Mathematical Institute
Slovak Academy of Sciences, Bratislava

Preprint 14/1999

Otakar Grošek
Ladislav Satko
Karol Nemoga

ZKDWCNDPDC...

August 13, 1999

PREPRINT SERIES

ZKDWCNDPDCVXWUDCGLGCVXJJHVWHG

...

Otokar Grošek and Ladislav Satko *
Department of Mathematics
Slovak University of Technology
812 19 Bratislava, Slovakia
e-mail: grosek/satko@kmat.elf.stuba.sk

and

Karol Nemoga †
Institute of Mathematics
Slovak Academy of Sciences
814 73 Bratislava, Slovakia
e-mail: nemoga@savba.sk

Dedicated to our respective colleague and friend
ZDENKA RIEČANOVÁ
on the occasion of her 65

*This work was supported by VEGA grant 1/4289/97
†This work was supported by VEGA grant 5123/99

Abstract

The earliest frequently known use of a substitution technique is one in which each letter of plaintext is replaced with the letter standing three places further down the alphabet. When we use the alphabet $\mathcal{P} = \{\sqcup, a, b, c, \ldots, w, x, y, z,\}$, and apply this method of ciphering to the plaintext

what kama sutra did suggested...

we get the title of this article... In these few pages we would like to introduce a very attractive branch of mathematics as well as of computer science called cryptology. Our aim is to introduce to a freshman in the field some basic ideas leading to the three methods of ciphering: classical, block and asymmetric ciphers.

1. What Caesar really did two thousand years ago

The Roman emperor Julius Caesar did not like to have his written messages to be red. Thus he decided to use a new idea: any message (now called **plaintext**) written in the alphabet $\mathcal{P} = \{\sqcup, a, b, c, \ldots, w, x, y, z,\}$ will be written in the same alphabet due to the following transformation:

$$\begin{array}{ccccccccccccccccccccccccccc}
\sqcup & a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z & \sqcup & A & B
\end{array}$$

Diagram 1. Caesar's cipher applied to the alphabet $\mathcal{P}$.

The resulting message (now called **ciphertext**) was totally unreadable for a person not familiar with the transformation... up to the moment when Cicero, a former ally, did not move to adversaries! Now, you also do not need a help of Cicero if you would like to know the title of this article.

Well, what to do now, if we would like to design a new system for making our messages secret. We do not trust Caesar's system because of this, and many others articles which treat it, providing many people know it. Hence we must start to analyse this system and find all common features for such methods. Below we list the first of them:

1. Plaintext is written in the lowercase alphabet $\mathcal{P}$, including space $\sqcup$ - the most frequent letter in all languages.[1]

[1] Have a look at your keyboard, which key is the largest!

2. Ciphertext is written in the uppercase alphabet $\mathcal{C}$, including space $\sqcup$. Here we use different alphabets in order to better distinguish plaintext and ciphertext. In fact these alphabets are the same.

3. There is a one-to-one **encryption** mapping

$$e_k : \mathcal{P} \to \mathcal{C}$$

depending on a secret parameter k called the **key**. In the case of above mentioned mapping the key is a cyclic shift of the alphabet three places further down.

4. The key k belongs to a keyspace $\mathcal{K}$. As we will see later, specification of keyspace gives the name to different methods. The larger is the $\mathcal{K}$, the secure is the method. But this is a necessary condition only!

5. To be able to read a message the used mapping e_k must be reversible. It means that there exists an inverse mapping

$$d_k : \mathcal{C} \to \mathcal{P}$$

such that $d_k(e_k(x)) = x$. Both **sender** as well as **receiver** use the same secret key and the same encryption as well as decryption mappings, i.e. the same e_k, d_k.

6. Caesar's system maps a single letter of plaintext to a single letter of ciphertext using a **substitution**. Such a system is called **monoalphabetic**.

The history of ciphering is very old. There are many true stories which are very popular among the folk all over the world. As a rule there are also those which could be classified as legends. We do not like to carry coals to Newcastle and simply recommend one of the best books in this field [**?**]. As a proof that ciphering is known from a very old past we mention except of Gaius Julius Caesar (100–44 B.C.) only two examples:

- A very similar idea of that of Caesar is known from Book of Jeremiah, a part of the Old Testament. In 587 B.C. Babylonians conquered Judah, destroyed the Temple, and took many Jews to Babylonia as prisoners. This period, called also the Babylonian Exile, lasts up to 539 B.C. when King Cyrus of Persia conquered Babylonia. Among taken Jews there was also a prophet Jeremiah who continued as prophetic voice during the fall of the kingdom of Judah. Now we would name him as *a dissident* in Babylon. Namely in 25:26 and 51:41 he criticizes the emperor of Sheshah (not of Babel). The reason is probably that he was afraid and thus used an old hebrew system of ciphering called **atbash**. In this system the first letter is substituted by the last one, the second by last but one, etc. as shown on Diagram 2. Applying this to the old Hebrew alphabet we get $babel \rightarrow (SH)E(SH)AH$.

$$\begin{array}{ccccccccccccccccccccccccccc} \sqcup & a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ Z & Y & X & W & V & U & T & S & R & Q & P & O & N & M & L & K & J & I & H & G & F & E & D & C & B & A & \sqcup \end{array}$$

Diagram 2. Atbash cipher applied to the alphabet $\mathcal{P}$.

