 2^{4s+2} = 4^{2s+1} = 4^n.$$

This proves the induction step and, hence, the theorem. □

Proof of Bertrand's Postulate. We will assume that there are no primes between n and $2n$ and obtain a contradiction. We will obtain that, under this assumption, the binomial coefficient $\binom{2n}{n}$ is smaller than it should be. Indeed, in this case we have the following prime factorisation for it:

$$\binom{2n}{n} = \prod_{p \leq n} p^{s_p},$$

where s_p is the exponent of the prime p in this factorisation. No primes greater than n can be found in this prime factorisation. In fact, due to Corollary 1(c) we can even write

$$\binom{2n}{n} = \prod_{p \le 2n/3} p^{s_p}.$$

Let us recap now that due to Corollary 1 $p^{s_p} \le 2n$ and that $s_p = 1$ for $p > \sqrt{2n}$. Hence

$$\binom{2n}{n} \le \prod_{p \le \sqrt{2n}} p^{s_p} \cdot \prod_{p \le 2n/3} p.$$

We will estimate now these product using the inequality $p^{s_p} \le 2n$ for the first product and Theorem 4 for the second one. We have no more that $\sqrt{2n}/2 - 1$ factors in the first product (as 1 and even numbers are not primes), hence

$$\binom{2n}{n} < (2n)^{\sqrt{2n}/2-1} \cdot 4^{2n/3}. \tag{6}$$

On the other hand, by Lemma 2(b)

$$\binom{2n}{n} \ge \frac{2^{2n}}{2n} = \frac{4^n}{2n}. \tag{7}$$

Combining (6) and (7) we get

$$4^{n/3} < (2n)^{\sqrt{n/2}}.$$

Applying logs on both sides, we get

$$\frac{2n}{3} \ln 2 < \sqrt{\frac{n}{2}} \ln(2n)$$

or

$$\sqrt{8n} \ln 2 - 3 \ln(2n) < 0. \tag{8}$$

Let us substitute $n = 2^{2k-3}$ for some k. Then we get $2^k \ln 2 - 3(2k-2) \ln 2 < 0$ or $2^k < 3(2k-2)$ which is true only for $k \le 4$ (you can prove that by

inducton). Hence (8) is not true for $n = 2^7 = 128$. Let us consider the function $f(x) = \sqrt{8x}\ln 2 - 3\ln(2x)$ defined for $x > 0$. Its derivative is

$$f(x) = \frac{\sqrt{2x} \cdot \ln 2 - 3}{x}.$$

let us note that for $x \geq 8$ this derivative is positive. Thus (8) is not true for all $n \geq 128$. We proved Bertrand's postulate for $n \geq 128$. For smaller n it can be proved by inspection. I leave this to the reader. □

Geometry Tutorial 1.
Ptolemy's inequality

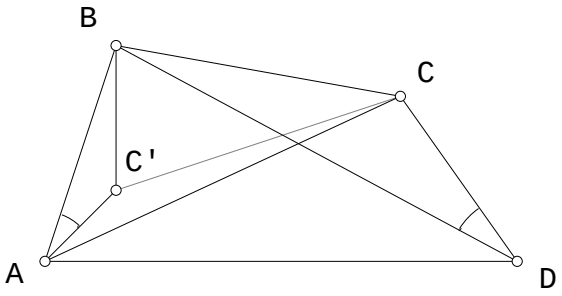
One of the most important tools in proving geometric inequalities is

Theorem 1 (Ptolemy's Inequality) *Let $ABCD$ be an arbitrary quadrilateral in the plane. Then*

$$AB \cdot CD + BC \cdot AD \geq AC \cdot BD.$$

This inequality becomes equality if and only if the quadrilateral is cyclic.

Proof: Firstly, we will consider the case, when the quadrilateral $ABCD$ is convex. Let us rotate the plane about B and then dilate, choosing the coefficient of the dilation k so that the image of D coincides with A. Let us denote the image of C as C'.



Since the triangles ABC' and DBC are similar we get $\frac{AB}{AC'} = \frac{BD}{CD}$ and hence

$$AC' = \frac{AB \cdot CD}{BD}.$$

The triangles $C'BC$ and ABD are also similar because $\angle C'BC = \angle ABD$ and

$$\frac{C'B}{BC} = \frac{AB}{BD} = k.$$

This similarity yields $\dfrac{BC}{C'C} = \dfrac{BD}{AD}$, whence

$$C'C = \frac{BC \cdot AD}{BD}.$$

By the Triangle inequality

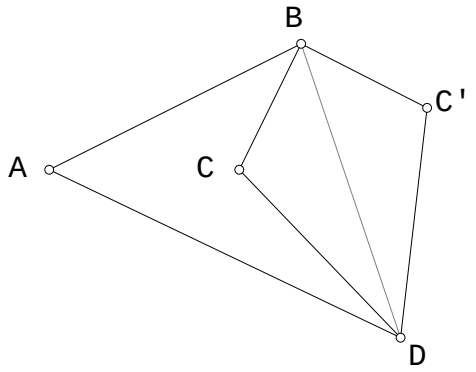
$$AC' + C'C = \frac{AB \cdot CD}{BD} + \frac{BC \cdot AD}{BD} \geq AC,$$

and therefore $AB \cdot CD + BC \cdot AD \geq AC \cdot BD$. This inequality is an equality if and only if C' is on the segment AC in which case we have

$$\angle BAC = \angle BAC' = \angle BDC$$

and the points A, B, C, D are concyclic.

Let us assume now that the quadrilateral is not convex. Then one of its diagonals, say BD does not have common points with the interior of the quadrilateral.



Reflecting C about BD we will get a convex quadrilateral $ABC'D$ whose side are of the same lengths as that of $ABCD$ but the product of the diagonals for $ABCD$ is smaller than for $ABC'D$ as $AC < AC'$ and BD is the same in both cases. Therefore Ptolemy's inequality holds in this case too, and inequality never becomes equality.

Another proof of Ptolemy's inequality can be obtained using inversion. We will prove even more general statement.

Theorem 2 (Generalised Ptolemy's inequality) *Let A, B, C, D be arbitrary points in the plane, but not on a line. Then*

$$AB \cdot CD + BC \cdot AD \geq AC \cdot BD.$$

This inequality becomes equality if and only if the points A, B, C, D are concyclic and each of the two arcs determined by the points A, C contains one of the two remaining points.

