TECHNICAL TRANSACTIONS 5/2017
CZASOPISMO TECHNICZNE 5/2017
MATHEMATICS
DOI: 10.4467/2353737XCT.17.073.6430

Maciej Zakarczemny (mzakarczemny@pk.edu.pl)
Institute of Mathematics, Faculty of Physics, Mathematics and Computer Science, Cracow university of Technology

ONE SOME CANCELLATION ALGORITHMS II

ALGORYTMY SITOWE II

Abstract

We define $b_f(n)$ to be the smallest integer (a natural number) d such that numbers $f(n_1, n_2, ..., n_m)$, where $n_1+n_2+ ... + n_m \leq n$ are not divisible by d. For the given functions $f: \mathbb{N}^m \longrightarrow \mathbb{N}$, we will obtain the asymptotic characterisation of the sequence of the least non canceled numbers $(b_f(n))_{n\in\mathbb{N}}$. In the case $f: \mathbb{N}^2 \ni (k, l) \longrightarrow k^3+l^3 \in \mathbb{N}$, this characterisation can be rewritten in the terms of the permutations polynomials of finite commutative quotient ring $\mathbb{Z}/m\mathbb{Z}$. There are situations in which we cannot expect formula for $b_f(n)$ to be simple, but we can provide the upper and lower bounds of it.

Keywords: cancellation algorithms, primes in arithmetic progression, quadratic and cubic forms

Streszczenie

Definiujemy $b_f(n)$ jako najmniejszą $d \in \mathbb{N}$, taką że liczby $f(n_1, n_2, ..., n_m)$, gdzie $n_1+n_2+ ... + n_m \leq n$ są niepodzielne przez d. Dla wybranych funkcji $f: \mathbb{N}^m \longrightarrow \mathbb{N}$ znajdziemy wartości elementów ciągu $(b_f(n))_{n\in\mathbb{N}}$, lub podamy inną charakteryzacje. Dla funkcji $f: \mathbb{N}^2 \ni (k, l) \longrightarrow k^3+l^3 \in \mathbb{N}$, Charakteryzacja ciągu $(b_f(n))_{n\in\mathbb{N}}$ może być podana z użyciem wielomianów permutacyjnych skończonego, przemiennego, pierścienia ilorazowego $\mathbb{Z}/m\mathbb{Z}$. W szczególnych przypadkach funkcji f podamy dolne i górne ograniczenia na wartości ciągu $b_f(n)$.

Słowa kluczowe: algorytm wykreślania, sito, liczby pierwsze w ciągu arytmetycznym, formy kwadratowe i sześcienne

1. Introduction

Assume that g: $\mathbb{N}\to\mathbb{N}$ is some special injective mapping. Let:

$$D_g(n) := \min\{m\in\mathbb{N} : g(1), g(2), \dots , g(n) \text{ are distinct modulo } m\}. \quad (1)$$

The function D_g is commonly called the discriminator of the function g, because it provides the least modulus which discriminates the successive values of the function g. The problem first appears in the context of the computation of square roots of a long sequence of integers (see [1]).

Bremser, Schumer, Washington [2] determined for each sufficiently large natural number, the smallest positive integer m such that $1^j, 2^j, \dots, n^j$ are all incongruent modulo m. Moree and Mullen [5] investigated the case of the Dickson polynomial. Recently, the discriminators of various types of functions have been considered by Zieve [10], Sun [8], Moree and Zumalacárregui [6], Haque and Shallit [4].

There is also a slightly different, equivalent definition of a discriminator in terms of cancellations algorithms (see Browkin and Cao in paper [3]).

Indeed, for $n \geq 2$ define the set

$$A_g(n) := \{g(s) - g(r) : 1 \leq r < s \leq n\}, \quad (2)$$

hence

$$A_g(n) := \{g(k+l) - g(l) : k+l \leq n;\ k, l \in \mathbb{N}\}. \quad (3)$$

Remove from $\mathbb{N}$ all numbers from the set $\{h \in \mathbb{N} : h|a \text{ for some } a \in A_g(n)\}$, then $D_g(n)$ is the least non-canceled number.

