POWERS AND POLYNOMIALS IN $\mathbb{Z}_m$

LORENZ HALBEISEN, NORBERT HUNGERBÜHLER AND HANS LÄUCHLI

Dedicated to the memory of Prof. Hans Läuchli

1. Introduction and Notations

In this article we consider powers and polynomials in the ring $\mathbb{Z}_m$, where $m \in \mathbb{N}$ is arbitrary, and ask for "reduction formulas". For example, for addition, multiplication and exponentiation, we have the following well known reduction formulas:

$$a + b \equiv \operatorname{mod}(a,m) + \operatorname{mod}(b,m) \mod m \tag{1}$$

$$a \cdot b \equiv \operatorname{mod}(a,m) \cdot \operatorname{mod}(b,m) \mod m \tag{2}$$

$$a^b \equiv \operatorname{mod}(a,m)^b \mod m \tag{3}$$

It is much more difficult to find reduction formulas which allow to reduce the *exponent*. Of course in general

$$a^b \not\equiv a^{\operatorname{mod}(b,m)} \mod m. \tag{4}$$

In the second section we will investigate for which numbers m the reduction formula (4) holds.

In the third and the two following sections we will consider generalizations of Fermat's little theorem and Euler's Theorem which allow to replace (in $\mathbb{Z}_m$) certain powers a^b by a polynomial $f(a)$ of degree $\deg(f)$ which is strictly less than b. Such formulas can be useful for different reasons: From an algorithmic point of view, it is cheaper to compute the polynomial $f(a)$ modulo m than the full power a^b modulo m. On the other hand one may wish for algebraic reasons to replace an arbitrary polynomial $g(a)$ by a polynomial of fixed (lower) degree (depending only on m but not on g) which is, as a function in $\mathbb{Z}_m$, identical to g (see Section 6).

In the last section, we address the question of the minimal degree $e(m)$ such that every polynomial in $\mathbb{Z}_m$ can be written as a polynomial of degree $q < e(m)$. We give a complete answer to this question by determining minimal (normed) null-polynomials modulo m.

Throughout this paper, we use the customary shorthand notation $a \mid b$ for $a, b \in \mathbb{Z}$ with $\frac{b}{a} \in \mathbb{Z}$. We write

$$a \equiv b \mod m$$

for numbers $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, if $m \mid a - b$ and we adopt the notation (a, b) for the greatest common divisor of a and b. Furthermore we denote by $\operatorname{mod}(a,m)$ the uniquely determined number $r \in \{0, 1, \dots, m-1\}$ such that $a = km + r$ for some $k \in \mathbb{Z}$ and $\operatorname{Mod}(a, b)$ denotes the number $r \in \{1, \dots, m\}$ such that $a = km + r$ for some $k \in \mathbb{Z}$.

We had been working on the present article for about two years, when the mournful message of Hans Läuchli's death reached us. At that time, only the first part (Section 2), which comprises a theorem resulting from joint work of Hans Läuchli and Ernst Specker on exponential rings, and the second part (Sections 3–5) had been finished. The third part about minimal polynomials was not yet concluded, and we would like to thank Prof. Ernst Specker for inspiring and helpful discussions and for valuable suggestions concerning that last section.

2. Special values of m

In this section we investigate for which values of m the reduction formula (4) holds. The answer is contained in the following theorem.

Theorem 1. *Let $G := \{1, 2, 6, 42, 1806\}$, then the following statements are equivalent:*

(a) $m \in G$.

(b) *For all integers a, b there holds*

$$a^b \equiv a^{\mathrm{Mod}(b,m)} \mod m.$$

(c) *For all integers a there holds*

$$a^{m+1} \equiv a \mod m.$$

Remark: The equivalence of (b) and (c) is obvious: (c) follows from (b) by choosing $b = m+1$. The opposite implication follows from (2) by an easy induction argument. However, notice that in (b) we cannot replace "Mod" by "mod" in the exponent. To make this point more precise we state without proof:

Theorem 2. *Let $m \in G$, then there holds $a^m \equiv 1 \mod m$ (and hence (b) holds with* Mod *replaced by* mod*) if and only if no prime factor of* $\mathrm{mod}(a, m)$ *belongs to the set $G + 1 = \{2, 3, 7, 43, 1807\}$.*

The proof of the equivalence of (a) and (c) relies on an induction principle, which we prove after the following lemma.