Proof: Consider an inversion i with pole D and any coefficient $r > 0$. Let A', B', C' be the images of A, B, C under this inversion respectively. Applying the Triangle inequality for the points A', B', C', we get

$$A'B' + B'C' \geq A'C'. \tag{1}$$

It is well-known (or easy to prove) how distances between points change under inversion. In our case, if X, Y are any two points different from D, and if X', Y' are their images under i then

$$X'Y' = \frac{r^2 \cdot XY}{DX \cdot DY}.$$

This formula can be applied to any pair of points A, B, C because they are all different from D. So we rewrite (1) in the form

$$\frac{r^2 \cdot AB}{DA \cdot DB} + \frac{r^2 \cdot BC}{DB \cdot DC} \geq \frac{r^2 \cdot AC}{DA \cdot DC}.$$

After multiplying both sides by $DA \cdot DB \cdot DC$, the latter becomes

$$AB \cdot CD + BC \cdot AD \geq AC \cdot BD, \tag{2}$$

as desired. It is clear that (2) becomes equality, only when (1) becomes equality. This happens, when A', B', C' are on the line with B' beeing between A' and C'. Since the points are not on the same line, this means that before the inversion they were on a circle with B and D on different arcs determined by A and C.

Comment 1: Theorem 2 is clearly independent of whether or not the given points lie in the same plane. It does not change in the slightest if they are in three-dimensional space.
Comment 2: Theorem 2 is also true in some cases, when the given points lie on the same line. This case can easily be sorted out but it is not of interest to us.

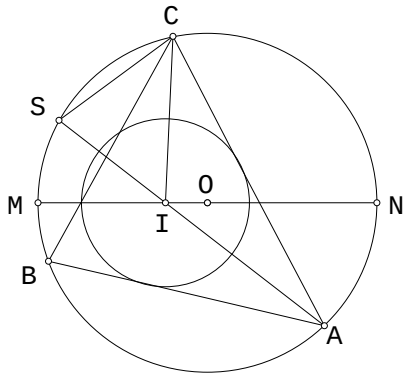
Geometry Tutorial 2.
Euler's theorem

We shall prove in this section Euler's theorem that was offered in 1962 to the participants of IMO and therefore introduced to the IMO sillabus forever.

We will prove the following lemma first and then derive Euler's theorem and several other corollaries.

Lemma 1 *A circle of radus r with center I is inside of a circle of radius R with center O. Suppose A is an arbitrary point on the larger circle, AB and AC are two chords of the larger circle which are tangent to the smaller one. Then BC is tangent to the smaller circle if and only if $IO = \sqrt{R(R-2r)}$.*

Proof. Let S be a point on the larger circle such that AS is the bisector of $\angle BAC$. Let us draw CI and CS.



BC is tangent to the smaller circle if and only if $\angle BCI = \angle ICA$. This, in turn, happens if and only if $\angle SCI = \angle CIS$, since $\angle CIS = \angle ICA + \angle IAC = \angle ICA + \angle SCB$. Furthermore, $\angle SCI = \angle CIS$ if and only if $SC = SI$.

Let MN be the diameter of the large circle passing through I and O. Then $SC = SI$ if and only if $SI \cdot IA = SC \cdot IA = 2R \sin\alpha \cdot \dfrac{r}{\sin\alpha} = 2rR$, where $\alpha = \angle CAS$.

As is well-known, $SI \cdot IA = MI \cdot IN = (R-d)(R+d)$, where $d = IO$. Hence we have $SI \cdot IA = 2rR$ if and only if $(R-d)(R+d) = 2rR$, which is the same as $d^2 = R^2 - 2rR$, and the lemma is proved. ■

From this lemma Euler's theorem follows:

Theorem 2 (Euler's theorem) *The distance between the incenter and the circumcenter of a triangle is equal to* $\sqrt{R(R-2r)}$.

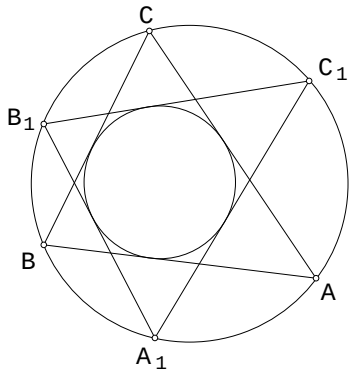
Two more remarkable corollaries from the same lemma:

Corollary 3 *Two positive real numbers* r *and* R *are the inradius and circumradius of some triangle* ABC *if and only if* $R \geq 2r$. *Moreover,*

$R = 2r$ *if and only if the triangle* ABC *is equilateral.*

If $R > 2r$ *there exist infinitely many nonsimilar triangles having* R *and* r *as the circumradius and inradius, respectively.*

Corollary 4 *Consider the incircle and the circumcircle of triangle* ABC. *Let us take an arbitrary point* A_1 *on the circumcircle and draw the chords* A_1B_1 *and* B_1C_1 *both of which are tangent to the incircle. Then the chord* C_1A_1 *is also tangent to the incircle.*



This is a partial case of the deep Poncelet's theorem.

Theorem 5 (Poncelet) *Suppose that one circle is placed inside another circle. Let* $A_1, \ldots, A_n$ *be the points on a larger circle such that each link of the closed broken line* $A_1A_2 \ldots A_nA_1$ *touches the smaller circle. Then if* $B_1, \ldots, B_n$ *be any points on the larger circle such that each link of the broken line* $B_1B_2 \ldots B_n$ *touches the smaller circle, then* B_nB_1 *also touches it.*

Enriching Mathematics Learning

AUSTRALIAN MATHEMATICS TRUST

+ home
+ what's new
+ events
+ for parents
+ book shop
+ people
+ activity
+ links
+ about us
+ contact us

What's New

Recent Postings

- AMC scoring changes from 2007
- BH Neumann Award winners announced for 2007
- AIO 2006 Results
- Eligibility and attendance at AMOC training schools
- Buying photos at AMC Presentations 2006
- Dates for key AMT events in 2007
- AIMO and AMOC Senior Contest 2006 Results
- AMC 2006 medallists announced
- Fields Medal for Medal for Terry Tao
- Cheryl Praeger appointed to International Committee for Mathematics
- IOI Results 2006 from Merida, Yucatan, Mexico, inc Gold and Silver Medals.
- IMO Results 2006 from Ljubljana including transcript of interview of Silver Medal winner Graham White by Adam Spencer on Sydney ABC Breakfast immediately after the Closing Ceremony.
- AIC Results 2006
- APMO 2006 Results (official)
- Announcement of 2006 Olympiad Teams
- Informatics, 2006 FARIO Results
- AMO 2006 Results
- AIIO 2006 Results

Archived Postings

2006: the 29th Australian Mathematics Competition for the Westpac Awards

- The 2007 AMC has been set for Wednesday 25 July. It is now very difficult to find a date which is clear in each state. Basic skills tests are scheduled for different dates around Australia and in some states there are end of year exam trials through early August. Please email us your view.
- 2006 medallists announced
- AMC innovations during 2004, 2005 and 2006, including scan of mark sense sheet, showing how students answer questions 26 to 30.

