CODES CORRECTING ERRORS 1-5

ANTONI PIERZCHALSKI

1. Introduction: Three Youtube Presentations

Error correcting codes 1
https://youtu.be/eixCGqdlGxQ

How to send a self-correcting mesage (Hamming codes)
https://youtu.be/X8jsijhlllA

Hamming codes, part 2, the elegance
https://youtu.be/b3NxrZOu_CE

2. Algebraic structures

2.1. **Group.**

A *group* is a set G with an algebraic operation

$$\cdot : G \times G \to G$$

such that the following three axioms are satisfied:
- associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \quad a, b, c \in G$,
- the neutral element: there is $e \in G$ such that for any $a \in G \;\; e \cdot a = a \cdot e = a$,
- the inverse element: for any $a \in G$ there is $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

If additionally the following fourth axiom is satisfied:
- commutativity: $a \cdot b = b \cdot a, a, b \in G$

the group is called *commutative* or *abelian*.

Example 2.1 (The additive group of real numbers)**.** *$G = \mathbb{R}$ the set of real numbers with the addition $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ as an algebraic operation is an abelian group.*

Example 2.2 (The multiplicative group of real numbers)**.** *$G = \mathbb{R} \setminus \{0\}$ the set of real numbers with the multiplication $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ as an algebraic operation is an abelian group.*

Example 2.3. *For a given nonempty set X The set G of all one-to one mappings of X onto itself with the composition of mappings $\circ : G \times G \to G$ as the algebraic operation is a group called the group of permutations of X. If X has more than two elements the group is not abelian.*

2.2. **Ring.**

A *ring* is a set P with two algebraic operations

$$+ : P \times P \to P \quad \text{and} \quad \cdot : P \times P \to P$$

such that P with $+$ is an abelian group. The neutral element of this group is denoted by 0.

Moreover, the following two additional axioms are satisfied:
- *multiplication associativity*: $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \quad a, b, c \in P$,
- *multiplication distributivity*: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

Additionally:
- If the multiplication $\cdot$ is commutative, P is called *commutative*
- If there is a neutral element 1 for the multiplication, P is called a *ring with unit*
- If $a \cdot b = 0$ implies $a = 0$ or $b = 0$ for $a, b \in P$, P is called an *integral ring* or a ring *without divisors of zero.*

Example 2.4 (The ring of integers)**.** *$P = \mathbb{Z}$ is the set of integers:*

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3...\}$$

with the addition $+$ and the multiplication $\cdot$ aa algebraic operations is a ring. P is commutative, with the unit 1,and without divisors of zero.

2.3. **Field.**

A fiel K is a set with two algebraic operations

$$+ : K \times K \to K \quad \text{and} \quad \cdot : K \times K \to K$$

such that K with $+$ and $\cdot$ is a ring with the unit 1, $0 \neq 1$ and such that all its nonzero elements are invertible. More exactly:
- for any $a \in K, a \neq 0$, there is $a^{-1} \in K$ such that such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Equivalently the definition may be formulated sd follows: K with $+$ is an abelian group, $K \setminus \{0\}$ with $\cdot$ is a group, the multiplication $\cdot$ is distributive and 1 is the unit: for any $a \in K$, $1 \cdot a = a \cdot 1 = a$

Example 2.5 (The field real numbers)**.** *$K = \mathbb{R}$ the set of real numbers with the addition $+$ and multiplication $\cdot$ as an algebraic operations is a field. $\mathbb{R}$ is a commutative field. The neutral elements for $+$ and $\cdot$ are 0 and 1, respectively.*

Example 2.6 (The field real rational numbers)**.** *$K = \mathbb{Q}$ is the set of rational numbers:*

$$\mathbb{Q} = \{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$$

with the addition $+$ and multiplication $\cdot$ as an algebraic operations is a field. $\mathbb{Q}$ is a commutative field. The neutral elements for $+$ and $\cdot$ are 0 and 1, respectively. $\mathbb{Q}$ is the smallest field of numbers in the sense that if K is any field of numbers than $Q \subset K$.

3. Sets of numbers

The following sets of numbers are important from our point of view.
$\mathbb{R}$ - the set of real numbers. With the natural algebraic operations: addition and multiplication $\mathbb{R}$ is a commutative field.
$\mathbb{Q}$ - the set of rational numbers. With the natural algebraic operations: addition and multiplication $\mathbb{R}$ is a commutative field
$\mathbb{Z}$ - the set of integers. With the natural algebraic operations: addition and multiplication $\mathbb{R}$ is a commutative ring without divisors of zero.
$\mathbb{N} = \{1, 2, 3...\}$ - the set oh natural numbers.

We have then

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

4. Divisibility in the set of integers

4.1. **Division with a Remain.**

Consider the set of integers $\mathbb{Z}$. The theory of the divisibility in $\mathbb{Z}$ is founded on the following fact on decomposition of integers.