The title of this paper is then

$$CRYFZOYMYGEFHYZVQVZGESSUGFUV$$

- In a brilliant book about the mystery of love between a man and woman, formerly written in Sanskrit about 100 B.C. [**?**] one can read: If a girl would like to be perfect in the art of love she must know and practice these 64 arts: 1. to sing, 2. to play musical instruments, …, 43. to know secret writing and secret characters, 44. to know various secret ways of talking, …

  Of course, communication to men is not prohibited, and thus this knowledge has been recommended to all… Following this suggestion we decided to split an introduction to this art among readers of these pages. This is also the origin of the title of our contribution.

2. Some facts from modular arithmetics and finite fields

In this section we explain some basic facts from number theory and theory of finite fields. For more details we recommend the book [**?**, **?**].

2.1. New arithmetics

On the set of real numbers $\mathbb{R}$ there are defined two operations with their inverses: addition/subtraction and multiplication/division. This enables to solve any equation $ax+b=0$ uniquely. Now, for a given integer $m>1$ we define a new arithmetics on the set $\mathbf{M}=\{0,1,2,\dots,m-1\}$. This arithmetics works as follows:

If $a,b\in\mathbf{M}$ then

1. Add a and b as usual, then divide the sum by m, and the result is the residuum r: we write $a + b \equiv r \pmod{m}$.
2. Multiply a and b as usual, then divide the product by m, and the result is the residuum r: we write $ab \equiv r \pmod{m}$.

It is a mater of theory that these two new operations are commutative, associative, and also the distribution law $c(a + b) \equiv ca + cb \pmod{m}$ is valid. In mathematics we use for the set $\mathbf{M}$ equipped with such an arithmetics notation Z_m. If we use multiplicative structure only, then we write S_m. The number m is called *modulus*. There is a very rich theory around this arithmetics studied also by ancient Greeks and Chines. We mention only some facts necessary to understand the article.

First of all, the equation $ax + b \equiv 0 \pmod{m}$ has a solution in Z_m if and only if $\gcd(a, m) = 1$. At the same time there exists the multiplicative inverse of a written as a^{-1} such that $aa^{-1} \equiv 1 \pmod{m}$.

The number of elements of Z_m such that there exists a multiplicative inverse is the number of all elements of $\mathbf{M}$ co-prime with the modulus m. This number is given by Euler function φ. For $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, p_i-different primes, we have

$$\varphi(m) = \begin{cases} 1 & \text{if } m = 1, \\ p_1^{\alpha_1} - p_1^{\alpha_1 - 1} & \text{if } r = 1, \\ \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \dots \varphi(p_r^{\alpha_r}) & \text{in other cases.} \end{cases}$$

Particularly, $\varphi(p) = p - 1$.

Without going into details, how to find multiplicative inverses, we only mention that except of trying all possibilities there is an effective method called Euclid Algorithm. Besides, for study purposes we recommend the WINDOWS scientific calculator for doing modular arithmetics. If you need an inverse of, say $14 \pmod{27}$ you must use a more sophisticated package like MAPLE, DERIVE, MATHEMATICA. They all have built in functions for calculating $1/14 \pmod{27}$. The displayed result will be 2 since $2 \times 14 = 28$ and after division by 27 the residuum is 1.

2.2. Groups and Semigroups

Let us assume a finite set G equipped with one binary operation $*$, i.e. to any $a, b \in G$ there is uniquely assigned their product $a * b \in G$. If not specified we call it multiplication. Let $G = \{1, 2, 3, 4, 5\}$. Then we can arrange a multiplication tables like Table 1a, 1b:

G_1	1	2	3	4	5
1	3	1	2	4	5
2	2	3	1	5	4
3	5	4	3	2	1
4	1	5	4	3	2
5	4	2	5	1	3

G_2	1	2	3	4	5
1	1	2	3	4	5
2	2	3	4	5	1
3	3	4	5	1	2
4	4	5	1	2	3
5	5	1	2	3	4

Tab. 1a – 1b

We also call them *Calley tables.* Moreover, any pair of equations

$$a * x = b, \quad y * a = b$$

with unknowns x and y have exactly one solution in these examples. (Do you know how to find it using Tab. 1a – 1b?) It can be proved that multiplication table with such property is necessarily so called *Latin square*, i.e. in each row and column there is a permutation of elements of G.

Among these two tables there is one important difference. While multiplication in Tab 1b is associative, i.e. $(a * b) * c = a * (b * c)$ for any $a, b, c \in G_2$, this is not true for G_1. (Try for $a = 2, b = 3, c = 4$.)

Any Latin square assuming as a multiplication rule for including elements with associative multiplication defines a structure which is known as a *group.* It can be proved, that in such a special Latin square

1. There always exists an element 1 satisfying relation $a * 1 = 1 * a = a$ for all $a \in G$;
2. To any $a \in G$ there exists the unique solution $x = y$ for $a * x = 1, \quad y * a = 1$. This solution is called the multiplicative inverse to a, $x = a^{-1}$;
3. In addition, if the Latin square is symmetric according to the main diagonal, than this operation is commutative, i.e. $a * b = b * a$.

Without going into details we present 3 Examples.

