Discrete Mathematics in the High School Curriculum.

Ian Anderson, Glasgow (United Kingdom)
Bram van Asch, Eindhoven (The Netherlands)
Jack van Lint, Eindhoven (The Netherlands)

Abstract: In this paper we present some topics from the field of discrete mathematics which might be suitable for the high school curriculum. These topics yield both easy to understand challenging problems and important applications of discrete mathematics. We choose elements from number theory and various aspects of coding theory. Many examples and problems are included.

Kurzreferat: In diesem Artikel stellen wir einige Themen vor, die sich unserer Meinung nach für den Mathematikunterricht der Sekundarstufe eignen. Diese Themen vermitteln sowohl leicht verständliche, anspruchsvolle Probleme als auch Einsicht in wichtige Anwendungen der Diskreten Mathematik. Wir haben Themen aus der Zahlentheorie und verschiedene Aspekte der Kodierungstheorie ausgewählt. Der Artikel enthält viele Beispiele und Aufgaben.

ZDM-Classification: E74, F64, M94, P24

1. Introduction

In the high school mathematics curriculum one usually finds subjects like algebra, geometry, differential and integral calculus, statistics. Mostly students learn algorithms for performing calculations and solving equations. Quite often they do not understand what they are doing, and doing mathematics is often considered to be very dull. There is no challenge in the given tasks. The important aspect of mathematics of proving statements is mostly forgotten. Using geometry to give them some feeling about the notion of proof is usually only successful for the more gifted students. Maybe the field of discrete mathematics can offer other, more challenging and accessible problems to get high school students interested in mathematics. We shall describe some possibilities in that direction.

2. Elementary Number Theory

The notion of positive integers is familiar to children from a very early age on. And in number theory there are many problems that ask for problem solving strategies and proofs. In each of the following sections there is a central theorem, definition or strategy, and in the examples applications are discussed.

2.1 Divisibility

The central part of this section is the unique factorization theorem.

Theorem 1
Every integer $n > 1$ can be written in a unique way as $n = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$, where $p_1 < p_2 < \cdots < p_t$ are prime numbers and $a_i \geq 1$.

This theorem states that a factorization exists, but it does not tell you how to find it. For large numbers that is a very hard problem. The safety of a very widely used cryptographic system, the so called RSA system, depends on this fact. But once you have found a factorization of a number n, it can be used for various purposes.

Example 1
This factorization enables us to determine in a systematic way all divisors of n: every divisor is of the form $d = p_1^{b_1} p_2^{b_2} \cdots p_t^{b_t}$ with $0 \leq b_i \leq a_i$. The number of divisors is therefore given by $(a_1 + 1)(a_2 + 1) \cdots (a_t + 1)$. What is the number of divisors of $20!$?

Example 2
Greatest common divisor and least common multiple can be described in a simple way: if $n = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ and $m = p_1^{b_1} p_2^{b_2} \cdots p_t^{b_t}$, with $a_i \geq 0$ and $b_i \geq 0$, then $\gcd(m,n) = p_1^{c_1} p_2^{c_2} \cdots p_t^{c_t}$ and $\mathrm{lcm}(m,n) = p_1^{d_1} p_2^{d_2} \cdots p_t^{d_t}$, where $c_i = \min(a_i, b_i)$ and $d_i = \max(a_i, b_i)$.

Problem 1
Prove that any real number of the form $\sqrt{p}$, where p is a prime number, is irrational.

Problem 2
A positive integer n is said to be perfect if n is equal to the sum of all its positive divisors, excluding n itself. For instance 6 is the smallest perfect number. Show that if the number $2^k - 1$ happens to be a prime number, then the number $n = 2^{k-1}\left(2^k - 1\right)$ is a perfect number.

2.2 Greatest common divisor

The factorization of positive integers can be used to determine the greatest common divisor. A much more efficient way is the so-called Euclidean algorithm, based on the following theorem.

Theorem 2
Given integers a and b, with $b > 0$, there exist unique integers q and r such that $a = qb + r$ and $0 \leq r < b$.

Example 3
Now we describe the Euclidean algorithm. Suppose integers $a \geq b > 0$ are given. Then there are integers q_1 and r_1 such that

$$a = q_1 b + r_1, \quad 0 \leq r_1 < b.$$

If $r_1 = 0$ then $b = \gcd(a,b)$. If $r_1 \neq 0$, then we can find integers q_2 and r_2 such that

$$b = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1.$$

If $r_2 = 0$, then we stop, otherwise we proceed as before to obtain q_3 and r_3 such that

$$r_1 = q_3 r_2 + r_3, \quad 0 \le r_3 < r_2.$$

At some stage a zero remainder appears, say

$$r_{n-2} = q_n r_{n-1} + r_n \text{ and } r_{n-1} = q_{n+1} r_n.$$

It is easy to check that $\gcd(a, b) = r_n$: by going back we see that r_n is a common divisor of a and b, and by going down again we see that any common divisor of a and b also divides r_n.
This is a very efficient way to compute the greatest common divisor of two integers. From the system of equations it also follows that $\gcd(a, b)$ can be written as a combination of a and b:

$$\gcd(a, b) = pa + qb$$

for some integers p and q. Starting with the next to last equation we write

$$r_n = r_{n-2} - q_n r_{n-1}.$$

Now solve the preceding equation in the algorithm for r_{n-1} and substitute to obtain r_n as a combination of r_{n-2} and r_{n-3}. Continuing in this way through the system of equations we finally reach a stage where $\gcd(a, b) = r_n$ is expressed as a combination of a and b.

Example 4
In particular, $\gcd(a, b) = 1$ if and only if there are integers p and q such that $pa + qb = 1$.