Lemma 1. *Let $E_1 := 2$ and $E_{n+1} := q + E_1 E_2 \cdots E_n$ for a fixed, odd $q > 0$. If $A := E_1 \cdots E_k$ such that E_i is prime for $i \le k$ and $x \mid A$, then $x + q \in \{E_1, \ldots, E_{k+1}\}$ or $x + q^s$ is not prime for an s with $1 \le s < k$.*

Proof: If $x = A$, then $x + q = E_{k+1}$ and we are done. If $x \ne A$, then let l be the smallest number such that $E_l \nmid x$. If $l = 1$, then $x + q^1$ is even, therefore $x + q = 2 \in \{E_1\}$ or $x + q$ is not prime. Hence, the claim is proved for $l = 1$ and only the case $l > 1$ remains to be checked: Since $E_1, \ldots, E_l$ are prime, we have $E_1 \cdots E_{l-1} \mid x$. Notice that $E_1 \cdots E_{l-1} \equiv -q \mod E_l$ (for $l > 1$) and that $E_j \equiv q \mod E_l$ for $j > l$ (by definition). Therefore we conclude $x \equiv -q^s \mod E_l$, where s is smaller than the number of prime factors of x, hence $s < k$. Therefore $E_l \mid x + q^s$ and the proof is finished. □

We will use the special case $q = 1$ in the proof of the following

Theorem 3 (Induction Principle). *Let $H \subseteq \mathbb{N}$ be a set of natural numbers with the following properties:*

(i) $1 \in H$,
(ii) *if $h \in H$ and $h+1$ is prime, it follows that $h(h+1) \in H$,*
(iii) *if $p^2 \mid x$ for $p > 1$, then $x \notin H$,*
(iv) *if $h = A\,p\,a \in H$, p prime, such that all divisors of a are greater than p, then $p-1 \mid A$.*

Then $H = G$.

Proof: By (i) and (ii), $G \subseteq H$. For the opposite inclusion we claim that $2 \leq h \in H$ implies $h = E_1 \cdot E_l$ with $l \leq 4$: In fact, by (iii), we know that $h = p_1 p_2 \cdots p_n$ with $p_1 < p_2 < \ldots < p_n$ being prime numbers. Now we use (iv) with $A = 1$, $p = p_1$ and $a = \frac{r}{p}$. Because $p_1 - 1 \mid 1$ (by (iv)), we have $p_1 = 2 = E_1$. Now, by induction, we assume that $p_j = E_j$ for all $j \leq k \leq l$. Applying (iv) again, this time with $A = E_1\, E_2 \cdots E_k$, $p = p_{k+1}$ and $a = \frac{r}{Ap}$, we have $p_{k+1} - 1 \mid A$. Thus, by Lemma 1, $p_{k+1} \in \{E_1, \ldots, E_{k+1}\}$ and since $p_{k+1} > p_j$ for $j \leq k$, we conclude $p_{k+1} = E_{k+1}$. □

Proof of Theorem 1: Now, we use the induction principle to prove Theorem 1. We have to check properties (i)–(iv) for the set L of numbers h which satisfy (c):

(i) is trivial.

(ii) follows easily from Fermat's little theorem (see Section 3).

(iii): Let $h = p_1 \cdots p_n \in L$, p_k prime. By (c), we know that $p_k^{h+1} \equiv p_k \mod h$. Thus, $h \mid p_k(p_k^h - 1)$ and hence we have $p_k^h \equiv 1 \mod \frac{r}{p_k}$. For $i \neq k$ it follows that $p_k^h \equiv 1 \mod p_i$ and therefore $p_i \neq p_k$.

(iv): By (c) we have for $h = A\,p\,a \in L$ that $c^{h+1} \equiv c \mod h$ for all c . Thus $h \mid c(c^h - 1)$ and

$$c^h = (c^{A\,a})^p \equiv 1 \mod p. \tag{5}$$

Now, let c be such that $(c,p) = 1$, then (by Fermat's little theorem)

$$(c^{A\,a})^{p-1} \equiv 1 \mod p. \tag{6}$$

Combination of (5) and (6) yields $c^{A\,a} \equiv 1 \mod p$. Since p is prime and $(c,p) = 1$, it follows that $p - 1 \mid A\,a$ and by definition of a we get $p - 1 \mid A$, which completes the proof of Theorem 1. □

3. Generalization of Fermat's little theorem

Let us start with a definition. Let $p_1, \ldots, p_k$ be distinct prime numbers and $m = p_1^{\varepsilon_1} \cdots p_k^{\varepsilon_k}$ with $\varepsilon_i \in \mathbb{N}$ be the factorization of a number $m \in \mathbb{N}$. Then we define the function φ_m for integer numbers n by

$$\begin{aligned} \varphi_m(n) &= n^m - \sum_i n^{\frac{m}{p_i}} + \sum_{i_1<i_2} n^{\frac{m}{p_{i_1}p_{i_2}}} - \cdots + (-1)^k n^{\frac{m}{p_1\cdots p_k}} \\ &= \sum_{j \in M_{\{1,\ldots,k\}}} (-1)^{|j|} n^{\frac{m}{p_j}}. \end{aligned}$$

Here, M_A denotes the set of all ordered subsets of a set A and $j = (j_1, \ldots, j_i) \in M_A$ is a multi-index with length $|j| = i$ and with $p_j := p_{j_1} \cdots p_{j_i}$. It is convenient to extend the definition of φ_m by $\varphi_1(n) := n$.