Browkin and Cao, in particular, found $b(n)$ in the cases $g(s) = ks$ for some $k \in \mathbb{N}$, $g(s) = s^2$ and showed that in the last case $b(n)$ is newer equal to a Sophie Germain prime.

Instead of (3) Browkin and Cao also considered an arbitrary function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ with the set $\{f(k, l) : k+l \leq n;\ k, l \in \mathbb{N}\}$.

2. Theorems and definitions

More generally, we consider an arbitrary function $f : \mathbb{N}^m \to \mathbb{N}$, $m \geq 1$.

Definition 2.1. For a given natural number n, a natural number h is a *cancelled* number if there exist $n_1, n_2, \dots, n_m \in \mathbb{N}$ such that $n_1 + n_2 + \dots + n_m \leq n$ and $h|f(n_1, n_2, \dots, n_m)$, i.e. $h \in H_f(n)$, where

$$H_f(n)=\{h \in \mathbb{N} : \exists_{v\in V_f(n)} h|v\}, \quad (4)$$

$$V_f(n) = \{f(n_1, n_2, \dots , n_m): n_1 + n_2 + \dots + n_m \leq n\}. \quad (5)$$

Definition 2.2. $b_f(n)$ is the least number in the set $\mathbb{N} \setminus H_f(n)$, being called a set of all non-cancelled numbers.

2.1. Sum of squares

Theorem 2.3. *For the function* $f : \ni \mathbb{N} \ni n_1 \longrightarrow n_1^2 \in \mathbb{N}$ *we have*

$$b_f(n) = \min\{m : m > n,\ m \ square - free\}.$$

Proof. See Tomski and Zakarczemny paper [9]. ☐

Theorem 2.4. *For the function* f: $\mathbb{N}^2 \ni (n_1, n_2) \to n_1^2 + n_2^2 \in \mathbb{N}$ *we have*

$b_f(n) = min\ \{m : 2m \geq n + 1,\ m\ square - free\ product\ of\ primes \equiv 3 \pmod{4}\}$.

Proof. See Browkin and Cao Theorem 11 in the paper [3]. ☐

Theorem 2.5. *For the function* $f : \mathbb{N}^3 \ni (n_1, n_2, n_3) \longrightarrow n_1^2 + n_2^2 + n_3^2 \in \mathbb{N}$ *we have*

$$b_f(1) = 1,\ b_f(2) = 1,\ b_f(3) = 2,\ b_f(4) = 4,\ b_f(5) = 4.$$

Moreover, for any integer $s \geq 1$ *we have:*

1) *If* $2 \cdot 2^s \leq n < 3 \cdot 2^s$, *then* $\frac{2\sqrt{3}}{3} \cdot 2^s < b_f(n) \leq 4^s$,
2) *If* $3 \cdot 2^s \leq n < 2 \cdot 2^{s+1}$, *then* $\sqrt{3} \cdot 2^s < b_f(n) \leq 5 \cdot 4^{s-1}$.

Proof. By straightforward verification

$$b_f(1) = 1,\ b_f(2) = 1,\ b_f(3) = 2,\ b_f(4) = 4,\ b_f(5) = 4.$$

Put $n \geq 5$.