For any integer $n \in \mathbb{Z}$ and any natural number $m \in \mathbb{N}$ there are two integers q and r such that

$$n = qm + r \tag{1}$$

.

Example 4.1. *For $n = 61$ and $m = 9$ we have*

$$61 = 5 \cdot 9 + 16$$

or

$$61 = 6 \cdot 9 + 7$$

or

$$61 = 7 \cdot 9 + (-2)$$

Under the additional request,

$$0 \leqslant r < m, \tag{2}$$

the decomposition (1) is *u n i q u e*. So we have the following fundamental

Theorem 4.1 (Division with the remain)**.** *For any $n \in \mathbb{Z}$ and $m \in \mathbb{N}$ there are unique integers q and r such that*

$$n = q \cdot m + r, \quad 0 \leqslant r < m. \tag{3}$$

The integers q and r are called then the *quotient* and the *remain*, respectively.

Example 4.2.

$$71 = 7 \cdot 10 + 1, \quad -71 = (-8) \cdot 10 + 9.$$

When the remain in (3) is zero, i.e., $r = 0$ we say that m *divides* n or that n is *divisible* by m. In this case m is called a *divisor* of n.

Exercise 4.1. *Write a computer program that for any two given integers $n \in \mathbb{Z}$ and $m \in \mathbb{N}$ evaluates the quotient q and the remain r.*

4.2. **Prime numbers.**

A natural number $m \in \mathbb{N}$ is called to be *prime* if it has exactly two divisors.

Example 4.3. *To get examples of prime numbers let us list a beginning set of them*

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ... \tag{4}$$

In the essence, the three dots at the end of (7) have no reasonable meaning. It can be proved namely that there is no general formula for calculating the next prime when all the previous ones are known. In each case to check whether a given natural number n is prime, all the the possible prime numbers less or equal to $\sqrt{n}$ should be tested as possible divisors.

Example 4.4 (Eratosthenes Sieve)**.** *To get all the prime numbers p from the interval $2 \leqslant p \leqslant n$, for a given natural n, list all the natural numbers from 2 to n:*

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \dots \ n \tag{5}$$

In the first step take the first prime number from the list i.e. 2 and remove from the list all its nontrivial multiplicities, namely 4,6,8,....The remianing list will be following:

$$2, 3, 5, 7, 9, 11, 13, \dots \ n \tag{6}$$

In the second step remove from the list all the nontrivial multiplicities of the second prime number i.e. 3. The remaining list will be following:

$$2, , 5, 7, 11, 13, \dots \ n \tag{7}$$

Continue the procedure up to to the moment all the nontrivial multiplicities of the sequential primes less then $\sqrt{n}$ will be used. Then the remaining list will be the complete list of primes for the given interval.

Generally if n is really big this is an extremely difficult task, even for the strongest computers. And the point is that this difficulty has the advantage that it can be successfully used in cryptography for constructing ciphers that are extremely difficult to be broken. A beautiful example is one of the most powerful cipher: RSA. The cipher will be described later.

Exercise 4.2. *Write a computer program that for any given natural number $n \in$ (not necessarily very big) realizes the Eratosthenes sieve.*

4.3. **Decomposition into Primes.**

It can be proved that any natural number greater then 1 is or prime or a product of primes. In each case we have the following:

Theorem 4.2 (Prime product decomposition)**.** *For any $n \in \mathbb{N},\ n > 1$, there is a natural number s, prime numbers $p_1 < \cdots < p_s$ and the natural numbers $\alpha_1, \dots, \alpha_s$ such that*

$$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s} \tag{8}$$

Moreover, with the above assumption, the formula (8) is unique!

Example 4.5. *For $n = 3240$ we have the following decomposition into primes*

$$3240 = 2^3 \cdot 3^4 \cdot 5^1$$

.

From the Theorem if follows directly the following

Corollary 4.1. *For a given n (written in the form (8)), the number m is a divisor of n if and only if it is of form*

$$m = p_1^{\beta_1} \cdots p_s^{\beta_s} \tag{9}$$

where

$$0 \leqslant \beta_1 \leqslant \alpha_1 \ldots 0 \leqslant \beta_s \leqslant \alpha_s. \tag{10}$$

.