Theorem 4. *The function $\varphi_m(n)$ has the property*

$$\varphi_m(n) \equiv 0 \mod m \tag{7}$$

for all numbers $n \in \mathbb{N}$.

Remarks: (i) If n is a prime number, then (7) follows from Gauss' observation that the number of irreducible polynomials of degree m over $\mathbb{Z}_n$ is given by $\varphi_m(n)/m$ (see [2]). Later Serret [8], Lucas [6] and Pellet [7] stated without proof that (7) holds true for arbitrary integer n. Later on, several proofs have been given for (7): S. Kantor presented in [3] and [4] geometric proofs and Weyr [9] used an involved inductive method.

(ii) Theorem 4 allows now to determine $\mathrm{mod}(n^m, m)$ by replacing the full power n^m by a polynomial in n of degree strictly less than m, which at least partially answers the question posed in the introduction.

Here, we show that (7) follows very easily from a combinatorial fact. To demonstrate the idea we consider the case of a prime number $m = p$. Consider the set $\{(n_1, \ldots, n_p) : n_i \in \{1, \ldots, n\}\}$ of points in the discrete p-dimensional cube $Q = \{1, \ldots, n\}^p$. Let d be the diagonal of Q through the edges $(0, \ldots, 0)$ and $(p, \ldots, p)$. The rotations with axes d which map Q to Q build the cyclic group C_p. The action of C_p on a point $(n_1, \ldots, n_p)$ is generated by $\sigma = \sigma_p : (n_1, \ldots, n_p) \mapsto (n_2, n_3, \ldots, n_p, n_1)$. According to Burnside's Lemma the total number of orbits in Q generated by C_p is given by

$$\text{number of orbits} = \frac{1}{|C_p|} \sum_{g \in C_p} \chi_g \tag{8}$$

where χ_g is the number of fix-points of Q under $g \in C_p$. Since $\chi_{\sigma^i} = n$ for $i = 1, \ldots, p-1$ and $\chi_{\sigma^p} = \chi_{\mathrm{id}} = n^p$ (and of course $|C_p| = p$) it follows from (8) that $n^p + (p-1)n \equiv 0 \mod p$ and hence

$$n^p - n \equiv 0 \mod p,$$

which is Fermat's little theorem.

For general m we proceed very similar, but instead of using Burnside's Lemma we count directly the orbits of given length.

Proof of Theorem 4: Let Q and C_m be as above but now with general $m = p_1^{\varepsilon_1} \cdots p_k^{\varepsilon_k}$. We claim that there exist $\frac{1}{m}\varphi_m(n)$ orbits of length m and hence the theorem follows. To prove this claim we proceed by induction on m:

1. step: $\varphi_1(n) = n$, hence the assertion is true for $m = 1$.

2. step: "$m' = p_1 \cdots p_{k-1} \to m = p_1 \cdots p_k$": Notice, that the number of orbits generated by C_m in $\{1, \dots, n\}^m$ of length $\frac{m}{m'}$ equals the number of orbits generated by $C_{m/m'}$ in $\{1, \dots, n\}^{m/m'}$ of length $\frac{m}{m'}$. So, by induction we have that

$$\begin{aligned}\text{number of orbits of length } \frac{m}{p_i} &= \frac{\varphi_{\frac{m}{p_i}}(n)}{\frac{m}{p_i}} \\ \text{number of orbits of length } \frac{m}{p_ip_j} &= \frac{\varphi_{\frac{m}{p_ip_j}}(n)}{\frac{m}{p_ip_j}} \\ &\cdots\end{aligned}$$

Hence,

$$\begin{aligned}(9)\qquad \text{number of orbits of length } m &= \\ &= \frac{1}{m}\Big(n^m - \sum_i \varphi_{\frac{m}{p_i}}(n) - \sum_{i<j} \varphi_{\frac{m}{p_ip_j}}(n) - \cdots - \varphi_i(n)\Big) \\ &= \frac{1}{m}\Big(n^m - \sum_{\substack{i \in M_{\{1,\dots,k\}} \\ i \text{ not empty}}} \; \sum_{j \in M_{\{1,\dots,k\}\setminus i}} (-1)^{|j|} n^{\frac{m}{p_ip_j}}\Big) \\ &= \frac{1}{m}\varphi_m(n).\end{aligned}$$

3. step: "$m' = p_1^{\varepsilon_1} \cdots p_k^{\varepsilon_k - 1} \to p' = p_1^{\varepsilon_1} \cdots p_k^{\varepsilon_k}$": analogous to the second step.