- AMC 2006 fact sheet
- See our Activity page (button at left) to try some warm-up exercises for Australian Mathematics Competition for the Westpac Awards
- In 2003 the Australian Mathematics Competition for the Westpac Awards celebrated its 25th Anniversary

Dates

- Key dates (where determined)

Australian Mathematical Olympiad Program

- AIMO and Senior Contest 2006 Results
- IMO Results 2006 from Ljubljana including transcript of interview of Silver Medal winner Graham White by Adam Spencer on Sydney ABC Breakfast immediately after the Closing Ceremony.
- APMO 2006 Results
- AMO 2006 Results

Informatics

- AIO Results 2006
- IOI Results 2006 from Merida, Yucatan, Mexico, inc Gold and Silver Medals.
- AIC Results 2006
- 2006 FARIO Results
- AIIO 2006 Results

ICMI Study on Challenging Mathematics

Official Web Site of the Study.

Seven Bridges of Königsberg

- What *Ever* Happened to Those Bridges? by Peter Taylor

International Mathematics Tournament of Towns

- Diploma Winners: Australia and New Zealand
- Recent Results: International

Enriching Mathematics Learning

AUSTRALIAN MATHEMATICS TRUST

- what's new
- events
- for parents
- book shop
- people
- activity
- links
- about us
- contact us
- privacy policy

AMC Scoring Changes
From 2007 a different point system will be used for the last five questions of the Australian Mathematics Competition for the Westpac Awards. more...

AIO 2006 Results
A total of 45 students wrote the Senior version and 32 students wrote the Intermediate version of the second Australian Informatics Olympiad. more...

Three BH Neumann Awards announced for 2007
The Australian Mathematics Trust has announced that three mathematics educators will receive BH Neumann Awards in 2007. These awards are given for service to the enrichment of mathematics learning in Australia. more...

Australian Informatics Competition 2007
Competition Day Thursday 10 May | Registration closes Friday 30 March

Enriching Mathematics Learning

AUSTRALIAN MATHEMATICS TRUST

+ home
+ what's new
+ events
+ for parents
+ book shop
+ people
+ activity
+ links
+ about us
+ contact us

Book Shop

News

- Australian Mathematics Competition for the Westpac Awards Book 4 (1999-2005) is now available.
- Strongly recommended for Primary students and teachers: *Problems for the Middle School*. (see catalogue)
- In addition to the books to be found in our catalogue we also recommend the publications of our sister organisation the United Kingdom Mathematics Trust, whose publications can be found here.

Enter Catalogue and Shop

or, alternatively (for purchase via post or fax)

Download catalogue and order form

Australian Mathematics Trust

PUBLICATIONS

COMPETITION MATERIALS

BUNDLES OF PAST AMC PAPERS

Bundles of past Australian Mathematics Competition papers are available for practice. Each bundle contains five different papers and an answer key. Bundles are available for Junior, Intermediate or Senior levels. Bundles are also available in sets of ten identical papers in each division of the Competition. Schools find these sets extremely valuable in setting their students miscellaneous exercises.

AMC SOLUTIONS AND STATISTICS

WJ ATKINS & PJ TAYLOR

This book provides, each year, a record of the AMC questions, answers and solutions, with details of medallists and prize winners. It also provides statistical data on levels of Australian response rates and other analytical information. From 2004 there is also a Primary version providing questions, answers, solutions and statistics for the Middle and Upper Primary papers.

AUSTRALIAN MATHEMATICS COMPETITION BOOK 1 1978–1984

J EDWARDS, D KING & PJ O'HALLORAN

This 258 page book consists of over 500 questions, full solutions and statistics from the AMC papers of 1978-84. The questions have been grouped by topic and ranked in order of difficulty. The book is a powerful tool for motivating and challenging students of all levels.

AUSTRALIAN MATHEMATICS COMPETITION BOOK 2 1985–1991

PJ O'HALLORAN, G POLLARD & PJ TAYLOR

Over 250 pages of challenging questions and solutions from Australian Mathematics Competition papers from 1985-1991.

AUSTRALIAN MATHEMATICS COMPETITION BOOK 3 1992–1998

WJ ATKINS, JE MUNRO & PJ TAYLOR

Over 290 pages of challenging questions and solutions from Australian Mathematics Competition papers from 1992-1998.

AUSTRALIAN MATHEMATICS COMPETITION BOOK 3 ON CD

PROGRAMMED BY E STOROZHEV

This CD contains the same problems and solutions as the corresponding book. The problems can be accessed by topics as in the book and in this mode, the CD is ideal to help students practice particular skills. In another mode students can simulate writing the actual papers and determine the score that they would have gained. The CD runs on all Windows platforms.

MATHEMATICAL CONTESTS—AUSTRALIAN SCENE

AM STOROZHEV, JB HENRY & A DI PASQUALE

These books provide an annual record of the Australian Mathematical Olympiad Committee's program. The books consist of the questions, solutions, results and statistics for: Australian Intermediate Mathematics Olympiad (formerly AMOC Intermediate Contest), AMOC Senior Mathematics Contest, Australian Mathematics Olympiad, Asian Pacific Mathematics Olympiad, International Mathematical Olympiad, and Maths Challenge Stage of the Mathematical Challenge for Young Australians.

CHALLENGE! 1991–1995

JB HENRY, J DOWSEY, A EDWARDS, L MOTTERSHEAD, A NAKOS & G VARDARO

The Mathematics Challenge for Young Australians attracts thousands of entries from Australian Schools annually. Each year it involves solving in-depth problems over a three week period. In 1991-95 there were two versions, a Junior version for Year 7 and 8 students and an Intermediate version for Year 9 and 10 students. This book reproduces the problems which have been set over the first 6 years of the event, together with solutions and extension questions. It is a valuable resource book for the classroom and the talented student.