1) Let $2 \cdot 2^s \leq n < 3 \cdot 2^s$, where $s \geq 2$.
   If $h = 4^j < 4^s$, then $j \leq s - 1$. We take $n_1 = n_2 = n_3 = 2^j$.
   Hence $h | n_1^2 + n_2^2 + n_3^2$ and $n_1 + n_2 + n_3 = 3 \cdot 2^j \leq \frac{3}{2} \cdot 2^s < n$.
   If $h = 2 \cdot 4^j < 4^s$, then $j \leq s - 1$. We take $n_1 = 2^{j+1}$, $n_2 = n_3 = 2^j$.
   Hence $h | n_1^2 + n_2^2 + n_3^2$ and $n_1 + n_2 + n_3 = 4 \cdot 2^j \leq 2 \cdot 2^s \leq n$.
   If $h = 5 \cdot 2^j < 4^s$, then $j \leq 2s - 3$. We take $n_1 = 5 \cdot 2^{\left[\frac{j}{2}\right]}$, $n_2 = 2 \cdot 2^{\left[\frac{j}{2}\right]}$, $n_3 = 2^{\left[\frac{j}{2}\right]}$.
   Hence $h | n_1^2 + n_2^2 + n_3^2$ and $n_1 + n_2 + n_3 = 8 \cdot 2^{\left[\frac{j}{2}\right]} \leq 8 \cdot 2^{s-2} = 2 \cdot 2^s \leq n$.
   If $h \neq 2^j$, $h \neq 5 \cdot 2^j$ and $h < \frac{2\sqrt{3}}{3} \cdot 2^s$, then, by Hurwitz theorem (see [7]), we may find natural numbers n_1, n_2, n_3 such that $h^2 = n_1^2 + n_2^2 + n_3^2$. We have $n_1 + n_2 + n_3 \leq \sqrt{3}\sqrt{n_1^2 + n_2^2 + n_3^2} = \sqrt{3}h < 2 \cdot 2^s \leq n$.

Therefore, in each case h is cancelled. Hence $b_f(n) > \frac{2\sqrt{3}}{3} \cdot 2^s$.
To get the upper bound assume that $4^s | k^2 + l^2 + m^2$, where $k, l, m \in \mathbb{N}$, then $2^s | k, 2^s | l, 2^s | m$.
Therefore $k + l + m \geq 3 \cdot 2^s > n$ and 4^s is non-cancelled. Hence in this case $b_f(n) \leq 4^s$.

2) Let $3 \cdot 2^s \leq n < 2 \cdot 2^{s+1}$, where $s \geq 1$.
If $h = 4^j < 5 \cdot 4^{s-1}$, then $j \leq s$. We take $n_1 = n_2 = n_3 = 2^j$.
Hence, $h | n_1{}^2 + n_2{}^2 + n_3{}^2$ and $n_1 + n_2 + n_3 = 3 \cdot 2^j = 3 \cdot 2^s \leq n$.
If $h = 2 \cdot 4^j < 5 \cdot 4^{s-1}$, then $j \leq s - 1$. We take $n_1 = 2^{j+1}$, $n_2 = n_3 = 2^j$.
Hence $h | n_1{}^2 + n_2{}^2 + n_3{}^2$ and $n_1 + n_2 + n_3 = 4 \cdot 2^j \leq 2 \cdot 2^s < n$.
If $h = 5 \cdot 2^j < 5 \cdot 4^{s-1}$, then $j \leq 2s - 3$ and $s \geq 2$. We take $n_1 = 5 \cdot 2^{\left[\frac{j}{2}\right]}$, $n_1 = 2 \cdot 2^{\left[\frac{j}{2}\right]}$, $n_1 = 2^{\left[\frac{j}{2}\right]}$.
Hence $h | n_1{}^2 + n_2{}^2 + n_3{}^2$ and $n_1 + n_2 + n_3 = 8 \cdot 2^{\left[\frac{j}{2}\right]} \leq 8 \cdot 2^{s-2} = 2 \cdot 2^s < n$.
If $h \neq 2^j$, $h \neq 5 \cdot 2^j$ and $h < \sqrt{3} \cdot 2^s$, then, by Hurwitz theorem (see [7]), we may find natural numbers n_1, n_2, n_3 such that $h^2 = n_1{}^2 + n_2{}^2 + n_3{}^2$. We have

$$n_1 + n_2 + n_3 \leq \sqrt{3}\sqrt{n_1^2 + n_2^2 + n_3^2} = \sqrt{3}h < 3 \cdot 2^s \leq n .$$