Example 1. *Let p be a prime. Then $S_p \setminus \{0\}$ is a group.*

Example 2. *Let m be arbitrary integer. Then $\mathbf{M} = \{0, 1, 2, \ldots, m-1\}$ with operation $+ \pmod m$ is the group.*

Example 3. *Let m be a composite integer. Then S_m is not a group. There are many reasons why it is so. First of all equation $0 * x = 0$ has as its solution arbitrary $x \in S_m$. Secondly, the equation $a * x = b$ has a solution if and only if a and m have no common divisor except of 1.*

Number of elements of the group G denoted by $|G|$, is called the *order of* G. It can be proved that for any $a \in G, \quad a^{|G|} = 1$. In fact, $|G|$ need not be the smallest exponent r such that $a^r = 1$. The smallest exponent with this property is called the order of a. Clearly r divides $|G|$.

In some cases it is worth to study a set G equipped with a multiplication which is associative only. If this is the case, Cayley table does not possess in rows/columns only permutations. Such algebraic structure is called a *semigroup*. It turns out that the set $\mathbf{M}$ with addition $\pmod m$ is a group, S_m with multiplication $\pmod m$ a semigroup.

It is possible, that a semigroup contains a subset which is itself a group. This is also the case for S_m. It is known, that multiplicative inverses do exist for a co-prime to m only. Let $G(1)$ be the set of all such elements co-prime to m. The cardinality of $G(1)$ is $\varphi(m)$. All elements of $G(1)$ satisfy associative law (since they belong at the same time to S_m), all have the unique multiplicative inverse. Hence $G(1)$ is a group referred to as the *group of units*. Moreover, for any $a \in G(1)$ the relation $a^{\varphi(m)} = 1$ is valid, a result known as Euler – Fermat Theorem.

2.3. Finite fields

As we have already mentioned in the two previous subsections, the structure of Z_m is more rich than a group, or semigroup. It possess two binary operations: with the addition it forms a group, and with multiplication a semigroup. Moreover, these two operations are connected by distribution law. Such a structure is called in abstract algebra a *ring*. Perticularly, for m prime $S_m \setminus \{0\}$ is also a group. Then it is called a *finite field*. Almost all theory known for real numbers can be transmitted to such a structure. More precisely, transferable are results for roots of polynomials. A very important result in this theory says that there are only special types of finite fields $\mathbb{F}_q$ with q elements. All finite fields Bbb F_q with q elements are isomorphic (roughly speaking, are the same). Moreover, q is a power of a prime, and for each prime p and integer n there exists a finite field Bbb F_q with $q = p^n$ elements. We emphasize that a construction of the field with $p^n, n > 1$ elements is more sophisticated than that for $n = 1$.

A polynomial $f(x)$ of the degree d over a field $\mathbb{F}_q$ is an expression

$$f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0, \quad a_i \in \mathbb{F}_q.$$

For, if $x \in \mathbb{F}_q$ then $f(x) \in \mathbb{F}_q$. Clearly, we have q choices for all a_i, i.e. q^{d+1} different polynomials of the degree d. But some of them are the same in the sense that $f(x) = g(x)$ for all $x \in \mathbb{F}_q$. It means that $f(x)$ and $g(x)$ may differ as polynomials, but they are identical as mappings from Bbb F_q to Bbb F_q.

3. Why to study permutations

A permutation of different objects is the notion known from high school mathematics. It is an arrangement of them from a basic one to another one. We used them also in multiplication tables for groups in subsection 2.2. Hence cipher systems described on Diagrams 1 and 2 can be viewed as permutations on the set $\mathbf{M} = \{0, 1, 2, \ldots, 26\}$. It is well known that there are altogether $27! = 1.09 \times 10^{28}$ such different permutations, i.e. different one-to-one mappings on $\mathbf{M}$, i.e. different ways of encryptions. But how to choose one of them, and how one can keep this secret mapping. To keep it as a look up table is very impractical even in a computer. One possible way is to make it dependent on a secret parameter, the key k.

Since permutations are functions which map the set $\mathbf{M}$ onto itself, $\pi : \mathbf{M} \to \mathbf{M}$, we can compose them as functions. This composition can be viewed as a special operation, and let us call it multiplication $\circ$. Denoting by γ and α, respectively the Caesar and Atbash cipher, we get two new examples of these mappings. Here we do not distinguish between $\mathcal{P}$ and $\mathcal{C}$). The direct calculation for u gives

$$\gamma(u) = x, \quad \alpha(x) = b \Rightarrow \alpha(\gamma(u)) = b$$

and

$$\gamma(\alpha(u)) = \gamma(e) = h,$$

hence $\alpha \circ \gamma \neq \gamma \circ \alpha$. Moreover, it is readily seen that if β is another permutation, then $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$. Summarizing:

Let $\mathfrak{G}$ be the set of all permutations on the finite set $\mathbf{M}$ with the binary operation $\circ$. Then

1. binary operation $\circ$ is associative, i.e. the resulting permutation from three distinct ones does not depend on brackets;
2. binary operation $\circ$ is not commutative, i.e. the resulting permutation from two distinct ones does depend on its order;
3. there exists identity permutation ι which maps any element of $\mathbf{M}$ to itself;
4. to any permutation π there exists the unique inverse permutation π^{-1} such that $\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = \iota$. The inverse permutation is given by a simple rule: if for $m_1, m_2 \in \mathbf{M}$, $\pi(m_1) = m_2$, then $\pi^{-1}(m_2) = m_1$.