An then the next one

Corollary 4.2. *For a given n (written in the form (8)) the number $\theta(n)$ of all its divisors is equal to*

$$\theta(n) = (\alpha_1 + 1) \cdots (\alpha_s + 1) \tag{11}$$

In particular

$$\theta(p^\alpha) = \alpha + 1$$

Example 4.6. *The number*

$$72 = 2^3 \cdot 3^2$$

has exactly $\theta(72) = 4 \cdot 3 = 12$ divisors, namely:

$$1 = 2^0 \cdot 3^0, \quad 2 = 2^1 \cdot 3^0, \quad 4 = 2^2 \cdot 3^0, \quad 8 = 2^3 \cdot 3^0,$$
$$3 = 2^0 \cdot 3^1, \quad 6 = 2^1 \cdot 3^1, \quad 12 = 2^2 \cdot 3^1, \quad 24 = 2^3 \cdot 3^1,$$
$$9 = 2^0 \cdot 3^2, \quad 18 = 2^1 \cdot 3^2, \quad 36 = 2^2 \cdot 3^2, \quad 72 = 2^3 \cdot 3^2$$

Exercise 4.3. *Write a computer program that for any given natural number $n \in \mathbb{N}$ (not necessarily very big) gives the decomposition n onto primes.*

Exercise 4.4. *Write a computer program that for any given natural number $n \in \mathbb{N}$ (not necessarily very big) lists all the posible natural divisors of that number.*

4.4. **The Greatest Common Divisor.**

For two given natural numbers m and n the nonempty set of their common divisors is finite. So it has the (exactly one) greatest element. This element is called *the greatest common divisor* and denoted by $\gcd(m, n)$ or shortly by (m, n).

Example 4.7. *For*

$$m = 16200 = 2^3 \cdot 3^4 \cdot 5^2, \quad n = 7875 = 3^2 \cdot 5^3 \cdot 7^1$$

we have

$$\gcd(m, n) = \gcd(16200, 7875) = 3^2 \cdot 5^2 = 225.$$

The greatest common divisors for some more then two natural numbers is defined and denoted similarly.

Exercise 4.5. *Write a computer program that for any two given natural numbers $m, n \in \mathbb{N}$ (not necessarily very big) evaluates* $\gcd(m, n)$.

4.5. **Relatively Prime Pairs of Numbers.**

Two natural numbers $m, n \in \mathbb{N}$ are called relatively prime if their greatest common divisor equals 1, i,e. $\gcd(m, n) = 1$.

Example 4.8. *Take $m = 16200 = 2^3 \cdot 3^4 \cdot 5^2$ and $n = 539 = 7^2 \cdot 11^1$. The two decompositions into primes have no common prime factor, so* $\gcd(16200, 539) = 1$

The following important criterion for two numbers being relatively prime can be proved.

Theorem 4.3. *Two natural numbers $m, n \in \mathbb{N}$ are relatively prime if and only if there are two integers $p, q \in \mathbb{Z}$ such that*

$$p \cdot m + q \cdot n = 1. \tag{12}$$

Some powerful consequences of the theorem will be presented later when the inverse elemts in the modular rings $\mathbb{Z}_p$ will be searched.

Example 4.9. *For $m = 16200 = 2^3 \cdot 3^4 \cdot 5^2$ and $n = 539 = 7^2 \cdot 11^1$. considered in the previous example we have that*

$$18 \cdot 16200 + (-541) \cdot 539 = 1.$$

So $p = 18$ and $q = -541$.

Exercise 4.6. *Write a computer program that for any pair of two given relatively prime numbers $m, n \in \mathbb{N}$ (not necessarily very big) evaluates the coefficients p and q from (12).*

Hint: use the Euclidenan Algorithm from the next section.

5. The Euclidean Algorithm

Recal that, by the theorem on division with remain, for any two natural numbers $n, m \in \mathbb{N}$ we have the following unique decomposition

$$n = q \cdot m + r, \quad 0 \leqslant r < m. \tag{13}$$

The idea that enables the construction of the famous and powerful *Euclidean Algorithm* is following:

Looking at the relation (18) We can easily see that if a number $d \in \mathbb{N}$ is divisor of both m and r then it is a divisor of n and then d is a divisor of both n and m. Conversly, rewritting (18) as

$$r = n - q \cdot m, \quad 0 \leqslant r < m. \tag{14}$$

we can see similarly that any divisor of both m and r is a divisor of both n and m.

Consequently, the two pairs of numbers

$$n, m \quad \text{and} \quad m, r$$

have the same sets of common divisors so, in particular, they have the same greatest common divisor, namely:

$$gcd(n, m) = gcd(m, r). \tag{15}$$

Notice yet that we have additionally that

$$m < n \quad \text{and} \quad r < m.$$

That way, we reduced the problem of finding "gcd" for a given pair of numbers to the problem of finding "gcd" for a pair of numbers that are essentially smaller. Of course, we can repeat the procedure and continue it to get, as a result, the *complete euclidean algorithm sequence*.