□

4. Generalisation of Euler's Theorem

One disadvantage of (7) is that it reduces in $\mathbb{Z}_m$ only the power m. Here, we present a formula which reduces yet another power and which is slightly stronger than Euler's Theorem. Let us recall the definition of Euler's φ function: For any integer n, $\varphi(n)$ denotes the number of integers $k \in \{1, \dots, n-1\}$ which are relatively prime to n, i.e.

$$\varphi(n) := |\{k \in \{1, \dots, n-1\} \,:\, (n, k) = 1\}|.$$

Furthermore, let $\vartheta(n)$ denote the highest power contained in n, i.e.

$$\vartheta(n) := \max\{k \,:\, m^k \mid n,\, m \in \mathbb{N},\, m > 1\}.$$

Theorem 5. *There holds*

(a) $n^{\vartheta(q)}(n^{\varphi(q)}-1) \equiv 0 \mod q$ *for all integers* n.
(b) $\vartheta(q)+\varphi(q) \leq q$ *for all* q *with equality if and only if* q *is prime.*

Proof: (a) Let $q = q_1^{\varepsilon_1} \cdots q_k^{\varepsilon_k}$ be the prime factorization of q. If $(n, q_i) = 1$ it follows from Euler's Theorem (which asserts that $n^{\varphi(q)} \equiv 1 \mod q$ provided $(n,q) = 1$) that $q_i^{\varepsilon_i} \mid n^{\varphi(q_i^{\varepsilon_i})} - 1$. Hence, since φ is multiplicative, i.e. $\varphi(ab) = \varphi(a)\varphi(b)$ for $(a,b) = 1$,

$$q_i^{\varepsilon_i} \mid n^{\varphi(q)} - 1 \qquad \text{if } (n, q_i) = 1. \tag{10}$$

Furthermore we have $q_i^{\varepsilon_i - 1} \mid q$ and hence $q_i^{\varepsilon_i - 1} \mid q - \varphi(q) > 0$. On the other hand, it is clear that $(n, q_i) > 1$ implies $q_i \mid n$. Hence we have

$$q_i^{\varepsilon_i} \mid n^{\vartheta(q)} \qquad \text{if } (n, q_i) > 1. \tag{11}$$

Now, combining the two cases (10) and (11) the assertion follows.

(b) *1. step:* If q is prime then obviously $\vartheta(q) + \varphi(q) = 1 + (q-1) = q$.

2. step: We have to show that $\vartheta(q) + \varphi(q) < q$ if q is not prime. If $q = p^n$ for a prime number p and $n \geq 2$, the assertion is equivalent to $n + (p-1)^n < p^n$, which is easily established by induction on $n \geq 2$. If $q = p^n q'$ with p prime, $q' > 1$ and $n = \vartheta(q) \geq 1$, then

$$\begin{aligned} \vartheta(q) + \varphi(q) &= n + (p-1)^n \varphi(q') \\ &\leq n + (p-1)^n (q'-1) \end{aligned}$$

and hence the assertion follows from the fact $n + (p-1)^n(q'-1) < p^n q'$ which is easily proved by induction on n. $\square$

Remarks: (i) Of course, Euler's Theorem follows from Theorem 5(a).

(ii) It is clear from the proof, that the exponent $\vartheta(q)$ in (a) is optimal, i.e. it cannot be replaced by a smaller integer.

(iii) Theorem 5 allows to replace $n^{\vartheta(q)+\varphi(q)}$ in $\mathbb{Z}_q$ by a polynomial in n of degree strictly less than $\vartheta(q) + \varphi(q)$.

5. Another application of Burnside's Lemma

In this section, we consider a variant of the arguments of Section 3. There, we considered the cyclic group C_m, i.e. the group with one generating element of order m. Notice that the set of points of the cube $Q = \{1, \ldots, n\}^m$ (on which C_m acts) may as well be considered as the set of colorings with n colors of the Cayley graph of C_m generated by the generating element. (The Cayley graph $G[A]$ of a group G generated by a subset $A = \{a_1, \ldots, a_k\} \subset G$ has the elements $\{g_1, \ldots, g_l\}$ of G as its vertex set and edges between g_i and g_j iff there exists $a_n \in A$ with $g_i \circ a_n = g_j$.) By applying Burnside's Lemma to this situation, we obtained (7).