Example 5
We consider the equation $ax + by = c$, where a, b and c are integers, and we are looking for integral solutions for x and y. It is clear that such solutions exist if and only if $\gcd(a, b)$ divides c. In that case we can easily write down all solutions in parametric form. First, using the Euclidean algorithm, we determine integers p and q such that $pa + qb = \gcd(a, b)$. If we put $x_0 = \dfrac{pc}{\gcd(a, b)}$ and $y_0 = \dfrac{qc}{\gcd(a, b)}$, then (x_0, y_0) is a solution. And once we have found a particular solution (x_0, y_0) it is not hard to see that we get all integral solutions by putting $x = x_0 + \dfrac{bt}{\gcd(a, b)}$, $y = y_0 - \dfrac{at}{\gcd(a, b)}$, where t is an arbitrary integer.
There are many problems that involve equations of this kind.
They arise for instance in puzzles of the following kind. A customer bought 15 pieces of fruit, oranges and bananas for \$ 2.07. An orange costs 3 cents more than a banana, and more oranges than bananas were purchased. How many pieces of each kind were purchased? By putting x for the number of oranges, y for the number of bananas and z for the price of a banana, we get the equations $(z + 3)x + yz = 207$ and $x + y = 15$, which can be reduced to $3x + 15z = 207$, or $x + 5z = 69$. This equation has infinitely many integral solutions, which can be determined in the way described above. Only those values of x with $7 < x < 15$ furnish solutions to the original problem. In fact there are two solutions to this particular problem.

2.3 Calculations modulo n

If you multiply two integers a and b, it is very easy to determine the last digit of this product: multiply the last digits of a and b and take the last digit of this product. In fact we are looking at the remainders on dividing a, b and ab by 10. If we are interested in the last two digits we can follow the same procedure by looking at the remainders on dividing by 100. Instead of 10 or 100 we can take any positive integer and this leads to the notion of congruence modulo an integer.
Let $n \ge 1$ be a fixed positive integer.

Definition 1
Two integers a and b are said to be congruent modulo n, symbolized by $a \equiv b \pmod{n}$, if n divides $a - b$.

The following properties of congruence modulo n are easy to verify.

Properties 1

(i) $a \equiv a \pmod{n}$,

(ii) *if* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$,

(iii) *if* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$,

(iv) *if* $a \equiv b \pmod{n}$, *then* $a + c \equiv b + c \pmod{n}$ *and* $ac \equiv bc \pmod{n}$,

(v) *if* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then* $a + c \equiv b + d \pmod{n}$ *and* $ac \equiv bd \pmod{n}$,

(vi) *if* $a \equiv b \pmod{n}$, *then* $a^k \equiv b^k \pmod{n}$ *for any integer* $k \ge 0$.

These properties can be used to perform straightforward calculations. For instance:

Problem 3

(i) Find the remainder when 20^{2003} is divided by 7.

(ii) What are the last two digits of the number $1! + 2! + \cdots + 100!$?

(iii) Show that the number $53^{103} + 103^{53}$ is divisible by 13.

Example 6
If $\gcd(a,n) = 1$, then we can find s and t such that $sa + tn = 1$. Therefore $sa \equiv 1 \pmod{n}$. In this case the equation $ax \equiv b \pmod{n}$ behaves in the same way as the ordinary equation $ax = b$ over the real numbers: multiply by s (the inverse of a modulo n), and we find exactly one solution $x = sb \pmod{n}$. If $\gcd(a,n) > 1$, then the situation is essentially different: there may be no solutions at all, or there may be more than one solution. A special case occurs if $n = p$ is a prime. Then we have $\gcd(a,p) = 1$ for all a such that a is *not* congruent to 0 modulo p. In that case the equation $ax \equiv b \pmod{p}$ has a unique solution modulo p for all b. In particular there is an inverse of a modulo p for all such a. When we are solving equations the system of integers with addition and multiplication modulo a prime number p behaves in many ways in the same way as the systems of rational or real numbers.

Example 7
The non-existence of solutions in integers of certain equations can sometimes be proved using congruences. For example the equations $3x^2 + 14 = y^2$ and $7x^3 + 5 = y^3$ have no integral solutions: $y^2 \equiv 2 \pmod{3}$ resp. $y^3 \equiv 5 \pmod{7}$ are impossible. And if $n \equiv 3 \pmod{4}$ then there are no integral x and y such that $x^2 + y^2 = n$; for such n there are no lattice points on the circle $x^2 + y^2 = n$.

Example 8
From the congruences $10 \equiv 1 \pmod{3}$, $10 \equiv 1 \pmod{9}$ and $10 \equiv -1 \pmod{11}$ we get some special divisibility tests. Let $N = a_m a_{m-1} \cdots a_1 a_0$ be a positive integer in decimal notation, so $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$. Put $S = a_0 + a_1 + \cdots + a_{m-1} + a_m$ and $A = a_0 - a_1 + \cdots + (-1)^m a_m$ (alternating sum of the digits). Then we have

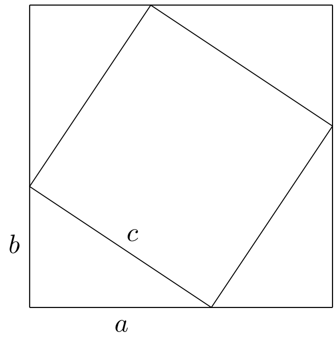
$$\begin{array}{lcll} N & \equiv & S & \pmod{3} \\ N & \equiv & S & \pmod{9} \\ N & \equiv & A & \pmod{11} \end{array}$$

From this it follows that:

N is divisible by 3 iff S is divisible by 3
N is divisible by 9 iff S is divisible by 9
N is divisible by 11 iff A is divisible by 11

There are similar, although slightly more complicated tests for divisibility by 7 and 13.

2.4 Pythagorean triples



Here is a simple proof of the Pythagorean Theorem:
$(a+b)^2 = c^2 + 2ab$,
from which it follows immediately that $a^2 + b^2 = c^2$.

In this section we are interested in integral solutions of the Pythagorean equation. The most well-known example is $a = 3$, $b = 4$ and $c = 5$. We give the following definition.

Definition 2
A triple (x,y,z) of integers is called a Pythagorean triple if $x^2 + y^2 = z^2$.