To describe it more precisely lest us start with a pair of natural numbers r_0 and r_1. Then, step by step, we obtain inductively the following sequence of divisions with rest:

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ &\cdots \\ r_{s-2} &= q_{s-1} r_{s-1} + r_s \\ r_{s-1} &= q_s r_s + 0. \end{aligned} \tag{16}$$

Now, in an analogy to (15), we obtain the following sequence of equalities:

$$\gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{s-2}, r_{s-1}) = \gcd(r_{s-1}, r_s). \tag{17}$$

Yet, the last equality in (16) says that r_s is a divisor of r_{s-1}. Then, of course, $\gcd(r_{s-1}, r_s) = r_s$ Consequently,

$$\gcd(r_0, r_1) = r_s.$$

We can state then the following general

Conclusion 5.1. *The greatest common divisor of a pair of natural numbers r_0 and r_1 is equal to the last nonzero remain in the euclidean algorithm sequence (16) for these numbers.*

Example 5.1. *For the pair of numbers* 378 *and* 360 *we have the following euclidean algorithm sequence*

$$\begin{aligned} 378 &= 1 \cdot 360 + 18 \\ 360 &= 20 \cdot 18 + 0. \end{aligned}$$

So, $\gcd(378, 360) = 18$.

Example 5.2. *For the pair of numbers* 75 *and* 28 *we have the following euclidean algorithm sequence*

$$\begin{aligned} 75 &= 2 \cdot 28 + 19 \\ 28 &= 1 \cdot 19 + 9 \\ 19 &= 2 \cdot 9 + 1 \\ 9 &= 9 \cdot 1 + 0. \end{aligned}$$

So, $\gcd(75, 28) = 1$ *and so, the numbers* 75 *and* 28 *are relatively prime.*

Exercise 5.1. *Write a computer program that for any pair of two given numbers* $m, n \in \mathbb{N}$ *(not necessarily very big) produces the complete euclidean algorithm sequence.*

Hint: Repeat sequentially the procedure from Exercise 4.1.

Exercise 5.2. *Write a computer program that for any pair of two given numbers* $m, n \in \mathbb{N}$ *(not necessarily very big) evaluates* $\gcd(m, n)$

Hint: Just extend the procedure of the previous Exercise 5.1

6. Modular Arithmetic

Consider the set of integers

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, \dots\}$$

As we know from the example 2.4, the set $\mathbb{Z}$ with the two algebraic actions: the addition and the multiplication is a ring.

The theory of divisibility in the set of integers presented in Section 4 enables us to introduce infinitely many finite rings. Indeed, fix a natural number $m \in \mathbb{N}$.

By the theorem on division with the remain (cf 4.1) any integer n has the unique decomposition:

$$n = q \cdot m + r, \quad 0 \leqslant r < m. \tag{18}$$

One can prove that the m - element set of all the possible remainders:

$$\mathbb{Z}_m = \{0, 1, \dots, m-1\} \tag{19}$$

is also a ring with two algebraic actions $+_m$ and $\cdot_m$ defined as follows:

$$a +_m b = \text{the reamainder of division of } a + b \text{ by } m,$$

and

$$a \cdot_m b = \text{the reamainder of division of } a \cdot b \text{ by } m.$$

When m is fixed we will be writing $a + b$ and $a \cdot b$ instead of $a +_m b$ and $a \cdot_m b$, respectively.

It is clear that $\mathbb{Z}_m$ is a commutative ring with unit.

An element $x \in \mathbb{Z}_m$ is called *invertible* if there is $y \in \mathbb{Z}_m$ that $xy = 1$. Such the y is then denoted by x^{-1}.

The set of all ivertible elements from $\mathbb{Z}_m$ is denoted by $\mathbb{Z}_m^*$.

One can show the following facts.

Proposition 6.1. *$\mathbb{Z}_m^*$ with the multiplication $\cdot$ is a group.*

Proposition 6.2. *An element $x \in \mathbb{Z}_m$ is ivertible if and only if $\gcd(x, m) = 1$ i.e., if and only if x and m are relatively prime.*

As a conclusion from the last two propositions we have that $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{0\}$ if and only if m is a prime number what, other words, can be formulated as the following

Theorem 6.1. *The ring $\mathbb{Z}_m$ is a field if and only if m is a prime number.*

Exercise 6.1. *List all invertible elements in $\mathbb{Z}_{24}$.*

Exercise 6.2. *Evaluate $5^{-1}, 11^{-1}, 23^{-1}$ in $\mathbb{Z}_{24}$.*

Exercise 6.3. *Solve the following equations in $\mathbb{Z}_{24}$*

$$5x + 10 = 12, \tag{20}$$

$$11x + 1 = 15, \tag{21}$$

$$23x + 6 = 18. \tag{22}$$

Exercise 6.4. *Evaluate $3^{-1}, 7^{-1}, 9^{-1}$ in $\mathbb{Z}_{10}$.*

Exercise 6.5. *Solve the following equations in $\mathbb{Z}_{10}$*

$$3x + 8 = 9, \tag{23}$$

$$7x + 1 = 6, \tag{24}$$

$$9x + 6 = 4. \tag{25}$$