In each case, we find out that h is cancelled. Hence, $b_f(n) > \sqrt{3} \cdot 2^s$.
To get upper bound assume that $5 \cdot 4^{s-1} | k^2 + l^2 + m^2$, where $k, l, m \in \mathbb{N}$,
then $2^{s-1} | k$, $2^{s-1} | l$, $2^{s-1} | m$ and $5 | (2^{1-s}k)^2 + (2^{1-s}l)^2 + (2^{1-s}m)^2$.
Hence, we have following inequalities $2^{1-s}k + 2^{1-s}l + 2^{1-s}m \geq 8$ and $k + l + m \geq 2 \cdot 2^{s+1} > n$.
We obtain that $5 \cdot 4^{s-1}$ is non-cancelled thus $b_f(n) \leq 5 \cdot 4^{s-1}$. ☐

Theorem 2.6. *For the function*

$$f : \mathbb{N}^4 \ni (n_2, n_2, n_3, n_4) \longrightarrow n_1{}^2 + n_2{}^2 + n_3{}^2 + n_4{}^2 \in \mathbb{N}$$

we have

$$b_f(1) = 1,\ b_f(2) = 1,\ b_f(3) = 1,\ b_f(4) = 3,\ b_f(5) = 3.$$

Moreover, for any integer $s \geq 1$ we have:
1) *If $3 \cdot 2^s \leq n < 4 \cdot 2^s$, then $b_f(n) \leq 2^{2s+1}$,*
2) *If $4 \cdot 2^s \leq n < 3 \cdot 2^{s+1}$, then $b_f(n) \leq 3 \cdot 2^{2s+1}$.*

Proof. By straightforward verification

$$b_f(1) = 1,\ b_f(2) = 1,\ b_f(3) = 1,\ b_f(4) = 3,\ b_f(5) = 3.$$

Let $s \in \mathbb{N}$.
If $3 \cdot 2^s \leq n < 4 \cdot 2^s$, then from

$$2^{2s+1} | n_1^2 + n_2^2 + n_3^2 + n_4^2 \Rightarrow \forall_i 2^s | n_i \Rightarrow n_1 + n_2 + n_3 + n_4 \geq 4 \cdot 2^s > n$$

we get $b_f(n) \leq 2^{2s+1}$.
If $4 \cdot 2^s \leq n < 3 \cdot 2^{s+1}$, then from

$$3 \cdot 2^{2s+1} | n_1^2 + n_2^2 + n_3^2 + n_4^2 \Rightarrow \forall_i 2^s | n_i \wedge \exists_i 3 | n_i \Rightarrow n_1 + n_2 + n_3 + n_4 \geq 6 \cdot 2^s > n$$

we find out that $b_f(n) < 3 \cdot 2^{2s+1}$. ☐

2.2. Sum of powers

Theorem 2.7. *For the function* $f : \mathbb{N}^2 \ni (n_1, n_2) \to n_1^{\,3} + n_2^{\,3} \in \mathbb{N}$ *we have*

$$b_f(n) = \min\{m : m > n, m \text{ square} - \mathit{free}, (3, \varphi(m)) = 1\}.$$

Proof. See Tomski and Zakarczemny paper [9]. $\square$

Remark 2.8. m is square-free and $(3, \varphi(m)) = 1$ iff the function x^3 permutes the elements of the finite ring $\mathbb{Z}/m\mathbb{Z}$ (see Lemma 2.9 below).

Lemma 2.9. *For a natural number* $k > 4$, *and an odd number* $j \geq 3$, *the following statements are equivalent*

(i) *For all* $a, b \in \mathbb{N}$ *such that* $a + b \leq k - 1$ *we have* $k \nmid a^j + b^j$,
(ii) $(j, \varphi(k)) = 1$ *and* k *is square-free,*
(iii) x^j *is a permutation polynomial of the finite ring* $\mathbb{Z}/k\mathbb{Z}$.