It is obvious that if (x,y,z) is a Pythagorean triple, then so is (tx,ty,tz) for all integers t. And if two of x, y and z have a common factor then this is a factor of the third one too. We will show in a constructive way that there are infinitely many Pythagorean triples (x,y,z) such that $\gcd(x,y,z) = 1$, the so called *primitive* Pythagorean triples.

Proposition 1
There are no primitive Pythagorean triples (x,y,z) such that z is even.

If z is even then both x and y have to be odd. But then $x^2 + y^2 \equiv 2 \pmod{4}$, and $z^2 \equiv 0 \pmod{4}$, so $x^2 + y^2 \neq z^2$.

Suppose now that (x,y,z) is a primitive Pythagorean triple such that x is even and y is odd. If $x = 2k$ we have $(z-y)(z+y) = 4k^2$, i.e. $\left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right) = k^2$. It is easy to see that $\gcd\left(\frac{z-y}{2}, \frac{z+y}{2}\right) = 1$ (the assumption $\gcd\left(\frac{z-y}{2}, \frac{z+y}{2}\right) = d > 1$ leads to the conclusion that d is a common divisor of x, y and z). We conclude that both $\frac{z-y}{2}$ and $\frac{z+y}{2}$ have to be squares, say $\frac{z-y}{2} = s^2$ and $\frac{z+y}{2} = t^2$. It then follows that $z = s^2 + t^2$, $y = t^2 - s^2$ and $x = 2st$. It is easy to check that these values for x, y and z indeed yield Pythagorean triples.

Proposition 2
All primitive Pythagorean triples with even x are given by

$$\begin{cases} x = & 2st \\ y = & t^2 - s^2 \\ z = & s^2 + t^2 \end{cases}$$

where s and t are relatively prime numbers of different parity.

2.5 Mathematical induction

A method of proof (and of definition as well), often used when dealing with properties of positive integers, is called *mathematical induction.* It can be stated for instance in the following way.

The principle of mathematical induction
Let $P(n)$ be some proposition for integers $n \geq 0$ and let $N \geq 0$. To prove that $P(n)$ is true for all $n \geq N$ perform the following two steps.

(*i*) *Prove that $P(N)$ is true,*
(*ii*) *Assume that $P(k)$ is true for an arbitrary $k \geq N$. Prove that $P(k+1)$ is true.*

Sometimes a variant of this principle of mathematical induction is used, where (*ii*) is replaced by

(*ii'*)*Assume that $P(j)$ is true for $N \leq j \leq k$. Prove that $P(k+1)$ is true.*

Problem 4
Prove the following well-known identities using mathematical induction.

(i) $1 + 2 + \cdots + n = \frac{1}{2}n(n+1)$.

(ii) $1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$.

(iii) $1 + r + r^2 + \cdots + r^n = \dfrac{r^{n+1} - 1}{r - 1}$.

Problem 5
Consider the Fibonacci sequence defined by

$$F_1 = 1, F_2 = 1, F_n = F_{n-1} + F_{n-2} \text{ for } n \geq 3.$$

Prove:

(i) $F_3, F_6, F_9, \cdots$ all are even numbers.

(ii) $F_n = \dfrac{1}{\sqrt{5}}\left(\left(\dfrac{1+\sqrt{5}}{2}\right)^n - \left(\dfrac{1-\sqrt{5}}{2}\right)^n\right)$.

(iii) $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$.

(iv) $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$.

Problem 6
Prove that for all $n \geq 3$ the sum of the interior angles of a convex n-gon is equal to $(n-2) \cdot 180^o$.

Example 9
Consider for all $n \geq 1$ a 2^n by 2^n square array. If you remove any one square the resulting squares can be covered by L-shaped trominos. For $n = 1$ this is obvious. Look at the next case, $n = 2$. Divide the original array into four quarters. The removed square came from one of these quarters. This quarter can be covered. If you can solve the problem of covering the other three quarters a proof by induction is straightforward.

Example 10
The last example is a bit more complicated. We consider linear binary codes, i.e. codes over the alphabet $\mathbb{Z}_2 = \{0,1\}$ with addition and multiplication modulo 2 (see also Section 4). An interesting family of codes are the so called first order Reed-Muller codes. They can be defined for instance in the following way.

(*i*) $R_0 = \mathbb{Z}_2 = \{0,1\}$.
(*ii*) For $n \geq 1$ we take R_n to be the subspace of $\mathbb{Z}_2^{2^n}$ whose basis consists of all vectors of the form $(\mathbf{u}, \mathbf{u})$ and $(\mathbf{0}, \mathbf{1})$, where $\mathbf{u}$ is a basis vector in R_{n-1}, and $\mathbf{0}$, $\mathbf{1}$ are the all-zero and all-one vector in $\mathbb{Z}_2^{2^{n-1}}$ respectively.

So for instance a basis for R_1 is given by

$$\{(1,1),(0,1)\}$$

and for R_2 by

$$\{(1,1,1,1),(0,1,0,1),(0,0,1,1)\}.$$

Here the principle of mathematical induction is used to *define* the code R_n for all $n \geq 0$. But it can also be used to *prove* properties of these codes. In a code the *weight* of a vector (i.e. the number of non-zero coordinates) is an important notion. Using mathematical induction it is not hard to prove that in the code R_n every vector except $\mathbf{0}$ and $\mathbf{1}$ has weight 2^{n-1}.

2.6 Double counting

We give a number of examples of a method that is often used in combinatorics. It is called *"double counting"*. Generally this means that certain objects are counted in two different ways. Since the results must be the same, we obtain an equation. Sometimes counting is extended to calculating a sum in two ways.

Example 11
A *graph* consists of a set V of *points*, sometimes called *vertices*, and a set E of pairs from V, called *edges*. Often the graph is described by a picture containing the

vertices, where a (not necessarily straight) line connects two of the vertices if the corresponding pair is an edge. The number of edges containing a given vertex is called the degree of that vertex. We claim that the sum of all the degrees is $2|E|$. To see this, count the ordered pairs (x, y), where $\{x, y\}$ runs through all the edges. On the one hand we thus count every edge twice. On the other hand, the number of ordered pairs (x, y) with a fixed x and $\{x, y\}$ an edge, is the degree of x.