A natural variant of this idea would be to look at the group $G = C_{p_1} \times \cdots \times C_{p_k}$ of k generating elements $a_1, \ldots, a_k$ of orders $p_1, \ldots, p_k$, acting on the Cayley graph $G[a_1, \ldots, a_k]$ over the generating elements and colored with n colors. In fact, if the p_i are chosen to be prime (but not necessarily different), we recover (7) by applying Burnside's Lemma. But we do in fact obtain a new congruence if we look at a "reduced Cayley graph" instead. More precisely we consider the graph $C_{p_1}[p_1] \times \cdots \times C_{p_k}[p_k]$ colored with n colors, and $g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k} \in G$ acting on it by application of g_i on $C_{p_i}[p_i]$. Counting orbits in a similar way as in Section 3 we find

Theorem 6. *If $m = p_1 \cdots p_k$ (p_i prime, but not necessarily distinct), then there holds for all integers n*

$$\sum_{j \in M_{\{1,\ldots,k\}}} (-n)^{|j|} n^{s(m)-s(p_j)} \equiv 0 \mod m$$

where we used the multi-index notation of Section 3 and $s(m) := p_1 + \cdots + p_k$ denotes the sum of the primes in m (with multiplicity).

Remarks: (i) Theorem 6 now allows to reduce $n^{s(m)}$ by a polynomial of lower degree in $\mathbb{Z}_m$.

(ii) If one does not insist on p_i being prime, one ends up with a polynomial of degree $p_1 + \cdots + p_k \geq s(m)$ which vanishes in $\mathbb{Z}_m$.

6. Minimal null-polynomials

6.1. Normed null-polynomials. Usually one defines two polynomials f and g to be congruent modulo m, written $f \equiv g \mod m$, if corresponding coefficients are congruent integers modulo m. This equivalence relation provides a nice structure in particular if m is chosen to be prime. On the other hand we will say that two polynomials (or, more general, two functions) f and g are *graph-congruent modulo* m, written $f \equiv g \operatorname{graph mod} p$, if they have the same graph as functions from $\mathbb{Z}_m$ to $\mathbb{Z}_m$, i.e. if $f(n) \equiv g(n) \mod m$ for all integers n. Of course, two congruent polynomials are graph-congruent, but the converse implication does not hold in general, e.g. $x^2 \equiv x \operatorname{graph mod} 2$, but x^2 and x are not congruent modulo 2. We say f is a *normed null-polynomial* modulo m, if f is graph-congruent to the polynomial 0 and if f is normed (i.e. the leading coefficient equals 1). Of course, for all m there exist normed null-polynomials, e.g. $f(x) = (x-1)(x-2)\cdots(x-m)$, and hence it makes sense to look for *minimal* normed null-polynomials modulo m, i.e. normed null-polynomials of minimal degree $e(m)$. It is easy to see, that if $m = p$ is prime, the polynomial

$$x^p - x \equiv (x-1)\cdots(x-p) \mod p$$

is (up to congruence) the unique minimal normed null-polynomial, and hence $e(p) = p$ for p prime. Minimal normed null-polynomials are useful since they allow to replace arbitrary polynomials by graph-congruent polynomials of degree less than or equal to $e(m)-1$ modulo m. To find a minimal normed null-polynomial on a computer by just checking polynomial after polynomial, would be extremely time consuming. On the other hand from Theorem 5 and 6 we infer, that

$$e(q) \leq \min\{q, s(q), \vartheta(q)+\varphi(q)\}.$$

Example: Let $m = 35$ and $f(n) = \sum_{i=0}^{35} n^i$. Find a polynomial g of lower degree which is as a function in $\mathbb{Z}_m$ identical to f.

Theorem 4 provides a normed null-polynomial of degree 35, which would allow to find a polynomial g of degree 34. Theorem 5 gives a normed null-polynomial of degree $\vartheta(m)+\varphi(m) = 25$ which is better, but Theorem 6 gives a polynomial of even lower degree, namely $s(m) = 12$, in fact

$$n^{12} \equiv n(n^5 + n^7 - n) \quad \text{graph} \bmod 35.$$

Replacing in f successively all powers n^{12} by $n(n^5+n^7-n)$ one finds

$$\sum_{i=0}^{35} n^i \equiv 1 + n - 15(n^2+n^3) - 13(n^4+n^5) + \\ 5(n^6+n^7) + 21(n^8+n^9) + 19(n^{10}+n^{11}) \quad \text{graph} \bmod 35.$$