The structure ($\mathfrak{G}$,$\circ$) is a noncommutative finite group called *symmetric group*. Thus, a monoalphabetic encryption rule is nothing else like an element from this very large group. Moreover, one can use an encryption chaining: to choose two or more such permutations, and apply them iteratively. If we choose permutations of "the same type", we may get a subset of $\mathfrak{G}$, which is a group itself. Then we are speaking about a subgroup of $\mathfrak{G}$. Particularly, if π is an arbitrary permutation, then the set of powers of π, $\pi \circ \pi = \pi^2, \pi^3, \ldots$ forms a cyclic subgroup generated by π. This group, the subgroup of $\mathfrak{G}$ must be also finite, i.e. there is a power d such that $\pi^d = \iota$.

Up to now we do not have a binary operation on the set $\mathbf{M}$. Next we will see that involving special operations will allow us to distinguish some ciphering systems.

Next we present three such special examples.

3.1. Caesar shift

There was nothing special to shift a letter by three down. We may speak generally about a shift of k letters down. This is a permutation γ_k defined by

$$\gamma_k(x) \equiv x + k \pmod{27} \quad \text{for all} \quad x, k \in \mathbf{M} \tag{1}$$

One can easily verify that $\gamma_k = \gamma_1^k$, and $\gamma^{27} = \iota$. Really, for $k = 2$ for instance, we have

$$\gamma_1^2(m) = \gamma_1(\gamma_1(m)) = \gamma_1(m+1) = (m+1) + 1 = m + 2 = \gamma_2(m).$$

Moreover, $\gamma_k \circ \gamma_l = \gamma_{k+l \pmod{27}}$, and thus we may say that Caesar shifts C form a very small subgroup of $\mathfrak{G}$. It consists of 27 elements (permutations) only. The unique inversion (deciphering) permutation for γ_k is γ_{27-k}.

3.2. Affine Cipher

This is another classical and very simple ciphering system, given by the formula

$$\alpha_{a,b}(x) \equiv ax + b \pmod{27} \text{ for all } x, a, b \in \mathbf{M}, \quad \gcd(a, 27) = 1. \quad (2)$$

Recall, that condition $\gcd(a, 27)$ is needed for the existence of the inverse permutation (for the unique deciphering). One can do an exercise that the composition of two affine ciphers is again an affine cipher. Affine ciphers form a little bigger subgroup A of $\mathfrak{G}$. It consists of $27 \times \varphi(27) = 27 \times 18 = 486$ elements (permutations, 27 choices for b, $\varphi(27) = 18$ choices for a). Still not too much… The unique inverse permutation to $\alpha_{a,b}$ is $\alpha_{a^{-1}, 27-a^{-1}b}$.

Example 4. *Let $\alpha_{2,1}(x) \equiv 2x + 1 \pmod{27}$ be an encryption rule. Then $2^{-1} \equiv 14 \pmod{27}$, and $\alpha_{2,1}^{-1} = \alpha_{14,13}$*

Another question is to find the order of the cyclic subgroup of A generated by $\alpha_{2,1}$. It is not difficult to see that

$$\alpha_{2,1}^d(x) = 2^d x + 2^d - 1 \pmod{27}.$$

If $2^d \equiv 1 \pmod{27}$, i.e. due to Euler–Fermat theorem $d = \varphi(27) = 18$, then $\alpha_{2,1}^d(x) = x \pmod{27}$. Hence the order of this permutation is 18, or after 18 encryptions we will have the initial letter.

The Atbash system from Diagram 2 is an affine cipher with parameters $a = b = 26$. It is clear, that C is a proper subgroup of A.

3.3. The power permutation

Since this example has a very serious application in so called RSA algorithm, we discuss it in general. For the semigroup S_m this permutation is given by

$$\pi_s(x) \equiv x^s \pmod m \quad \text{for all} \quad x \in S_m. \tag{3}$$

1. Let λ denotes the Carmichael function defined for $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ by

$$\lambda(m) = \begin{cases} 1 & \text{if } m = 1, \\ 2^{\alpha-2} & \text{if } m = 2^\alpha,\ \alpha > 2, \\ \varphi(m) & \text{if } m = 2, 4, p^\alpha \text{ with } p \text{ an odd prime}, \\ \operatorname{lcm}\{\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \dots, \lambda(p_r^{\alpha_r})\} & \text{in other cases.} \end{cases}$$

   Then there are two necessary and sufficient conditions for m such that π_s be a permutation on S_m [?]: m is squarefree, and $\gcd(s, \lambda(m)) = 1$. Moreover in this case, by Proposition 6,4 in [?] the group P of all power permutations π_s of S_m is isomorphic to the group of units of $S_{\lambda(m)}$. Hence $\pi_s = \pi_{s+\lambda(m)}$ and the period $\lambda(m)$ cannot be replaced by a smaller number.

2. Recall also the *global Euler–Fermat theorem* [?]: For any $x \in S_m$ we have $x^{\max \alpha_i + \lambda(m)} = x^{\max \alpha_i}$ and the period $\lambda(m)$ cannot be replaced by a smaller number.

Example 5. *Since $m = 27 = 3^3$ is not a squarefree number, there is no such permutation on S_{27}.*

If $m = 26 = 2 \times 13$, then $\lambda(26) = 12$, $\gcd(s, 12) = 1$ gives $s = 1, 5, 7, 11$, the same set as $G(1)$ of S_{12}.

When $m = pq,\ p, q \neq 2-$ primes, then $\lambda(m) = \operatorname{lcm}(p-1, q-1)$, and for all s such that $\gcd(s, \operatorname{lcm}(p-1, q-1)) = 1$, π_s is a permutation on S_m. Moreover, the cardinality of the group of units $G(1)$ of $S_{\lambda(m)}$ is $\varphi(\lambda(m))$, there is precisely the same number of such different permutations.