PROBLEMS TO SOLVE IN MIDDLE SCHOOL MATHEMATICS

B HENRY, L MOTTERSHEAD, A EDWARDS, J MCINTOSH, A NAKOS, K SIMS, A THOMAS & G VARDARO.

This collection of problems is designed for use with students in Years 5 to 8. Each of the 65 problems is presented ready to be photocopied for classroom use. With each problem there are teacher's notes and fully worked solutions. Some problems have extension problems presented with the teacher's notes. The problems are arranged in topics (Number, Counting, Space and Number, Space, Measurement, Time, Logic) and are roughly in order of difficulty within each topic. There is a chart suggesting which problem-solving strategies could be used with each problem.

AUSTRALIAN MATHEMATICAL OLYMPIADS 1979–1995

H LAUSCH & PJ TAYLOR

This book is a collection of Australian Mathematical Olympiad papers from the first in 1979 to 1995. The solutions to all problems are included and in a number of cases alternative solutions are also offered. The material is recommended for senior and advanced students.

EXTENSION MATERIALS

ENRICHMENT STUDENT NOTES

The Student Notes are supplied to students enrolled in the program along with other materials provided to their teacher. We are making these Notes available as a text book to interested parties for whom the program is not available. These six stages offer extension material for students from year 5 to year 10, in that order.

NEWTON: Recommended for students of about Year 5 and 6, topics include polyominoes, arithmetricks, polyhedra, patterns and divisibility.

DIRICHLET: This book has chapters on some problem solving techniques, tessellations, base five arithmetic, pattern seeking, rates and number theory. It is designed for students in Year 6 or 7.

EULER: Recommended for students of about Year 7, topics include elementary number theory and geometry, counting and pigeonhole principle.

GAUSS: Recommended for students of about Year 8, topics include Pythagoras' theorem, Diaphantine equations, counting and congruences.

NOETHER: Recommended for students of about Year 9, topics include number theory, sequences, inequalities and circle geometry.

PÓLYA: Recommended for students of about Year 10, topics include polynomials, algebra, inequalities and geometry.

SEEKING SOLUTIONS

JC BURNS

Professor John Burns, formerly Professor of Mathematics at the Royal Military College, Duntroon and Foundation Member of the Australian Mathematical Olympiad Committee, solves the problems of the 1988, 1989 and 1990 International Mathematical Olympiads. Unlike other books in which only complete solutions are given, John Burns describes the complete thought processes he went through when solving the problems from scratch. Written in an inimitable and sensitive style, this book is a must for a student planning on developing the ability to solve advanced mathematics problems.

PROBLEM SOLVING VIA THE AMC

WARREN ATKINS

This 210 page book shows how to develop techniques for solving problems in the Australian Mathematics Competition. These problems have been selected from topics such as Geometry, Motion, Diophantine Equations and Counting Techniques–areas that students consistently find difficult.

MATHEMATICAL TOOLCHEST

AW PLANK & N WILLIAMS

This 120 page book is intended for talented or interested secondary school students who are keen to develop their mathematical knowledge. It contains a comprehensive collection of theorems and other results from many branches of mathematics.

METHODS OF PROBLEM SOLVING, BOOKS 1 & 2

JB TABOV & PJ TAYLOR

These books introduce senior students aspiring to Olympiad competition to particular mathematical problem solving techniques. The books contain formal treatments of methods which may be familiar or may introduce the student to new, sometimes powerful techniques.

INTERNATIONAL MATHEMATICS

USSR MATHEMATICAL OLYMPIADS 1989–1992

AM SLINKO

Arkadii Slinko, now at the University of Auckland, was one of the leading figures of the USSR Mathematical Olympiad Committee during the last years before democratisation. This book brings together the problems and solutions of the last four years of the All-Union Mathematics Olympiads. Not only are the problems and solutions highly expository but the book is worth reading alone for the fascinating history of mathematics competitions to be found in the introduction.

INTERNATIONAL MATHEMATICS–TOURNAMENT OF TOWNS 1980-1984, 1984-1989, 1989-1993, 1993-1997

PJ TAYLOR

The International Mathematics Tournament of Towns is a problem solving competition in which teams from different cities are handicapped according to the population of the city. Ranking only behind the International Mathematical Olympiad, this competition had its origins in Eastern Europe (as did the Olympiad) but is now open to cities throughout the world. These books of 115, 180, 200 and 180 pages respectively, contain all the problems and solutions of the Tournaments.

POLISH & AUSTRIAN MATHEMATICAL OLYMPIADS 1981-1995

ME KUCZMA & E WINDISCHBACHER

Poland and Austria hold some of the strongest traditions of Mathematical Olympiads in Europe even holding a joint Olympiad of high quality. This book contains some of the best problems from the national Olympiads. All problems have two or more independent solutions, indicating their richness as mathematical problems.

CHINESE MATHEMATICS COMPETITIONS & OLYMPIADS BOOK 1 1981-1993 & BOOK 2 1993-2001

A LIU

These books contain the papers of two contests, the Chinese National High School Competition and the Chinese Mathematical Olympiad. The problems are meticulously constructed, many with distinctive flavour and come in all levels of difficulty, from the relatively basic to the most challenging.

ASIAN PACIFIC MATHEMATICS OLYMPIADS 1989-2000

H LAUSCH & C BOSCH-GIRAL

With innovative regulations and procedures, the APMO has become a model for regional competitions around the world where costs and logistics are serious considerations. This 159 page book reports the first twelve years of this competition, including sections on its early history, problems, solutions and statistics.

101 PROBLEMS IN ALGEBRA

EDITED BY T ANDREESCU & Z FENG

This book contains one hundred and one highly rated problems used in training and testing the USA International Mathematical Olympiad (IMO) team. It gradually builds students algebraic skills and techniques and aims to broaden students' views of mathematics and better prepare them for possible participation in mathematical competitions. It provides in-depth enrichment in important areas of algebra by reorganizing and enhancing students' problem-solving tactics, and stimulates interest for future study of mathematics.