Example 12
Let $S_1, S_2, \dots, S_b$ be subsets of size k of the set $N = \{1, 2, \dots, n\}$. We are given that every pair $\{x, y\}$ of distinct elements from N occurs in exactly two of the k-tuples. We wish to show that every element in N occurs in a fixed number r of the k-tuples and we wish to express the value of b in n and k.

For the first of these, pick an i in N. Suppose it occurs in r_i of the k-tuples. How many pairs $\{i, j\}$ do these k-tuples contain? On the other hand, we know that each such pair occurs twice in all the k-tuples. What is our conclusion? Once we know that r_i does not depend on i we can count in two ways what the total number of elements in all the sets S_j is. This gives us the value of b.

Example 13
Consider the so-called *complete graph* on 6 vertices. In this graph, every pair is an edge. So, there are 15 edges. We are told that the edges have been colored red or blue but we are not told how this was done. We are asked to prove that in the graph there are at least two *monochromatic* triangles, i.e. triples a, b, c such that $\{a, b\}$, $\{b, c\}$, and $\{c, a\}$ have the same color. Try this first without reading on. Hard? Now we shall do some double counting. We count two-colored *forks*, i.e. triples $\{a, b, c\}$ of vertices such that the two edges $\{a, b\}$ and $\{a, c\}$ have different colors. Given a vertex a, how many two-colored forks can have a as the central vertex? So, the maximum number of two colored forks is what? Every triangle that is not monochromatic contains exactly two such two-colored forks. Complete the proof.

Example 14
Consider a Hadamard matrix H, i.e. H is a matrix of size n by n in which all entries are $+1$ or -1, with the property that the inner product of two distinct rows is 0. Denote the entry in row i and column k by h_{ik}. Count the total number of pairs $\{h_{ik}, h_{jk}\}$ ($1 \leq i < j \leq n$, $1 \leq k \leq n$) that have different sign. Let s_k be the sum of the n entries in the k-th column of H. Now show that $\sum_{k=1}^{n} s_k^2 = n^2$.

Example 15
Let G be a graph on v vertices in which every vertex has degree k. (So, how many edges does G have?) There are *no* triangles in G. G has the property that for any pair x, y of vertices such that $\{x, y\}$ is not an edge, there are exactly two other vertices a, b such that $\{a, x\}$ and $\{a, y\}$ are edges and also $\{b, x\}$ and $\{b, y\}$ are edges. A square (four vertices) is an example. Prove that $v = (k^2 + k + 2)/2$. Do this as follows. Take any vertex x. Let S be the set of vertices joined to x by an edge and let T be the set of vertices that are not joined to x. Count in two ways how many edges there are with one vertex in S and the other in T.

3. Check digits in the supermarket

Every day in the supermarket arithmetic modulo 10 or 11 is used in various ways to provide check digits in the code numbers assigned to individual items on the shelves and in the 16-digit numbers on credit cards. We look at four important examples.

3.1 The EAN system

All items on the supermarket shelves have a code number and barcode on them. The most common code in Europe is the 13-digit code known as EAN 13; EAN stands for European Article Number, but it is now used world wide. As an example, a 500 gram packet of Kellogs cornflakes, bought in the UK, has the number

$$5\,0\,0\,0\,1\,2\,7\,0\,1\,2\,0\,9\,7.$$

The 50 at the beginning indicates a UK manufacturer or distributor. The subsequent numbers up to the 9 are assigned by Kellogs, the 00127 being common to all Kellogs products, and the final digit 7 is a *check digit* chosen so that

3(sum of digits in even positions) + (sum of digits in odd positions)

is divisible by 10. Here we have

$$3(0+0+2+0+2+9)+(5+0+1+7+1+0+7)$$
$$= 39 + 21 = 60.$$

Problem 1
Find the check digit x on a tin of beans

$$5\,0\,0\,0\,1\,5\,7\,0\,0\,4\,1\,8\,x.$$

It should be fairly clear that, because of the check digit, any single error will be detected, in the sense that the resulting number will not give a multiple of 10. For example, if the cornflakes number were misread as $5\ 0\ 0\ 0\ 1\ 2\ 7\ 0\ 1\ 3\ 0\ 9\ 7$, our calculation would give 63 instead of 60. The next most common type of error is a transposition of two (normally adjacent digits.

Example 1

(a) If the cornflakes number is misread as

$$5\,0\,0\,0\,1\,2\,7\,0\,2\,1\,0\,9\,7$$

then the error is detected.

(b) If it is misread as

$$5\,0\,0\,0\,1\,7\,2\,0\,1\,2\,0\,9\,7$$

then the error is not detected, since the calculation does indeed yield a multiple of 10.

Problem 2

Show that $3x + y$ and $3y + x$ differ by a multiple of 10 if and only if x and y differ by 5. Does this help to explain the previous example ?

The EAN 13 system was set up shortly after the United States introduced its 12-digit Universal Product Code (UPC) system. You can convert any UPC number into an EAN 13 number by putting a 0 at the front. EAN 13 numbers contain information about country of origin. A TDK audio tape with number $4\ 9\ 0\ 2\ 0\ 3\ 0\ 1\ 2\ 9\ 7\ 5\ 0$ has Japanese origin , as the 49 at the start indicates. A 0 at the start indicates US or Canada, 40 Germany, 743 Nicaragua, 471 Taiwan, and so on. Any book is considered as coming from 'Bookland', and has number starting with 978, while periodicals have numbers beginning 977.

Sometimes an 8-digit EAN system is used instead. The final digit is again a check digit, chosen so that

3(sum of digits in odd positions) + (sum of digits in even positions)

is a multiple of 10.