We include the following list, which decides for which m Theorem 5 or Theorem 6 yields a normed null-polynomial of lower degree:

(1) $\vartheta(q)+\varphi(q) = s(q)$ if and only if q is prime or $q \in \{4, 18\}$
(2) $\vartheta(q)+\varphi(q) < s(q)$ if $q = 2p$, p prime, or $q \in \{12, 30\}$
(3) for all other q there holds $\vartheta(q)+\varphi(q) > s(q)$

Since for $m = 18$ both theorems give a polynomial of degree 8, we can look at the difference which is the (normed) null-polynomial $n^7+2n^6-2n^5-n^4+n^3-n^2$. But still, it is not minimal. In fact $n^6+n^4-2n^2$ is a minimal normed null-polynomial modulo 18, i.e. $e(18) = 6$. The following theorem gives the general answer to the problem:

Theorem 7. *The polynomial $g(x) = \prod_{i=1}^{\mathfrak{s}(m)}(x+i)$ is a minimal normed null-polynomial in $\mathbb{Z}_m$ and hence $e(m) = \mathfrak{s}(m)$. Here, $\mathfrak{s}(m)$ denotes the Smarandache function $\mathfrak{s}(m) := \min\{k \in \mathbb{N} : m \mid k!\}$.*

The function $\mathfrak{s}(m)$ is named after the Rumanian Mathematician Florentin Smarandache, but it has been introduced already in 1918 by Kempner in [5]. It has many interesting properties and applications in number theory (see e.g. the Smarandache Function Journal).

Proof: *1. step:* $g(x)$ is a normed null-polynomial in $\mathbb{Z}_m$: This follows immediately from the fact that for all $x \in \mathbb{Z}$

$$g(x) \quad = \quad \binom{x+\mathfrak{s}(m)}{\mathfrak{s}(m)}\mathfrak{s}(m)!$$

Now, the first factor is an integer, and $\mathfrak{s}(m)! \equiv 0 \mod m$.

2. step: $e(m) \geq \mathfrak{s}(m)$: Let us consider the normed polynomial $f(x) := a_1 x + a_2 x^2 + \ldots + a_{r-1} x^{r-1} + x^r$ with $a_i \in \mathbb{Z}$ and $r > 1$. We define

$$M = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 2 & 2^2 & \cdots & 2^{r-1} \\ 3 & 3^2 & \cdots & 3^{r-1} \\ \vdots & \vdots & \ddots & \vdots \\ r-1 & (r-1)^2 & \cdots & (r-1)^{r-1} \end{pmatrix}$$

and the vectors

$$a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{r-1} \end{pmatrix}, \quad h = \begin{pmatrix} f(1) \\ f(2) \\ \vdots \\ f(r-1) \end{pmatrix}, \quad \rho = \begin{pmatrix} 1^r \\ 2^r \\ \vdots \\ (r-1)^r \end{pmatrix}.$$

In this notation, we have

$$Ma = h - \rho.$$

Now, suppose that

$$f(x) \equiv 0 \mod m \text{ for all } x = 1, 2, \ldots, r-1,$$

i.e. $h = m\,q$ for some $q \in \mathbb{Z}^{r-1}$. Notice that M is a Vandermonde matrix and that in particular $\det(M) \neq 0$. Hence, the equation $Ma = m\,q - \rho$ determins for any given right hand side a unique solution a. From Lemma 2 below we infer

$$\begin{aligned} f(r) &= r^r + \sum_{i=1}^{r-1} a_i r^i \\ &= r^r + \sum_{i=1}^{r-1} (-1)^{i+r} \binom{r}{i} (i^r - m q_i) \\ &\equiv \sum_{i=1}^{r} (-1)^{i+r} \binom{r}{i} i^r \mod m. \end{aligned}$$

Lemma 3 below now gives that $f(r) \equiv r! \equiv 0 \mod m$ implies $r \geq \mathfrak{s}(m)$. This completes the proof. $\square$

Lemma 2. *Let M be the Vandermonde matrix $(i^j)_{i,j=1,\ldots,r-1}$ as above. Then, for $a \in \mathbb{R}^{r-1}$ and $b = Ma$ there holds*

$$\sum_{i=1}^{r-1} a_i r^i = -\sum_{i=1}^{r-1} (-1)^{i+r} \binom{r}{i} b_i. \tag{12}$$

Proof: By linearity, it suffices to show (12) for $a_i = \delta_{i,j}$, $j = 1, 2, \ldots, r-1$. That is, we have to show that for $1 \leq j \leq r-1$

$$r^j = -\sum_{i=1}^{r-1} (-1)^{i+r} \binom{r}{i} i^j .$$

This follows also from Lemma 3. $\square$

Lemma 3. *For $r \in \mathbb{N}_0$ and $j \in \mathbb{N}_0$, there holds*

$$\sum_{i=0}^{r} (-1)^{r-i} \binom{r}{i} i^j = r!\, S_2(j,r),$$

where S_2 is the Stirling number of the second kind.