3.4. Bigger subgroups

Since a composition of two permutations is again a permutation, we can define a new ciphering system by successive applying, say two of them, e.g. Caesar shift γ_k, and power permutation π_s in both orders:

$$\pi_s(\gamma_k(x)) = (x+k)^s \pmod{27} \text{ or } \gamma_k(\pi_s(x) = x^s + k \pmod{27}.$$

Moreover, given any set of power permutations, and any set of Caesar shifts yields by arbitrary composition a new permutation. All such permutations form a group PC, the smallest group generated by groups C and P respectively. Clearly, $P \subset PC, \quad C \subset PC$. All permutations belonging to the group PC have a polynomial formula.

3.5. Polynomial permutations

One might think about a polynomial function which is at the same time a permutation on Z_m. Unfortunately, only partial results have been attained so far (see below). For example, it is not difficult to prove that no second degree polynomial is a permutation for any $m > 2$.

For a given modulus m let $d \geq 1$ be the least integer such that every permutation polynomial function f is expressible in the form

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_1 x + a_0 \pmod{m}, a_i \in Z_m.$$

Then we have at most $(m-1)m^d$ such polynomials (recall $a_d \neq 0$) but exactly $m!$ different permutations. By the global Euler–Fermat theorem $d < \max \alpha_i + \lambda(m)$. Thus we have (try to do some computation and check this inequality!)

$$(m-1)m^d < (m-1)m^{\max \alpha_i + \lambda(m)}.$$

Example 6. *Let, again,* $m = 27, \lambda(27) = 3^3 - 3^2 = 18, \max \alpha_i + \lambda(m) = 21$. *Thus for all* $x \in S_{27}$ *the relation* $x^{21} = x^3$ *is valid, and* $d \leq 20$. *The number of possible permutation polynomials is bounded by* $26 \times 27^{20} = 1.1 \times 10^{30}$, *approximately 100 times more than 27!. From this estimation one may conclude a hypothesis that any permutation is of this type (see Example 7 below).*

Another choice $m = 6$ *gives* $\lambda(6) = 2, \max \alpha_i + \lambda(m) = 3$. *Thus for all* $x \in S_6$ *the relation* $x^3 = x$ *is valid, and* $d \leq 2$. *Since there is no permutation polynomial of the degree 2, we have only affine permutations. The number of such polynomials is given by* $\varphi(6) \times 6 = 18$, *a much smaller number than 6!= 720.*

Now, a small excursion to the world of real numbers will be fruitful. The problem of determining a polynomial of the degree 1 that passes through the distinct points $(x_1, y_1), (x_2, y_2)$ is the same as approximating a permutation f for which $f(x_0) = y_0$ and $f(x_1) = y_1$ by means of a first-degree polynomial agreeing with the values of f at the given points. The well known solution of this problem from high school algebra, or geometry is (check!)

$$f(x) = \frac{(x - x_1)}{x_0 - x_1)} y_0 + \frac{(x - x_0)}{x_1 - x_0)} y_1. \tag{4}$$

A similar solution for a polynomial which passes 3 points is

$$f(x) = \frac{(x - x_1)(x - x_2)}{(x_0 - x_1)(x_0 - x_2)} y_0 + \frac{(x - x_0)(x - x_2)}{(x_1 - x_0)(x_1 - x_2)} y_1 + \frac{(x - x_0)(x - x_1)}{(x_2 - x_0)(x_2 - x_1)} y_1. \tag{5}$$

The generalization for a polynomial of the degree k which passes $k + 1$ points is readily seen.

Questions which arise from switching to the world of polynomials (permutations) over the ring Z_m are not easy. It is of our interest to find conditions which will guarantee that a given permutation can be represented as a polynomial. If m is not a prime we cannot use formulas like (5), because we cannot always provide a division. Arguments $x_s = s$ for all $s \in Z_m$, and values $f(s)$ represent permutation itself. A particular solution was found by Carlitz [**?**] for the case $m = p^n$, p-prime.

Theorem 1. *Let $\mu(r)$ denote the highest power of p that divides $r!$, and $\nu(r) = \min\{\mu(r), n\}$. Let f be a function (not necessarily a permutation) given by points $(s, f(s))$ for all $s \in Z_{p^n}$. Then f can be represented by a polynomial over Z_{p^n} if and only if*

$$\Delta^r f(0) = \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} f(s) \equiv 0 \pmod{p^{\nu(r)}} \tag{6}$$

for all r, $0 \le r < p^n$.

Next we show the importance of the Theorem 1 for our Example 6.

Example 7. *Let $m = 27 = 3^3$. Then the following Table 2 displays all conditions on $f(s) = f_s$ which, if satisfied, guarantee that such a permutation can be expressed as a polynomial.*