HUNGARY ISRAEL MATHEMATICS COMPETITION

S GUERON

The Hungary Israel Mathematics Competition commenced in 1990 when diplomatic relations between the two countries were in their infancy. This 181 page book summarizes the first 12 years of the competition (1990 to 2001) and includes the problems and complete solutions. The book is directed at mathematics lovers, problem solving enthusiasts and students who wish to improve their competition skills. No special or advanced knowledge is required beyond that of the typical IMO contestant and the book includes a glossary explaining the terms and theorems which are not standard that have been used in the book.

BULGARIAN MATHEMATICS COMPETITION 1992-2001

BJ LAZAROV, JB TABOV, PJ TAYLOR & A STOROZHEV

The Bulgarian Mathematics Competition has become one of the most difficult and interesting competitions in the world. It is unique in structure combining mathematics and informatics problems in a multi-choice format. This book covers the first ten years of the competition complete with answers and solutions. Students of average ability and with an interest in the subject should be able to access this book and find a challenge.

JOURNALS

MATHEMATICS COMPETITIONS

This bi-annual journal is published on behalf of the World Federation of National Mathematics Competitions. It contains articles of interest to academics and teachers around the world who run mathematics competitions, including articles on actual competitions, results from competitions, and mathematical and historical articles which may be of interest to those associated with competitions.

PARABOLA incorporating FUNCTION

In 2005 Parabola will become *Parabola incorporating Function* edited by Bruce Henry at the University of New South Wales. This tri-annual journal publishes articles on applied mathematics, mathematical modelling, statistics, pure mathematics and the history of mathematics, that can contribute to the teaching and learning of mathematics at the senior secondary school level. The journal's readership consists of mathematics students, teachers and researchers with interests in promoting excellence in senior secondary school mathematics education.

T-SHIRTS

T-SHIRT SIZES XL & MEDIUM (POLYA ONLY)

The t-shirts in this series are based on different mathematicians and one informatician depicting an outstanding area of their work in a brightly coloured cartoon representation. They are Leonhard Euler's famous Seven Bridges of Königsberg question, Carl Friedrich Gauss' discovery of the construction of a 17-gon by straight edge and compass, Emmy Noether's work on algebraic structures, George Pólya's Necklace Theorem, Peter Gustav Lejeune Dirichlet's Pigeonhole Principle and Alan Mathison Turing's computing machine. The t-shirts are made of 100% cotton and are designed and printed in Australia.

Publication Order Form

To order any of the listed items, complete the Publications Order Form below and return by email, fax or mail to:
Australian Mathematics Trust, University of Canberra ACT 2601, AUSTRALIA

Ph: (02) 6201 5137
Fax: (02) 6201 5052
] from within Australia

Ph: +61 (2) 6201 5137
Fax: +61 (2) 6201 5052
] from outside Australia

Email: publications@amt.edu.au Web: www.amt.edu.au/amtpub.html

BOOK TITLE	QTY	UNIT PRICE	TOTAL
COMPETITION MATERIALS			
BUNDLES OF PAST AMC PAPERS (write quantity in box) 10 identical papers per bundle with answer key for school use		$A13.50 PER BUNDLE	

	2000	2001	2002	2003	2004	2005
MIDDLE PRIMARY						
UPPER PRIMARY						
JUNIOR						
INTERMEDIATE						
SENIOR						

PAST PAPERS (for home use) Junior (years 7 & 8) – Bundle contains one each of: 2001, 2002, 2003, 2004, 2005 past papers with answer key		$A21.00 PER BUNDLE	
Intermediate (years 9 & 10) – Bundle contains one each of: 2001, 2002, 2003, 2004, 2005 past papers with answer key		$A21.00 PER BUNDLE	
Senior (years 11 & 12) – Bundle contains one each of: 2001, 2002, 2003, 2004, 2005 past papers with answer key		$A21.00 PER BUNDLE	
AMC SOLUTIONS & STATISTICS (Junior, Intermediate and Senior Divisions) 2005		$A35.00	
Editions from previous years are available (1992-2004) (write in box which year/s you wish to order)		$A28.50	
AMC SOLUTIONS & STATISTICS (Middle & Upper Primary Divisions) 2005		$A35.00	
No other previous editions are available 2004		$A28.50	
AUSTRALIAN MATHEMATICS COMPETITION BK 1		$A40.00	
AUSTRALIAN MATHEMATICS COMPETITION BK 2		$A40.00	
AUSTRALIAN MATHEMATICS COMPETITION BK 3		$A40.00	
AUSTRALIAN MATHEMATICS COMPETITION BK 3 - CD		$A40.00	
MATHEMATICAL CONTESTS – AUSTRALIAN SCENE 2005*		$A35.00	
Editions from previous years are available (1992-2004) (write in box which year/s you wish to order)		$A28.50	
CHALLENGE! 1991–1995		$A40.00	
PROBLEMS TO SOLVE IN MIDDLE SCHOOL MATHEMATICS		$A50.00	
AUSTRALIAN MATHEMATICAL OLYMPIADS 1979–1995		$A40.00	
EXTENSION MATERIALS			
ENRICHMENT STUDENT NOTES (write quantity in box)		$A40.00	

NEWTON	DIRICHLET	EULER	GAUSS	NOETHER	POLYA

SEEKING SOLUTIONS		$A40.00	
PROBLEM SOLVING VIA THE AMC		$A40.00	
MATHEMATICAL TOOLCHEST		$A40.00	
METHODS OF PROBLEM SOLVING, BOOK 1		$A40.00	
METHODS OF PROBLEM SOLVING, BOOK 2		$A40.00	

Prices valid to 31 Dec 2006. Please allow 14 days for delivery.

continued over

BOOK TITLE	QTY	UNIT PRICE	TOTAL
INTERNATIONAL MATHEMATICS			
USSR MATHEMATICAL OLYMPIADS 1989–1992		$A40.00	
TOURNAMENT OF TOWNS (indicate quantity in box) 1980-1984 / 1984-1989 / 1989-1993 / 1993-1997		$A40.00	
POLISH & AUSTRIAN MATHEMATICAL OLYMPIADS 1981-1995		$A40.00	
ASIAN PACIFIC MATHEMATICS OLYMPIADS 1989-2000		$A40.00	
CHINESE MATHEMATICS COMPETITIONS & OLYMPIADS BOOK 1 1981-1993		$A40.00	
CHINESE MATHEMATICS COMPETITIONS & OLYMPIADS BOOK 2 1993-2001		$A40.00	
101 PROBLEMS IN ALGEBRA		$A40.00	
HUNGARY ISRAEL MATHEMATICS COMPETITION		$A40.00	
BULGARIAN MATHEMATICS COMPETITION 1992-2001		$A40.00	
JOURNALS			
MATHEMATICS COMPETITIONS – WORLD FEDERATION JOURNAL 2005 Subscription – (2 issues annually in July & Dec)		$A68.00	
PARABOLA inc FUNCTION – 2005 Subscription (3 issues annually from Jan–Dec)		$A28.00	
T-SHIRTS			
(indicate quantity in box) DIRICHLET XL / EULER XL / GAUSS XL / NOETHER XL POLYA MED / POLYA XL / TURING XL		$A25.30 EACH	
Overseas Postage–for postage and handling outside Australia add $A13.00 for first book then add $A5.00 for each additional book.			$A
		TOTAL	$A

* Not available till March 2006

Prices valid to 31 Dec 2006. Please allow 14 days for delivery.