Problem 3

Find the check digit x in the following EAN 8 number:

$$5\,0\,1\,1\,4\,4\,7\,x$$

3.2 The ISBN system

All books are given an International Standard Book Number, consisting of 10 digits including a check digit. Take for example the hardback edition of *Harry Potter and the Goblet of Fire*. Its number is

$$0 - 7\,4\,7\,5 - 4\,6\,2\,4 - X$$

The 0 indicates that it is from an English speaking country. The $7\ 4\ 7\ 5$ is the number assigned to the publisher (Bloomsbury). The $4\ 6\ 2\ 4$ is a number assigned by the publisher to this particular book, and the X at the end is the check digit which is chosen so that
$10(0)+9(7)+8(4)+7(7)+6(5)+5(4)+4(6)+3(2)+2(4) +$ check digit
is a multiple of 11. Here we have

$$0 + 63 + 32 + 49 + 30 + 20 + 24 + 6 + 8 = 232$$

and the next multiple of 11 is 242, so we take check digit 10. Since 10 unfortunately uses TWO digits, we use the Roman ten, X. In general, an ISBN is of the form

$$a_{10}\ a_9\ a_8\ a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1$$

where

$$\sum_{k=1}^{10} k a_k \equiv 0 \pmod{11}.$$

Problem 4

A book has ISBN

$$0 - 9\,0\,6\,2\,1\,2 - 7\,7 - x$$

where x denotes the check digit. Find x.

Problem 5

When receiving a book order over the telephone, the bookseller did not hear the second last digit (x) clearly. Find what x is.

$$0 - 1\,7 - 4\,3\,1\,4\,9\,x - 3.$$

The ISBN system detects all single digit errors and all transpositional errors. Consider, for example, the transposition of xy, in the 5th and 4th positions from the right, into yx. The contribution $5x + 4y$ to the sum is replaced by $5y + 4x$. Can these two numbers differ by a multiple of 11 ?

The EAN 13 number for a book is obtained from the ISBN by removing the check digit, adding $9\ 7\ 8$ at the front, and then adding the EAN check digit at the end.

Problem 6

The Harry Potter book mentioned above has EAN 13 number $9\ 7\ 8\ 0\ 7\ 4\ 7\ 5\ 4\ 6\ 2\ 4\ x$ for some x. Find x.

3.3 The IBM system

This system was introduced by IBM, and is used by many libraries and some credit card systems such as Visa. A Visa card has a 16-digit number, wheareas Glasgow University Library uses a 14-digit system in which all numbers begin with 30114. As in the systems discussed above, the final digit is a check digit, but in the

IBM scheme the rule is slightly more complicated. Recall that, in the EAN system, every second digit was multiplied by 3. It should be clear that if 2 were used instead of 3, then not even every single digit error would be detected (e.g. a 3 misread as an 8). The IBM system uses 2 as the multiplier, but to distinguish between numbers that differ by 5 it introduces a further level of sophistication. To illustrate this, take the GU library book whose library number is

$$3\ 0\ 1\ 1\ 4\ 0\ 0\ 5\ 2\ 9\ 7\ 3\ 6\ 4.$$

The requirement is that

2(sum of odd placed digits) + (sum of even placed digits)

+ (number of odd placed digits which are ≥ 5)

must be a multiple of 10. In this example the odd placed digits are 3,1,4,0,2,7,6 of which two are ≥ 5. We have

$$2(3+1+4+0+2+7+6)+(0+1+0+5+9+3+4)+2 = 46+22+2 = 70.$$

Problem 7
Find the check digit x in the following credit card number :

$$4\,5\,4\,7 \quad 3\,0\,1\,2 \quad 5\,4\,7\,8 \quad 1\,0\,3\,x$$

Problem 8
The following credit card number was read over the phone when tickets for a concert were being ordered.

$$4\,5\,4\,7 \quad 3\,0\,1\,2 \quad 3\,2\,4\,1 \quad 1\,2\,3\,4.$$

Will it be accepted? If not, can you find a possible transposition of adjacent digits which might have been made when a valid number was misread?

Problem 9
Will the following be accepted as a valid Visa number?

$$4\,5\,6\,0 \quad 1\,7\,7\,2 \quad 5\,0\,1\,1 \quad 9\,0\,1\,3$$

In fact,

it has been misread. Can you suggest a transpositional error that is *never* detected ? Is this the only one ?

3.4 Barcodes
We are now going to see how the barcode version of an EAN 13 code is formed. Each digit $0, ..., 9$ will be represented by a binary sequence of length 7 in which there is a change from 0 to 1 or 1 to 0 exactly three times. For example, 0110001 is such a sequence, but 1100111 is not. It is easy to check that there are 20 such sequences beginning with 0 and 20 beginning with 1. Those beginning with 0 are of two types: those of type A have an odd number of 1s, and those of type B have an even number of 1s.

How a particular digit is encoded depends on whether it is in the left or right half of the EAN codeword. Consider for example the 500 g box of cornflakes with EAN 13 number

$$5\,0\,0\,0\,1\,2\,7\,0\,1\,2\,0\,9\,7$$

and the following barcode.

5 0 0 0 1 2 7 0 1 2 0 9 7

In the barcode a black line represents a 1, a white space represents 0. So 11 would be represented by a black line of double width, and so on. All barcodes start and finish with 101, represented usually by longer lines, and they have 01010 in the middle. In the above example, the other bars in the left half represent

0001101 0100111 0100111 0011001 0010011 0010001

which stands for

0	0	0	1	2	7
(A)	(B)	(B)	(A)	(A)	(B)

according to the following table

Number	Lefthand A	Lefthand B	Righthand
0	0001101	0100111	1110010
1	0011001	0110011	1100110
2	0010011	0011011	1101100
3	0111101	0100001	1000010
4	0100011	0011101	1011100
5	0110001	0111001	1001110
6	0101111	0000101	1010000
7	0111011	0010001	1000100
8	0110111	0001001	1001000
9	0001011	0010111	1110100

Note in passing how the columns of the table are related to one another - do you see how to get the second and third columns from the first?

The bars on the right of the above codeword represent

1110010 1100110 1101100 1110010
1110100 1000100
which therefore stands for

$$0 \quad 1 \quad 2 \quad 0 \quad 9 \quad 7$$

as can be checked from the table.