r	$\mu(r)$	$\nu(r)$	$\Delta^r f(0) \pmod{3^{\nu(r)}}$
0	0	0	$f_0 \equiv 0$
1	0	0	$-f_0 + f_1 \equiv 0$
2	0	0	$f_0 - 2f_1 + f_2 \equiv 0$
3	1	1	$-f_0 + f_3 \equiv 0$
4	1	1	$f_0 - f_1 - f_3 + f_4 \equiv 0$
5	1	1	$-f_0 + 2f_1 - f_2 + f_3 - 2f_4 + f_5 \equiv 0$
6	2	2	$f_0 - 2f_3 + f_6 \equiv 0$
7	2	2	$-f_0 + f_1 + 2f_3 - 2f_4 - f_6 + f_7 \equiv 0$
8	2	2	$f_0 - 2f_1 + f_2 - 2f_3 + f_4 - 2f_5 + f_6 - 2f_7 + f_8 \equiv 0$
9	4	3	$-f_0 + f_9 \equiv 0$
10	4	3	$f_0 - f_1 - f_9 + f_{10} \equiv 0$
11	4	3	$-f_0 + 2f_1 - f_2 + f_9 - 2f_{10} + f_{11} \equiv 0$
12	5	3	$f_0 - f_3 - f_9 + f_{12} \equiv 0$
13	5	3	$-f_0 + f_1 + f_3 - f_4 + f_9 - f_{10} - f_{12} + f_{13} \equiv 0$
14	5	3	$f_0 - 2f_1 + f_2 - f_3 + 2f_4 - f_5 - f_9 + 2f_{10} - f_{11} + f_{12} - 2f_{13} + f_{14} \equiv 0$
15	6	3	$-f_0 + 2f_3 - f_6 + f_9 - 2f_{12} + f_{15} \equiv 0$
16	6	3	$f_0 - f_1 - 2f_3 + 2f_4 + f_6 - f_7 - f_9 + f_{10} + 2f_{12} - 2f_{13} - f_{15} + f_{16} \equiv 0$
17	6	3	$-f_0 + 2f_1 - f_2 + 2f_3 - f_4 + 2f_5 - f_6 + 2f_7 - f_8 + f_9 -$ $2f_{10} + f_{11} - 2f_{12} + f_{13} - 2f_{14} + f_{15} - 2f_{16} + f_{17} \equiv 0$
18	8	3	$f_0 - 2f_9 + f_{18} \equiv 0$
19	8	3	$-f_0 + f_1 + 2f_9 - 2f_{10} - f_{18} + f_{19} \equiv 0$
20	8	3	$f_0 - 2f_1 + f_2 - 2f_9 + f_{10} - 2f_{11} + f_{18} - 2f_{19} + f_{20} \equiv 0$
21	9	3	$-f_0 + f_3 + 2f_9 - 2f_{12} - f_{18} + f_{21} \equiv 0$
22	9	3	$f_0 - f_1 - f_3 + f_4 - 2f_9 + 2f_{10} + 2f_{12} - 2f_{13} + f_{18} - f_{19} - f_{21} + f_{22} \equiv 0$
23	9	3	$-f_0 + 2f_1 - f_2 + f_3 - 2f_4 + f_5 + 2f_9 - f_{10} + 2f_{11} - 2f_{12} + f_{13}$ $-2f_{14} - f_{18} + 2f_{19} - f_{20} + f_{21} - 2f_{22} + f_{23} \equiv 0$
24	10	3	$f_{18} - 2f_{21} + f_{24} + f_0 + f_6 - 2f_3 - 2f_9 + f_{12} - 2f_{15} \equiv 0$
25	10	3	$-f_{18} - 2f_{16} - 2f_{22} + 2f_{21} + f_{19} + f_{25} - f_{24} - f_0 - f_6 + f_1 + 2f_3 - 2f_4$ $+f_7 + 2f_9 - 2f_{10} - f_{12} + f_{13} + 2f_{15} \equiv 0$
26	10	3	$f_{18} + f_{16} - 2f_{23} - 2f_{17} + f_{22} - 2f_{21} + f_{20} - 2f_{19} + f_{26} - 2f_{25} + f_{24} + f_0$ $+f_6 - 2f_1 + f_2 - 2f_3 + f_4 - 2f_5 - 2f_7 + f_8 - 2f_9 + f_{10} - 2f_{11} + f_{12} -$ $2f_{13} + f_{14} - 2f_{15} \equiv 0$

Tab. 2 Conditions for permutation functions $\pmod{27}$.

As one can see, Theorem 1 is useless for $\nu(r) = 0$. Moreover, one of necessary and sufficient conditions for a permutation f to be expressible via a polynomial is for $r = 3$, $f(3) \equiv f(0) \pmod 3$. Thus, contrary to our hypothesis mentioned at the end of Example 6, there are nonpolynomial permutations!

Using advanced methods of number theory in Z_m it is possible to enumerate the number of all polynomial functions. Unfortunately the number of all polynomial permutation functions for some special cases only. Here is a survey of these results.

Let M_m be the number of all functions expressible as a polynomial over Z_m. The number M_m was enumerated by A. J. Kamper [?]. Another proofs were given by J. Weisenbauer [?], G. Keller and F. R. Olson [?], G. Mullen and H. Stevens [?], and others. G. Keller and F. R. Olson, G. Mullen and H. Stevens gave also the number of all permutation polynomial functions over Z_m for the case $m = p^n$.

Survey of all these results is possible to find in W. Narkiewicz book on polynomial mappings [?].

Theorem 2. *Let $N = N_m$ be the largest integer such that m does not divide $N!$. We have*

1. *if m is not a prime power then*

$$M_m = \prod_{i=0}^{N} \frac{m}{\gcd(m, N!)},$$

2. *if $m = p^k$ is a prime power, then*

$$M_n = p^{k(N+1)-s},$$

   where s is the exponent of the prime p in the canonical factorization of $\prod_{j=2}^{N} j!$.