Proof. It follows from [2, p.32] that (ii) and (iii) are equivalent.
Assume that (ii) holds. If there exist $a, b \in \mathbb{N}$ such that $a + b \leq k - 1$ and $a^j + b^j \equiv 0 \pmod{k}$, then $a^j \equiv (k - b)^j \pmod{k}$ and $1 \leq a < k - b \leq k - 1$. We obtain a contradiction with (iii). Hence (ii) implies (i).
On the other hand, assume that (i) holds.
Then, for all $a, b \in \mathbb{N}$, $1 \leq a < b \leq k - 1$ we have following relations $k \nmid a^j + (k - b)^j$, $k \nmid a^j - b^j$.
Hence, $1^j, 2^{\,j}, \ldots, (k - 1)^{\,j}$ are distinct mod k.
We will show that k is square-free. Suppose the contrary, we put $k = p^2 l > 4$, where $l \in \mathbb{N}$ and p is a prime number. If we take

$$a = \begin{cases} pl - p & \text{if } p = 2,\ l > 1 \\ pl & \text{if } p \geq 3,\ l \geq 1 \end{cases}, \quad \mathrm{b} = \begin{cases} p & \text{if } p = 2,\ l > 1 \\ pl & \text{if } p \geq 3,\ l \geq 1 \end{cases},$$

then $a + b \leq k - 1$ and $a^j + b^j \equiv 0 \pmod{k}$, thus, we get contradiction with (i). Consequently, k is a square-free number.
Therefore, $a^j \equiv 0 \pmod{k}$ implies $a \equiv 0 \pmod{k}$. Thus $0^j, 1^{\,j}, \ldots, (k - 1)^{\,j}$ are distinct mod k and (iii) holds, therefore, (ii) holds also. $\square$

Theorem 2.10. *We fix some odd integer* $j \geq 3$. *For the function*

$f : \mathbb{N}^2 \ni (n_1, n_2) \to n_1^{\,j} + n_2^{\,j} \in \mathbb{N}$ *we have*

$$n < b_f(n) \leq \min\{m : m > n, m \ \mathit{square} - \mathit{free}, (j, \varphi(m)) = 1\}.$$

Proof. The first inequality follows from the fact that if j is an odd integer then $n_i + n_2 | n_1^j + n_2^j$. Indeed, for a natural number $2 \le h \le n$, we take $n_1 = 1, n_2 = h - 1$.

Hence $h | n_1^j + n_2^j$ and $n_1 + n_2 = h \le n$. Therefore, h is cancelled. Hence, $b_f(n) > n$. For the proof of the second inequality assume that $m > n$, m is square-free number, $(j, \varphi(m)) = 1$, then, by Lemma 2.9 for all $n_1, n_2 \in \mathbb{N}$ such that $n_1 + n_2 \le n$ we have $m \nmid n_1^j + n_2^j$. Hence, $b_f(n) \le m$ and theorem follows. $\square$

Remark 2.11. We fix some integer j greater or equal to 2. For the function $f : \mathbb{N} \ni n_1 \longrightarrow n_1^j \in \mathbb{N}$, we have $b_f(n) = \min\{m : m > n, m \textit{ square} - \textit{free}\}$.
For the proof, see Tomski and Żakarczemny paper [9].

3. Conjectures, remarks and open problem

Conjecture 3.1. *For the function*

$$f : \mathbb{N}^3 \ni (n_1, n_2, n_3) \longrightarrow n_1^2 + n_2^2 + n_3^2 \in \mathbb{N}$$

and any integer $s \ge 1$ we have:

1) *If* $2 \cdot 2^s \le n < 3 \cdot 2^s$, *then* $b_f(n) = 4^s$,
2) *If* $3 \cdot 2^s \le n < 2 \cdot 2^{s+1}$, *then* $b_f(n) = 5 \cdot 4^{s-1}$.