METHOD OF PAYMENT ABN: 39 120 172 502

☐ CHEQUE ☐ BANKDRAFT ☐ AUSTRALIAN BANKCARD
☐ VISA ☐ MASTERCARD ☐ AMERICAN EXPRESS

SCHOOL PURCHASE ORDER NUMBER:

Total Amount: $A Tel (bh):

IF PAYING BY AUSTRALIAN BANKCARD, VISA, MASTERCARD OR AMERICAN EXPRESS COMPLETE THE FOLLOWING:

Card Number: ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ Card Expiry Date:

Cardholder's Name:
(as shown on card)

Cardholder's Signature: Date:

ALL PAYMENTS (CHEQUES/BANKDRAFTS) SHOULD BE IN AUSTRALIAN CURRENCY, MADE PAYABLE TO AUSTRALIAN MATHEMATICS TRUST AND SENT TO:
Australian Mathematics Trust, University of Canberra ACT 2601, AUSTRALIA

PLEASE ALLOW 14 DAYS FOR DELIVERY. THE AMT REGRETS THAT NON-SCHOOL ORDERS CANNOT BE ACCEPTED WITHOUT PAYMENT.

PLEASE FORWARD PUBLICATIONS TO:

NAME

ADDRESS

SUBURB POSTCODE COUNTRY

Enriching Mathematics Learning

AUSTRALIAN MATHEMATICS TRUST

+ home
+ what's new
+ events
+ for parents
+ book shop
+ people
+ activity
+ links
+ about us
+ contact us

Activity

This page is designed give students a wide range of opportunities to practice their mathematics and informatics, and teachers warm-up papers and other problems to give their class. Problems to be found here will cover a wide range of standards, from accessible to all students up to challenging.

When a question is posted without solution, if you are from a participating school and within the valid school year, send your solutions here, making it clear which problems you are answering. If your solution is complete we will acknowledge with your name, school and school year. Generally when a sufficient number of correct solutions are in we will post the complete solutions, and follow with new problems.

For informatics a separate method of interactive assessment is provided.

- **Australian Mathematics Competition for the Westpac Awards**
- **Mathematics Challenge for Young Australians**
- **International Mathematics Tournament of Towns**
- **Informatics**

What's New !!!
Events
Information for Parents
Book Shop
People
Activity
Links
Email Us
About the Trust
Home

AUSTRALIAN MATHEMATICS TRUST

Mathematics Activity

Mathematics Challenge for Young Australians

This page will be developed to give students a wide range of opportunities to practice their mathematics, and teachers warm-up papers and other problems to give their class. Problems to be found here will cover a wide range of standards, from accessible to all students up to challenging.

When a question is posted without solution, if you are from a participating school and within the valid school year, send your solutions here, making it clear which problems you are answering. If your solution is complete we will acknowledge with your name, school and school year. Generally when a sufficient number of correct solutions are in we will post the complete solutions, and follow with new problems.

The problems below will require syllabus skills from the relevant year, and are for students who enjoy mathematics and wish to test their problem solving skills.

Current Warm-up problems

- **Primary, Years 5, 6 and 7**
  Problem 2
  Correct Solution was received from
  - Sheree Deng, Year 5, Essex Heights Primary School, Mt Waverley, Victoria
  - Gabriel Gregory, Year 5, Sydney Grammar School, St Ives, NSW
  - Siddharth Jain, Year 7, Box Hill High School, Box Hill, Victoria
  - Cameron Segal, Year 4, The King David School, Armadale, Victoria
  - Abdullah Sarker, Year 7, Sydney Boys High School, Surry Hills, NSW

  Solution to Problem 1
  Correct Solution was received from
  - Kate Charters, Year 7, St. Catherine's School, Victoria
  - Rowan Clymo-Rowlands Year 5, Lenah Valley Primary School, Tasmania
  - Sebhatleb Gebrezgabir, Year 6, Campbell Street Primary School, Tasmania
  - Gabriella Hannah Kontorovich, Year 5, The Emanuel School, Sydney, NSW
  - Matthew O'Brien, Year 5, Kennington Primary School, Bendigo, Victoria
  - Mengtong Xia, Year 5, Balwyn Primary School, Victoria
- **Junior, Years 7 and 8**
  Problem 2

  Correct Solution was received from
  - Brian Fernandes,Year 8, Hurlstone Agricultural High School, NSW
  - Gabriel Gregory, Year 5, Sydney Grammar School St Ives, NSW

Solution to Problem 1

Correct Solution was received from

- Varun Nayyar, Year 8 Trinity Grammar School NSW (2004)

- **Intermediate, Years 9 and 10**
  Problem 2

  Solution to Problem 1

  Correct Solution was received from
  - Giles Gardam, Year 9, Hurlstone Agricultural High School, NSW
  - Vinayak Hutchinson, Year 9, Shenton College, WA
  - Sarah Liu, Year 10, Arthur Phillip High School, NSW
  - Andrew Watts, Year 9, Hurlstone Agricultural High School, NSW

MATHEMATICS CHALLENGE FOR YOUNG AUSTRALIANS

PRIMARY, YEARS 5, 6 and 7

WARM UP PROBLEM 02

Wildlife Park

The local wildlife park has an area where there are three types of native animals — bandiccots, bettongs and quolls — for visitors to see on torch-light tours.

The Park Rangers keep records of the numbers of each type of animal. At the end of both the first and second years, there were three times as many bettongs as quolls and half the total animal population was bandicoots.