Moreover M_m is a multiplicative function, i. e. $\gcd(m_1, m_2) = 1$ *implies*

$$M_{m_1 m_2} = M_{m_1} M_{m_2},$$

Let P_m be the number of all permutation polynomial functions over Z_m. Valuable results for the cardinality of P_m are known for $m = p^n$ only. In the case $n = 1$, Z_m has a field structure, and every function over Z_p is a polynomial function. Two polynomial functions $f(x), g(x)$ over Z_p are identical as functions if and only if $f(x) - g(x)$ is divisible by the polynomial $x^p - x$.

It means that we have p^p polynomial functions including $p!$ permutation polynomial functions over Z_p.

Formula for P_m with m prime power is due to Mullen and Stevens paper [?].

Theorem 3. *Let p be a prime, $n \geq 2$, $m = p^n$. Let N be the largest integer with $c(N) < n$, where $c(N)$ is the exponent of p in factorization of $n!$, and*

$$D = (N+1)(n - c(N)) + \delta(N) - 2p,$$

where[2]

$$\delta(n) = \frac{1}{2}\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]\left(\left[\frac{n}{p^r}\right]+1\right).$$

Then

$$P_m = p!(p-1)^p p^D.$$

If $n \leq p$ we can use more simple formula:

Theorem 4. *Let $1 < n \leq p, p$ prime, $m = p^n$. Then*

$$P_m = p!(p-1)^p p^{\frac{1}{2}p(n^2+n-4)}. \tag{7}$$

Theorems 2 and 4 enable us to compute the number of polynomial functions and polynomial permutation functions over Z_{27} exactly. (Compare with estimation in Example 6.)

Example 8. *Let N_{27} has the meaning defined above. The largest integer N such that $N!$ is not divisible by 27 is 8, providing $N_{27} = 8$. The exponent s of 3 in $\prod_{j=2}^{8} j!$ is $s = 9$.*

According to formula 2 in the Theorem 2 we have exactly

$$M_{27} = 3^{3(8+1)-9} = 3^{18}$$

different polynomial functions over Z_{27}.

According to formula 7 we have

$$P_{27} = 3!(3-1)^3 3^{\frac{1}{2}3(3^2+3-4)} = 6 \times 2^3 \times 3^{12} = 2^4 3^{13}$$

different polynomial permutation functions.

A different story is, when we define a new structure on the set **M**.

[2] $\left[\frac{a}{b}\right]$ denotes the smallest integer greater or equal to $\frac{a}{b}$.

3.6. Permutation polynomials over a field

It is clear that if f is a permutation polynomial over the field $\mathbb{F}_q,\ q = p^n$, then we can form a polynomial like (5) (recall that $1/a = a^{-1}$). Let $f(s) = f_s,\ s \in \mathbb{F}_q$. Then

$$f(x) = \sum_{s \in \mathbb{F}_q} f_s(1 - (x - s)^{q-1}), \tag{8}$$

and we prove that this is another form of this polynomial. Since $\mathbb{F}_q \setminus \{0\}$ is the multiplicative group of order $q-1$ we have $a^{q-1} = 1$ for any $a \neq 0$. Hence $f(s) = f_s$ for any $s \in \mathbb{F}_q$.

Here we mention only one result due to Hermite [**?**].

Theorem 5. *Let $d > 1$ be a divisor of $q - 1$. Then there is no permutation polynomial over $\mathbb{F}_q$ of the degree d. Particularly, since for $p > 2,\quad 2|p^n - 1$, there is no permutation polynomial of the degree 2.*

Thus we can conclude: If cardinality of $\mathbf{M}$ is a prime power, then involving the unique field structure on $\mathbf{M}$ we can express any permutation of elements of $\mathbf{M}$ via the unique polynomial. On the other hand, a polynomial over $\mathbb{F}_q$ need not be a permutation polynomial.

There is a very nice theory studying permutation polynomials over finite fields. To an interested reader we recommend the book [**?**]. Here we mention one result for $p = 3$ which is closely related to our example $q = 27$:

If we assume polynomials $f(x)$ and $f_1(x) = cf(x + b) + d,\ c \neq 0$ to be equivalent, then there is only one type of permutation polynomials, namely

$$f(x) = x^3 - ax, \quad a \text{ not a square}, \tag{9}$$

a nice simplification of (8).

4. Cryptology is a science

As we could read on the first lines of this article, secret writing is probably as old as writing in general... Vast new applications in computer

This preprint series was founded in 1996. Its purpose is to present manuscripts of submitted or unpublished papers and reports of fellows of the Mathematical Institute of the Slovak Academy of Sciences in Bratislava and its Košice branch. The authors are fully responsible for the content of the preprints. Postal addresses:

Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
SK–814 73 Bratislava
SLOVAKIA

Tel./Fax (+421 7) 5249 7316

Mathematical Institute
Slovak Academy of Sciences
Grešákova 6
SK–040 01 Košice
SLOVAKIA

Tel./Fax (+421 95) 6228291

PostScript files of preprints are available at WWW address:
http://www.mat.savba.sk/preprints

Latest preprints of the series:

14/1999 *Otakar Grošek, Ladislav Satko, Karol Nemoga*: ZKDWCNDPDC...