Remark 3.2. The author verified Conjecture 3.1 for $n = 4, \dots, 206$.

Conjecture 3.3. *For the function*

$$f : \mathbb{N}^4 \ni (n_1, n_2, n_3, n_4) \longrightarrow n_1^2 + n_2^2 + n_3^2 + n_4^2 \in \mathbb{N}$$

and any integers $s \ge 1$, $n > 16$ we have:

1) *If* $3 \cdot 2^s \le n < 4 \cdot 2^s$, *then* $b_f(n) = 2^{2s+1}$,
2) *If* $4 \cdot 2^s \le n < 3 \cdot 2^{s+1}$, *then* $b_f(n) = 3 \cdot 2^{2s+1}$.

Remark 3.4. The author verified Conjecture 3.3 for $n = 17, \dots, 127$.

Conjecture 3.5. *We fix some odd integer $j \ge 3$. For the function $f : \mathbb{N}^2 \ni (n_1, n_2) \longrightarrow n_1^j + n_2^j \in \mathbb{N}$, if a natural number $n \ge 4$ then*

$$\begin{aligned} b_f(n) &= \min\{m : m > n, m \textit{ square} - \textit{free}, (j, \varphi(m)) = 1\} \\ &= \min\{m : \textit{polynomial } x^j \textit{ permutes elements of } \mathbb{Z}/m\mathbb{Z}\}. \end{aligned} \tag{6}$$

Remark 3.6. For proof of Conjecture 3.5 in the case $j = 3$, see Theorem 2.7.
The author found that the equation (6) holds for $j \in \{5, 7, 9, 11, 13\}$ and $n \in \{4, 5, \dots, 200\}$.

Open Problem 3.7. *For the function*

$$f : \mathbb{N}^3 \ni (n_1, n_2, n_3) \longrightarrow n_1^{\,3} + n_2^{\,3} + n_3^{\,3} \in \mathbb{N}, \text{ we have}$$

n	1, 2	3	4, 5	6, ..., 10	11, ..., 17	18, 19	20, ..., 24	25, 26	27, 28, 29	30, ..., 34
$b_f(n)$	1	2	4	7	13	52	65	117	156	169

n	35, 36, 37	38, ..., 41	42, ..., 48	49, ..., 57	58, 59	60, 61, 62	63, ..., 66	67, ...,73
$b_f(n)$	241	260	301	481	802	903	973	1118

Find and prove an explicit formula or asymptotic characterisation for the above sequence.

The author thanks the referee for several helpful suggestions.

References

[1] Arnold L.K., Benkoski S.J., McCabe B.J., *The discriminator (a simple application of Bertrand's postulate)*, Amer. Math. Monthly, 1985, 92, 275–277.

[2] Bremser P.S., Schumer P.D., Washington L.C., *A note on the incongruence of consecutive integers to a fixed power*, J. Number Theory, 1990, 35, No. 1, 105–108.

[3] Browkin J., Cao H-Q., *Modifications of the Eratosthenes sieve*, Colloq. Math. 135, 2014, 127–138.

[4] Haque S., Shallit J., *Discriminators and k-regular sequences*, INTEGERS 16, 2016, Paper A76.

[5] Moree P., Mullen G.L., *Dickson polynomial discriminators*, J. Number Theory 59, 1996, 88–105.

[6] Moree P., Zumalacárregui A., *Salajan's conjecture on discriminating terms in an exponential sequence*, J. Number Theory 160, 2016, 646–665.

[7] Sierpiński W., *Elementary Theory of numbers*, Ed. A. Schinzel, North-Holland 1988.

[8] Zhi-Wei Sun, *On funtions taking only prime values*, J. Number Theory 133, 2013, 2794–2812.

[9] Tomski A., Zakarczemny M., *On some cancellation algorithms*, NNTDMM 23, 2017, 101–114.

[10] Zieve M., *A note on the discriminator*, J. Number Theory 73, 1998, 122–138.