1. If there were three quolls at the end of the first year, what was the total animal population?

2. If the total population at the end of the second year was 40, how many bandicoots, bettongs and quolls were there?

At the end of the third year, the total animal population had grown to 55. There were still three times as many bettongs as quolls and more than half the total population was bandicoots.

3. The Chief Ranger thought he had counted eight quolls. Explain why this was a mistake.

4. What is the largest possible number of quolls in the area at the end of the third year?

MATHEMATICS CHALLENGE FOR YOUNG AUSTRALIANS

JUNIOR, YEARS 7 and 8

WARM UP PROBLEM 02

The Price is Perfect

On the TV show 'The Price is Perfect', Chloe will win all the prizes if she can work out the mystery number. Joe, the host of the show, says:

'To-night's mystery number is the **largest** 7-digit number which has these properties:

(a) no two digits in the number are the same;

(b) each of the number's digits divide into the number exactly.'

1. Find the three digits which cannot be in the mystery number.

Explain why they must be excluded.

2. Find the mystery number.

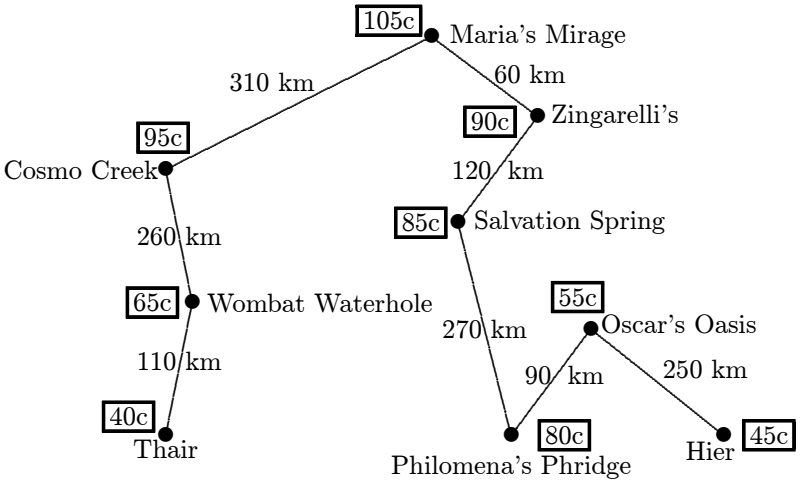
Explain why it is the largest 7-digit number which has these two properties.

MATHEMATICS CHALLENGE FOR YOUNG AUSTRALIANS

INTERMEDIATE, YEARS 9 and 10

WARM UP PROBLEM 02

Cornelius the Camel



Gianna rides her camel Cornelius across the Gibson Desert from Hier to Thair, stopping occasionally to recharge Cornelius with water. Cornelius holds 50 litres and can travel 100 km on 10 litres. The water sellers at the oases between Hier and Thair charge varying amounts per litre of water, as shown on the map. Gianna stops as infrequently as possible on her journey as it is difficult to get Cornelius going after a stop. She fills Cornelius with 50 litres of water at Hier and starts her journey.

When she does stop, including the beginning of the journey at Hier and the end of the journey at Thair, she always lets Cornelius fill up with water *completely*.

1. What is the minimum number of times Gianna must stop for water for Cornelius? Give reasons for your answer.
2. Gianna crosses the Gibson Desert with a minimum number of stops. At which oases should she stop to spend as little as possible on water for Cornelius? How much does this cost her?

3. Suppose that Gianna allows for more than the minimum number of stops (including Hier and Thair), still letting Cornelius fill up completely at each stop. What is the cheapest way to get across the desert?

What's New !!!
Events
Information for Parents
Book Shop
People
Activity
Links
Email Us
About the Trust
Home

AUSTRALIAN MATHEMATICS TRUST

Mathematics Activity

International Mathematics Tournament of Towns

This page will be developed to give students a wide range of opportunities to practice their mathematics, and teachers warm-up papers and other problems to give their class. Problems to be found here will cover a wide range of standards, from accessible to all students up to challenging.

When a question is posted without solution, if you are from a participating school and within the valid school year, send your solutions here, making it clear which problems you are answering. If your solution is complete we will acknowledge with your name, school and school year. Generally when a sufficient number of correct solutions are in we will post the complete solutions, and follow with new problems.

These Tournament questions can be extremely challenging.

Problem 1.

INTERNATIONAL MATHEMATICS TOURNAMENT OF TOWNS

PRACTICE QUESTION 1

The least common multiple of positive integers a, b, c and d is equal to $a + b + c + d$. Prove that $abcd$ is divisible by at least one of 3 and 5.

What's New !!!
Events
Information for Parents
Book Shop
People
Activity
Links
Email Us
About the Trust
Home

AUSTRALIAN MATHEMATICS TRUST

Mathematics Activity

Australian Mathematics Competition for the Westpac Awards

Westpac

This page will be developed to give students a wide range of opportunities to practice their mathematics, and teachers warm-up papers and other problems to give their class. Problems to be found here will cover a wide range of standards, from accessible to all students up to challenging.

When a question is posted without solution, if you are from a participating school and within the valid school year, send your solutions here, making it clear which problems you are answering. If your solution is complete we will acknowledge with your name, school and school year. Generally when a sufficient number of correct solutions are in we will post the complete solutions, and follow with new problems.

These questions use mathematics from within the school syllabus, and the questions within each set range from broadly accessible to challenging, requiring problem solving skills.

Current Warm-up papers

- **Middle Primary, Years 3 and 4**
  Current Problems
  Correct solutions have been received from
  - Sam Bird, Year 4, St Peters Lutheran School, Blackwood, SA
  - Kevin Ge, Year 3, Haberfield Public School, NSW
  - Leticia Holt. Year 4, St. Joachim's Primary School, Carrum Downs, Victoria
  - Devon Kaluarachchi, Year 4, St Joachim's Primary School, Victoria
  - Khaw Wei Kit, Year 3, S.J.K.(C) Serdang Baru 2, Malaysia
  - Samantha Molloy, Year 4, Woodlands Primary School, Langwarrin, Victoria
  - Laura Roden, Year 3, Aranda Primary School, ACT
  - Minmin Tai, Year 4, Haberfield Public School, NSW
  - Wong Xiang Qing, Year 3, Sin Min Primary School (B), Kedah, Malaysia
  - Mark Nielsen, Year 3, Castle Hill Public school, NSW
- **Upper Primary, Years 5, 6 and 7**
  Current Problems
  Correct solutions have been received from
  - Michelle He, Year 6, Fintona Girls School, Victoria
  - Hannah Nilsson, Year 6, Marysville Primary School, Victoria