Proof: A proof of this well-known lemma can be found e.g. in [1]. But for the sake of completeness, we like to give a proof by combinatorial arguments which are similar to those in the proof of Burnside's Lemma. Moreover, we shall give a special proof for the case $j = r$ and will consider the general case afterwards in a slightly different way.

First notice, that from the binomial expansion of $(1+x)^r$ with $x = -1$, we get

$$(\diamond) \qquad \sum_{i=0}^{r} (-1)^{r-i} \binom{r}{i} = 0^r,$$

which is (for $r > 0$) obviously equivalent to

$$(*) \qquad \sum_{i=0}^{r-1} (-1)^{i+1} \binom{r}{r-i} = (-1)^r .$$

Let $A := \{a_0, \ldots, a_{r-1}\}$ be an alphabet of $r > 0$ symbols and let $w_r(k)$ denote the set of words of length r, such that every word in $w_r(k)$ consists of exactly k different letters. Further, let $W_r(k)$ denote the cardinality of $w_r(k)$. Obviously we have $W_r(0) = W_r(r+i) = 0$ (for $i \geq 1$) and $W_r(r) = r!$. And in general we have

$$(**) W_r(k) = \binom{r}{k} k^r - binomr - k + 11W_r(k-1) - \binom{r-k+2}{2} W_r(k-2) - \ldots$$
$$\ldots - \binom{r-1}{k-1} W_r(1) - \binom{r}{k} W_r(0).$$

To see this, remember that with k different letters we can form k^r words for length r, but of course, not all of them contain k different letters. So, to compute $W_r(k)$, we have to exclude the words which contain less than k different letters.

Combining $(*)$ and $(**)$ we get

$$W_r(r) = \binom{r}{r} r^r - \binom{r}{r-1} (r-1)^r + \binom{r}{r-2} (r-2)^r - \ldots (-1)^r \binom{r}{0} 0^r = r!\,.$$

Because $S_2(n,n) = 1$ (for all $n \in \mathbb{N}_0$), this proves the Lemma for $r = j$ even in the case when $r = j = 0$ (because $W_0(0) = \binom{0}{0}0! = 0!$).

Now we consider the general case. Again, $w_j(k)$ denotes the set of all words of length j, such that every word in $w_j(k)$ consists of exactly k different letters. For an arbitrary word u (of length j) let $\bar{u}$ be the set of all letters occurring in u and $|\bar{u}|$ be its cardinality. So, if $u \in w_j(k)$, then $|\bar{u}| = k$. For a set of letters $I \subseteq A$ let $v_j(I)$ be the set of all indexed I-words u_I of length j, such that $\bar{u_I} \subseteq I$. To each indexed word u_I there corresponds in a natural way the (non-indexed) word u. For two different I and I' such that $|I| = |I'|$ we call two indexed I-words u_I and $u_{I'}$ equivalent ($u_I \sim u_{I'}$) if the (non-indexed) words are equal. Let $[u]_i := \{v_I : v_I \sim u_{I'} \wedge |I| = |I'| = i\}$. Finally let

$$V_j(i) := \sum_{\substack{I \subseteq A \\ |I| = i}} |v_j(I)| \,.$$

Evidentially we have $V_j(i) = \binom{r}{i} i^j$. For an arbitrary word u of length j with $\bar{u} \subseteq I \subseteq A$ with $|I| = i$ we get

$$|[u]_i| = \binom{r - |\bar{u}|}{r - i}.$$

For a word u with $\bar{u} < r$, we have by ($\diamond$) that

$$\sum_{i=|\bar{u}|}^{r} (-1)^{r-i} |[u]_i| = 0 \,.$$

Therefore, $\sum_{i=0}^{r-1} (-1)^{r-i} \binom{r}{i} i^j = 0 = r!\, S_2(j,r)$. Now, with the alphabet A we can form $r!\, S_2(j,r)$ words u of length j, such that $\bar{u} = A$, which completes the proof. □

Remark: As a corollary of the previous lemma, we obtain Wilson's Theorem: $(p-1)! \equiv -1 \mod p$ if and only if p is prime. To see this, notice first that if $p = ab$, where a, b both bigger than 1 and $(a,b) = 1$, then $a \mid (p-1)!$ and $b \mid (p-1)!$, therefore $(p-1)! \equiv 0 \mod p$. For p prime, set $r = j = p-1$ and use Fermat's little theorem in the Lemma 3 (for the only even prime number $p = 2$, notice that $-1 \equiv 1 \mod 2$).