13/1999 *Otakar Grošek, Karol Nemoga, Ladislav Satko*: A remark to Luby-Rackoff and Ueli M. Maurer pseudorandom generators

12/1999 *Beloslav Riečan*: On the sum of observables in product MV algebras

11/1999 *Peter Eliaš*: A hierarchy of thin sets related to the boundedness of trigonometric series

10/1999 *Miloslav Duchoň, Peter Maličký*: On Herglotz theorem in partially ordered vector spaces

9/1999 *Ján Jakubík*: Torsion classes of specker lattice ordered groups

8/1999 *Ján Jakubík*: Graph automorphisms and cells of lattices

7/1999 *Miloslav Duchoň, Peter Maličký*: Positive linear maps on trigonometric polynomials

6/1999 *Miloslav Duchoň, Anna Kolesárová*: Fourier transforms of vector-valued measures on a certain compact semigroup

5/1999 *Miroslav Ploščica*: Separation properties in congruence lattices of lattices

4/1999 *Georges Chevalier, Anatolij Dvurečenskij, Karl Svozil*: Piron's and Bell's geometric lemmas and Gleason's theorem

3/1999 *Jarmila Hedlíková*: Relatively orthomodular lattices

2/1999 *Anatolij Dvurečenskij, Pekka Lahti, Kari Ylinen*: Some remarks on the moment problem

1/1999 *Anatolij Dvurečenskij*: Loomis-Sikorski theorem for σ-complete MV-algebras and ℓ-groups

27/1998 *Martin Kochol*: Cubic graphs without a Petersen minor have nowhere-zero 5-flows

26/1998 *Anatolij Dvurečenskij, Ferdinand Chovanec, Eva Rybáriková*: D-homomorphisms and atomic σ-complete Boolean D-posets

25/1998 *Anatolij Dvurečenskij*: Commutative BCK-algebras with product

24/1998 *Anatolij Dvurečenskij, Antonio Di Nola*: Product MV-algebras

23/1998 *Anatolij Dvurečenskij, Maria Gabriella Graziano*: Dedekind complete commutative BCK-algebras

22/1998 *Anatolij Dvurečenskij*: Ideals of commutative BCK-algebras

21/1998 *Anatolij Dvurečenskij, Beloslav Riečan*: Weakly divisible MV-algebras and product

20/1998 *Ivan Korec*: Definability of addition and multiplication from Pascal's triangle modulo n and number-theoretical functions

(continued on inside back cover)

19/1998 *Roberto Giuntini, Sylvia Pulmannová*: Ideals and congruences in effect algebras and QMV algebras

18/1998 *Ivan Korec*: Definability of exact arithmetical operations from approximate ones

17/1998 *Georges Chevalier, Sylvia Pulmannová*: Some ideal lattices in partial abelian monoids

16/1998 *Anatolij Dvurečenskij*: On categorical equivalences of commutative BCK-algebras

15/1998 *Ivan Korec*: Definability of addition and multiplication from some quadratic forms $ax^2 + cy^2$

14/1998 *Beloslav Riečan*: On the L^p space of observables on product MV algebras

13/1998 *Beloslav Riečan*: On the strong law of large numbers on some ordered structures

12/1998 *Ladislav Mišík, jr., Tibor Žáčik*: A simplified formula for calculation of metric dimension of converging sequences

11/1998 *Beloslav Riečan*: On the joint distribution of observables

10/1998 *Beloslav Riečan*: On the product MV algebras

9/1998 *Roman Frič*: A Stone-type duality and its applications to probability

8/1998 *Roman Frič*: Ring of maps: sequential convergence and completion

7/1998 *Roman Frič, Ján Jakubík*: Sequential convergences on Boolean algebras defined by systems of maximal filters

6/1998 *Roman Frič*: Categorical reflections on fields of events and probability

5/1998 *Beloslav Riečan*: On the probability theory and fuzzy sets

4/1998 *Ivan Korec*: Definability of arithmetical operations from binary quadratic forms

3/1998 *Beloslav Riečan*: On the conditional expectation of observables in MV algebras of fuzzy sets

2/1998 *Beloslav Riečan*: On the conditional probability on MV algebras

1/1998 *Paula B. Cohen, Robin L. Hudson, K. R. Parthasarathy, S. Pulmannová*: Hall's transformation via quantum stochastic calculus

13/1997 *Ivan Korec*: Real-time generation of primes by a one-dimensional cellular automaton with 9 states

12/1997 *Ivan Korec*: Arithmetical operations strongest with respect to the first order definability

11/1997 *Otokar Grošek, Karol Nemoga, Marcel Zanechal*: Why use bijective S-boxes in GOST-algorithm

10/1997 *Beloslav Riečan*: On the L^p space of observables

9/1997 *Ladislav Mišík Jr., Tibor Žáčik*: A formula for calculation of metric dimension of converging sequences

8/1997 *Anatolij Dvurečenskij, Maria Gabriella Graziano*: Commutative *BCK*-algebras and lattice ordered groups

7/1997 *Anatolij Dvurečenskij, Maria Gabriella Graziano*: On representations of commutative BCK-algebras

6/1997 *Sylvia Pulmannová, Karl Svozil*: Ideals in ortholattices, Bell inequalities and simultaneously definite properties

5/1997 *Camille Debiève, Miloslav Duchoň, Beloslav Riečan*: Moment problem in some ordered vector spaces

4/1997 *Miloslav Duchoň, Beloslav Riečan*: On the Kurzweil–Stieltjes integral in ordered spaces

3/1997 *Anatolij Dvurečenskij, Maria Gabriella Graziano*: Remarks on representations of minimal clans

2/1997 *Ivan Korec*: Elementary definability from Pascal's triangle modulo p and the set of e-th powers