We thus have the whole of the EAN 13 code number apart from the 5 at the beginning. What about this 5 ? Where is it ? It is actually 'hidden' in the choice of As and Bs on the left, a choice which so far has not been explained. The secret lies in the following table! Note that the encoding of 5 did indeed use the pattern

$$ABBAAB$$

0	$AAAAAA$	5	$ABBAAB$
1	$AABABB$	6	$ABBBAA$
2	$AABBAB$	7	$ABABAB$
3	$AABBBA$	8	$ABABBA$
4	$ABAABB$	9	$ABBABA$

Two very clever points emerge.

(i) The 13-digit EAN 13 numbers are effectively encoded as 12 digits, the sequence of As and Bs determining the initial digit which is apparently absent. American UPC numbers, which have 12 digits, can be thought of as EAN 13 numbers by adding a 0 at the start, are encoded in type A words only. So scanners can deal with both EAN 13 and UPC words together!

(ii) A scanner can read a barcode upside down; indeed it knows which end is the beginning and which is the finish.

Problem 10
Explain how a scanner knows which end is the beginning. (It has something to do with odd numbers of 1s on the left.)

Problem 11
A packet of tea from Taiwan has EAN 13 code

$$4\,7\,1\,1\,4\,0\,6\,8\,8\,3\,3\,8\,3.$$

How would you encode (a) 7, (b) 0 in the barcode? Write down the complete barcode as a sequence of 0s and 1s.

4. Coding Theory

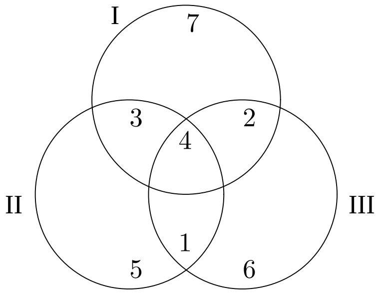
4.1 Error-correcting Codes

Information is often stored on a medium or transmitted from a (so-called) sender to a receiver via sequences of symbols from a fixed set which we usually call the *alphabet*. For instance 'good morning' is a sequence using our usual alphabet. Another example is '$\pi\alpha\nu\tau\alpha \quad \rho\epsilon\iota$' which uses another familiar alphabet. The sequence '2003' conveys something to the reader, this time using as alphabet the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. The binary system has an alphabet with only two symbols, namely 0 and 1. In most cases that we are familiar with, only certain sequences have a meaning. For instance in Morse the sequence $\cdots - - - \cdots$ has a well known meaning. It often happens that a recorded or transmitted sequence is received with one or more errors. If we see the word 'alpjabet' we realize that the 'j' should be an 'h', i.e. we are able to correct the error.

In the theory of error-correcting codes we start with some alphabet, say $\{0, 1\}$ and formulate rules with which to form sequences of n symbols, which we call *codewords*. When transmitting information, only the sequences satisfying the rules can be used. The problem is to find rules that make it possible for a receiver to spot and correct an error. If the alphabet has only two symbols, spotting is enough because there is only one possible way to change the symbol. In our example above, spotting the 'j' as wrong leaves us 25 candidates for the right symbol. Our knowledge of the rules (i.e. of English words) makes us choose 'h'. We now wish to have mathematical ways of correcting errors.

We start with a very simple example. However, we point out that this was the first error-correcting code ever constructed and it was used in practice (1949). Suppose that we have a channel over which we can transmit two different symbols (as when Morse is used). We call these symbols 0 and 1. Suppose furthermore that there is a certain probability p that a transmitted symbol is received incorrectly (0 as 1 or 1 as 0). We are to transmit a long sequence of 0s and 1s and we wish to reduce the probability of error for the receiver. We do the following. We split our sequence into *four-tuples*. Below, we shall indicate a rule that maps each four-tuple into a *seven-tuple*. The seven-tuples are the codewords of our code. We transmit the seven-tuples, separated by synchronization symbols. In each seven-tuple we include the original four-tuple and adjoin three so-called *redundant* bits.

Consider the figure formed by the three circles in the figure below.



The circles are numbered I, II, III. The seven parts inside one or more circles are numbered 1 to 7 (see figure). The four bits of information are put into parts 1 to 4. The *rule* for the other three (in parts 5,6,7) is: every circle contains an even number of 1s. This uniquely defines the codeword. Note that in order to transmit information in this way, we need 7/4 times as many symbols. We say that we have a *code* with *information rate* 4/7.

In the figure we see that the four-tuple 1101 is mapped to 1101010. Now suppose the receiver gets 1001010. We see that the second bit is wrong but can the receiver also find that out? The seven bits are put into the figure in the positions 1 to 7. The number of 1s in circle II is even but in the other two circles the number of 1s is odd. The receiver now knows that one or more errors have occurred. One error is more likely than two or more. If there is one error, then it is in circle I and also in circle III but not in circle II. There is exactly one part with this property, namely part 2. So, changing the second bit to 1 yields a seven-tuple that satisfies the coding rule and therefore the receiver assumes (correctly) that 1101010 was transmitted.

If $\mathbf{a} = (a_1, a_2, \dots, a_n)$ and $\mathbf{b} = (b_1, b_2, \dots, b_n)$ are two sequences with elements from some alphabet Q, then we define the (*Hamming*)*-distance* of $\mathbf{a}$ and $\mathbf{b}$ to be the number of positions i where $a_i \neq b_i$.

Suppose that C is a code of length n over the alphabet Q, i.e. C is a subset of Q^n. Assume that any two distinct words of C have distance at least $2e+1$. Suppose we take a codeword and alter t of the symbols, where $t < e$. The word that we obtain now has distance t to the original codeword but its distance to all the other codewords is at least $2e + 1 - t > e$. In other words, the altered word is closer to the original codeword than to any other codeword. So, if we see the altered word, we know it contains errors and we also know the most likely word that it originated from. This is the same thing that we did above when 'alpjabet' was changed to 'alphabet'.

Problem 1
Show that the code defined with the circles is a subspace of $\mathbb{Z}_2^7$ with basisvectors (1,0,0,0,1,1,0), (0,1,0,0,0,1,1), (0,0,1,0,1,0,1), and (0,0,0,1,1,1,1). Also show that any two distinct codewords have distance ≥ 3 (which is why we can correct one error if it occurs). We say that the code is a [7,4,3] code.