6.2. General null-polynomials. Except in the case when m is prime, the minimal normed null-polynomials are far from unique. For example, given a normed null-polynomial, one can add a general (not normed) null-polynomial of lower degree. So, let us look now for non-trivial minimal null-polynomials (which need not be normed). Let $\tilde{e}(m)$ denote the degree of a general non-trivial minimal null-polynomial modulo m. Then there holds:

Theorem 8. *$\tilde{e}(m)$ equals the smallest prime factor in m.*

Proof: Let $m = p_1^{\varepsilon_1} \cdots p_k^{\varepsilon_k}$ with p_i prime and $p_1 \leq p_j$ for all $j > 1$.

1. step: If $p_1 > 2$, then the polynomial

$$f(x) = \frac{m}{p_1}\, x \prod_{i=1}^{\frac{p_1-1}{2}} (x^2 - i^2)$$

is a null-polynomial. For $p_1 = 2$ the polynomial $f(x) = \frac{m}{2}x(1+x)$ is a null-polynomial. Thus we have $\tilde{e}(m) \leq p_1$.

2. step: Let $f(x)$ be a non-trivial null-polynomial in $\mathbb{Z}_m$. Without loss of generality, we may assume that the coefficients of f do not contain a common divisor $p_i^{\delta_i}$ with $\delta_i > \varepsilon_i$ (otherwise, one can divide f by $p_i^{\delta_i - \varepsilon_i}$ which would still be a non-trivial null-polynomial in $\mathbb{Z}_m$, but with the desired property). Let $\prod_{i=1}^k p_i^{\gamma_i}$ be the largest common divisor (of this form) of the coefficients of f. In particular, we have that $0 \leq \gamma_i \leq \varepsilon_i$ for all i. Thus, we have $f(x) = \prod_{i=1}^k p_i^{\gamma_i} g(x)$ for a polynomial $g(x)$ with integer coefficients and for all $x \in \mathbb{Z}$ there exists an integer h_x such that $f(x) = m\, h_x$. Hence, we conclude for $g(x)$ that $g(x) = h_x \prod_{i=1}^k p_i^{\varepsilon_i - \gamma_i}$. This means that g is a null-polynomial in $\mathbb{Z}_{m'}$ with $m' = \prod_{i=1}^k p_i^{\varepsilon_i - \gamma_i} > 1$. Furthermore, g is non-trivial in $\mathbb{Z}_{m'}$ since the greatest common divisor of the coefficients of g does not contain a factor p_i. Now, let j denote the smallest index with the property that $\varepsilon_j - \gamma_j > 0$. Then, g is a non-trivial null-polynomial in the field $\mathbb{Z}_{p_j}$. Since a non-trivial polynomial has in a field at most as many zeros as the degree indicates, we conclude $\deg(f) = \deg(g) \geq p_j \geq p_1$. $\square$

References

[1] M. Aigner: Kombinatorik. Springer, 1975

[2] C.F. Gauss. Posthumous papers, Werke 2 (1863), p. 222

[3] S. Kantor: Wie viele cyclische Gruppen gibt es in einer quadratischen Transformation der Ebene? Annali di matematica, Serie II, **10** (1880), 64–70

[4] S. Kantor: Beantwortung derselben Frage für Cremona'sche Transformation, Annali di matematica, Serie II, **10** (1880), 71–73

[5] A.J. Kempner: Concerning the smallest integer $m!$ divisible by a given integer n. Amer. Math. Monthly **25** (1918), 204–210.

[6] E. Lucas: Sur la généralisation du théorème de Fermat. Comptes rendus **96** (1883), 1300–1301

[7] M. Pellet: Sur une généralisation du théorème de Fermat. Comptes rendus **96** (1883), 1301–1302

[8] M. Serret: Théorème de Fermat généralisé. Nouvelles annales de mathématiques **14** (1855), 261–262

[9] E. Weyr: O jisté větě číselné. Časopis mathematiky a fysiky **11** (1882), 39–47

Lorenz Halbeisen, Centre de Recerca Matemàtica, Institut d'Estudis Catalans, Apartat 50, 08193 Bellaterra (Spain)

Norbert Hungerbühler, Mathematik Departement, ETH Zürich, 8092 Zürich (Switzerland)