- Khaw Syn Li, Year 6, S.J.K.(C) Serdang Baru 2, Malaysia
- Sherilyn Yao, Year 5, St. Michael's Primary School, Baulkham Hills, NSW
- Wong Ze Ying, Year 5, Sin Min Primary School (B), Kedah, Malaysia
- Edward Yoo, Year 5, Burrendah Primary School, WA

- **Junior, Years 7 and 8**
  Current Problems
  Correct solutions have been received from
  - Kaalya De Silva. Year 8, Smith's Hill High School, NSW
  - Siddharth Jain, Year 7, Box Hill High School, Victoria
  - Cara Joseph, Year 8, Wheelers Hill Secondary College, Victoria
  - Hannah Nilsson, Year 6, Marysville Primary School, Victoria
  - Shereen Susan Stanley, Year 8, Hunter Christian School, Mayfield, NSW
  - Sherilyn Yao, Year 5, St. Michael's Primary School Baulkham Hills, NSW
  - Edward Yoo, Year 5, Burrendah Primary School, WA
  - Peter Yang, Year 8, North Sydney Boys High School, NSW
  - Abdullah Sarker, Year 7, Sydney Boys High School, NSW
- **Intermediate, Years 9 and 10**
  Current Problems
- **Senior, Years 11 and 12**
  Current Problems
  Correct solutions have been received from
  - Paulino Casimiro, Year 12, Willow International School, Mozambique
  - Khaw Syn Wei, Year 11, Sekolah Menengah Kebangsaan Seri Serdang, Malaysia
  - Kerri Lam, Year 12, East Doncaster Secondary College, Melbourne, Victoria
  - Jeremiah Lock, Year 12, Raffles Junior College, Singapore
  - Nazmus Salehin, Year 11, Peterborough High School, SA

AMC WARM-UP PAPER
MIDDLE PRIMARY PAPER 3

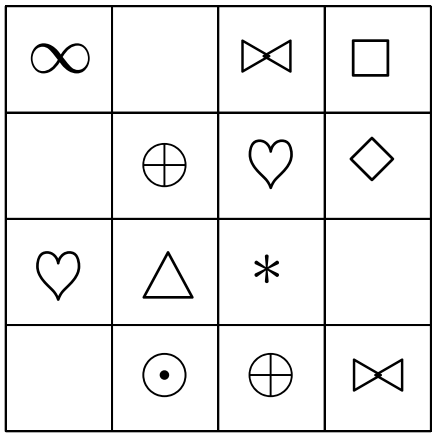
1. Which of these numbers is the largest?

(A) 321 (B) 213 (C) 317 (D) 231 (E) 198

2. My dog eats $\frac{1}{2}$ kg of dog food each day. How much dog food does he eat each week?

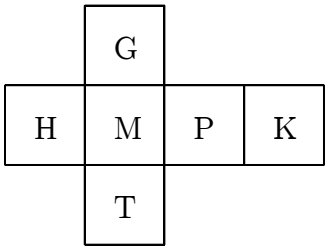
(A) $\frac{1}{2}$ kg (B) 1 kg (C) 2 kg (D) $3\frac{1}{2}$ kg (E) 7 kg

3. In the grid, which object is found in the third square from the right, on the second row from the top?



(A)  (B)  (C)  (D)  (E)

4. A net of a cube is drawn with letters on it as shown. When the net is made into a cube, what letter is opposite M?



(A) H (B) T (C) P (D) K (E) G

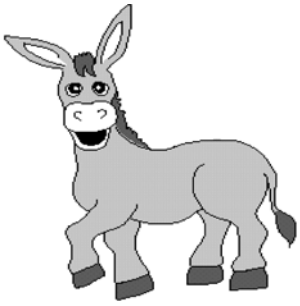
---

5. Anne, Bob and Claire have 20 sweets in a pile. Anne takes half the pile and Bob then takes half of what is left. Claire gets the remaining sweets. How many sweets does Claire get?

(A) 0 (B) 4 (C) 5 (D) 10 (E) 15

---

6. In Farawayland animals are measured in swords and daggers. Puss-in-Boots is 2 swords tall or 5 daggers tall. Donkey is 15 daggers tall.

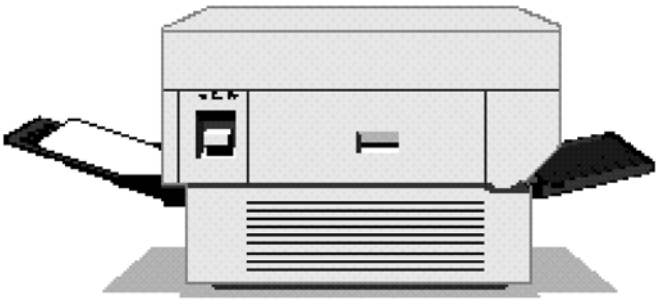


How tall is Donkey in swords?

(A) 2 (B) 5 (C) 6 (D) 30 (E) 525

---

7. A printer prints 3 pages per minute.

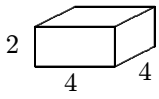


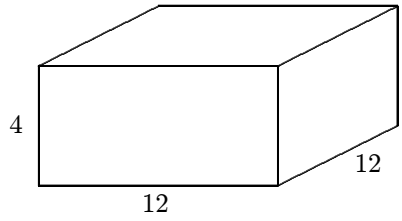
How long would it take to print 189 pages?

(A) 50 mins (B) 55 mins (C) 58 mins (D) 1 hr 3 mins (E) 1 hr 5 mins

---

8. How many shapes 4 cm long, 4 cm wide and 2 cm high will fit in a box which measures 12 cm long, 12 cm wide and 4 cm high?





(A) 12 (B) 16 (C) 18 (D) 20 (E) 24

9. If 4 days after the day before yesterday is Sunday, what day of the week is tomorrow?

(A) Thursday (B) Friday (C) Saturday (D) Sunday (E) Monday

10. Lee buys two drinks and one ice-cream for \$7. Kim buys one drink and two ice-creams for \$8. Mario buys one drink and one ice-cream. How much, in dollars, will this cost Mario?

* * *