Problem 2
Suppose that we transmit a codeword of the code described above and the seven-tuple 11?10?0 is received, i.e. two of the received symbols are illegible (these are called *erasures*). What was the codeword? Prove that no matter where the two erasures occur, there is a unique codeword corresponding to the five other bits (assuming that no errors have occurred).

We have seen that if p is a prime, then in $\mathbb{Z}_p$ (the integers mod p) we can not only add, subtract and multiply but division by a non-zero integer is also possible. This makes it possible to use algebraic methods to define codes over the alphabet $\mathbb{Z}_p$.

Example 1
We define a code C over $\mathbb{Z}_3$ to consist of the nine words $(a, b, a + b, a - b)$, where a and b are in $\mathbb{Z}_3$. Note that a multiple of a codeword is also a codeword and that the sum of two codewords (coordinatewise addition) is again a codeword. We say that C is a *linear* code.

Problem 3
Show that if (p, q, r, s) is not in C, then we can obtain a codeword by changing one of the symbols p, q, r, s.

We define the *weight* $w(\mathbf{c})$ of a word $\mathbf{c}$ to be the number of non-zero coordinates of $\mathbf{c}$. If a code C is linear, then the distance $d(\mathbf{a}, \mathbf{b})$ of two codewords $\mathbf{a}, \mathbf{b}$ is the weight of the codeword $\mathbf{a} - \mathbf{b}$. So, if we wish to show that C is a one error-correcting code, it is sufficient to show that all non-zero codewords have weight at least 3. Note that that is very easy for the code of Problem 3. So, for every codeword $\mathbf{c}$, there are nine possible four-tuples that will be decoded to the word $\mathbf{c}$. Does that make Problem 3 easier?

Problem 4
Let the binary code C consist af all possible words $(a, b, c, b + c, a + c, a + b)$. Show that C is one error-correcting.

Problem 5
Construct a linear binary code of length 7, with eight codewords, such that any two distinct codewords have distance at least 4.

Problem 6
We define a binary code C to be the set of words $(a, b, c, d, a+b, c+d, a+b+c+d)$. Decode the following received messages : (1,1,0,1,0,1,1) and (0,1,1,0,1,1,1).

The easiest way to do this is to observe that C can also be defined as the set of words $\mathbf{c} = (c_1, c_2, \ldots, c_7)$ such that the three equations $c_1+c_2+c_5 = 0$, $c_3+c_4+c_6 = 0$, and $c_5 + c_6 + c_7 = 0$ are satisfied.

Problem 7
Consider an alphabet with q symbols. Let C be a code of length n over this alphabet. Show that if C is one error-correcting, then

$$C \text{ has at most } \frac{q^n}{1+n(q-1)} \text{ words.}$$

Problem 8
From the previous problem it looks as if it might be possible to construct a binary one error-correcting code of length 6 with nine words. Show that this is not possible. (Hint : Suppose such a code exists and consider the first two symbols of the codewords. How many possibilities are there?).

4.2 Coding for the Compact Disc

Digital recording of music on a Compact Disc is a complicated procedure. We give a brief description. The music as a continuous waveform is sampled with a frequency of 44100 times per second and the samples are *quantized*, i.e. each measurement is expressed as an integer in the binary number system. In practice *sixteen* bits are used. For stereo-music there are two measurements per sampling, resulting in 32 bits. These are interpreted as a sequence of four so-called *bytes*. A byte is a sequence of eight bits. In the coding for the disc, the bytes are the symbols of the alphabet. So, the alphabet has 256 symbols. As in earlier sections, there are rules to add redundancy. A sequence of 24 symbols (i.e. 24 bytes of eight bits each) is mapped to a sequence of 32 bytes. After some more transformations which we do not go into, the 32-tuples are recorded. So, using earlier terminology, the information rate of the code for CD is 3/4.

There are several causes of errors on a CD, for instance little particles or air bubbles in the plastic, scratches, fingerprints, etc. Even on a brand new CD, as many as 500000 errors are present. By complicated mathematics these are located and corrected by the CD-player. The high quality of the music would have been impossible without error-correcting codes.

The actual mathematics of the coding scheme would be too complicated to explain here. Instead, we shall treat an example in which a coding scheme is used that is *essentially the same* as the one for CD. However, it uses a much smaller alphabet. This enables the reader to actually check that the method works. In our example, we assume that a page from a book is to be transmitted over some channel to a receiver. We consider an alphabet of 31 symbols. These are the 26 letters of our regular alphabet, a space and four punctuation signs (say .,?!). We identify these with the integers 0 to 30. We use 0 for the space, 1 for a, 2 for b, . . . , 26 for z, and 27 to 30 for the punctuation signs. So 'a code' would be interpreted as '1,0,3,15,4,5'.

The channel has the unpleasant property that there is a probability p (specified later) that a symbol is changed into one of the thirty other symbols. So, the received page will contain a number of misprints (depending on p). We wish to reduce the number of misprints by encoding the message before it is sent. As in our first example, we divide the symbols on the page into four-tuples. We map each four-tuple into a six-tuple $(a_0, a_1, a_2, \ldots, a_5)$ where a_0 and a_1 are the two redundant symbols. The encoding rule is as follows.

$$a_0 + a_1 + \cdots + a_5 \equiv 0 \pmod{31} \quad (1)$$
$$a_1 + 2a_2 + \cdots + 5a_5 \equiv 0 \pmod{31} \quad (2)$$

As example we take CODE, which is the sequence 3,15,4,5. The second equation gives us $a_1 + 2\cdot 3 + 3\cdot 15 + 4\cdot 4 + 5\cdot 5 \equiv a_1 + 30 \equiv 0 \pmod{31}$,
so $a_1 = 1$ and substitution in the first congruence then yields $a_0 = 3$. So the two redundant symbols are C and A, i.e. CODE is mapped to CACODE =3,1,3,15,4,5.

Let us now look at what the receiver does. Suppose the six-tuple WXPART is received. At first glance it looks like PART with two redundant symbols in front. However, substitution in (1) yields

$$c_0 + c_1 + \cdots + c_5 \equiv 9 \pmod{31} \quad (3)$$
$$c_1 + 2c_2 + \cdots + 5c_5 \equiv 14 \pmod{31} \quad (4)$$

We see that one or more errors have occurred. Since one error is the most likely, we try that first. From the first congruence we see that one of the six integers is 9 larger than it should be. In the second congruence the error is multiplied by the position in which it occurs. Since $14 \equiv 45 = 5\cdot 9 \pmod{31}$ we see that the error has occurred in position 5. So, the number 20 (corresponding to T) should be reduced by 9 to 11, which corresponds to the letter K. Now we can remove the two redundant symbols to find the correct word PARK. Next, suppose we receive WYPART. The two congruences of (1) and (2) now yield 10, respectively 15. The multiples $10i$ with $0 \leq i \leq 5$ are 0,10,20,30,9, and 19. The second outcome (=15) is not the expected multiple of 10. We therefore know that this word contains at least two errors. We cannot correct the two errors.

Consider the example of transmitting the printed page. It has about 3000 symbols. We take the probability of error (per symbol) to be 0.5 %. So, without coding, we expect about fifteen misprints on the page, a bad result if we keep the original example of the CD in mind (fifteen ticks on one record is not pleasant listening!). Now we use our [6,4,3] code over $\mathbb{Z}_{31}$. Because the information rate is 2/3, we now must transmit 4500 symbols. If this is done with the same transmitter power, the probability of error doubles! Note that the same problem occurs on the CD. To put 4/3 times as many bits on the disc without making it larger, the bits become smaller and the probability that errors (e.g. caused by small particles) occur increases. So, when we transmit the page, the receiver gets a message with about 45 incorrect symbols. Luckily, a number of errors can be corrected, namely in all cases where a six-tuple contains only one error. The probability that a received six-tuple contains no error or just one is $(0.99)^6 + 6 \cdot (0.01)(0.99)^5 \approx 0.99854$. Since we have transmitted 750 six-tuples, we can expect that one of them is received with two or more errors and the rest will be correct, quite an improvement. But that one (loud) tick on the CD is still too much.

We will try another code but because of the problem discussed above, we take one with the same information rate. We now split the message into eight-tuples and call these $(a_4, a_5, \dots, a_{11})$. We shall give rules that specify four redundant symbols a_0 to a_3, again in front of the other eight. The rules are $0^k \cdot a_0 + 1^k \cdot a_1 + 2^k \cdot a_2 + \cdots + 11^k \cdot a_{11} \equiv 0 \pmod{31}$, where $0 \le k \le 3$. This gives us four congruences from which we can determine the redundant symbols. It can be shown that we now have a two error-correcting code (and the CD uses exactly the same kind of code with its larger alphabet of 256 symbols). Like we did above, we can calculate the probability that a received twelve-tuple contains more than two errors. It is about 0.02%. Since each page consists of 375 twelve-tuples the probability that one of them is wrong is now small.

Problem 9
Suppose a twelve-tuple is received and the results of the substitutions into the four defining congruences yield 0,6,11,and 17. If we assume that an error of size e_i has occurred in position i and one of size e_j in position j, we have the four equations
$i^k \cdot e_i + j^k \cdot e_j \equiv$ respectively $0, 6, 11, 17,$ for $k = 0, 1, 2, 3$. Solve these to find the positions of the two errors and their size.

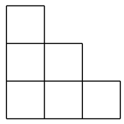
There is a lot more fascinating mathematics in the CD but this section is enough as an introduction.

5. Miscellaneous Problems

Problem 1
Let a and b be vertices of a graph G. We wish to start a walk along the edges of G in a and to end in b having used every edge exactly once. Give necessary and sufficient conditions for this to be possible.

Problem 2
A cube of cheese of size $3 \times 3 \times 3$ is divided into 27 cubes. A mouse wishes to eat the cubes, one per day. Each day he wishes to eat a cube adjacent to the one he ate the day before. Can he start on the outside and eat the central cube on the last day?

Problem 3
The number of squares in a configuration like

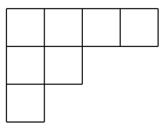


is called a triangular number $T(n)$, where n is the number of squares in the bottom row. So $T(1) = 1$, $T(2) = 3$, $T(3) = 6$ etc. Find a formula for $T(n)$

(i) by induction,

(ii) by using two copies of the picture.

Problem 4
A partition of n into k parts is a sequence $t_1 \le t_2 \le \cdots \le t_k$ with $t_1 + t_2 + \cdots + t_k = n$. A picture of one partition of 7 into 3 parts $1, 2, 4$ is:



Prove that the number of different partitions of n into k parts equals the number of partitions into parts, the largest of which is k.

Problem 5
We can depict the assertion $1+3+2=6$ as $o|ooo|oo \to 6$. How many solutions does the equation

$$x_1 + x_2 + x_3 + x_4 + x_5 = 10$$

have

(i) with integers $x_i \ge 0$,

(ii) with integers $x_i \ge 1$?

Literature

[1] L. Lovasz, J. Pelikan, K. Vesztergombi, *Discrete Mathematics, Elementary and Beyond*, Springer, New York etc. 2000.

[2] David M. Burton, *Elementary Number Theory*, Mc Graw Hill, Boston etc., 2002.

[3] Joseph Kirtland, *Identification Numbers and Check Digit Schemes*, Math. Assoc. of America, 2001.

[4] Thomas Koshy, *Elementary Number Theory with Applications*, Harcourt/Academic Press, 2002.

[5] R. Hill, *A First Course in Coding Theory*, Clarendon Press, Oxford, 1986.

Authors

Ian Anderson, Department of Mathematics, University of Glasgow, University Gardens, Glasgow G12 8QW, United Kingdom
Email: i.anderson@maths.gla.ac.uk

Bram van Asch, Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands
Email: a.g.v.asch@tue.nl

Jack van Lint, Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands
Email: j.h.v.lint@tue.nl