Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 23, 2017, No. 1, 101–114

On some cancellation algorithms

Andrzej Tomski[1] **and Maciej Zakarczemny**[2]

[1] Institute of Mathematics, University of Silesia
Bankowa 14, 40-007 Katowice, Poland
e-mail: andrzejtomski@wp.pl

[2] Institute of Mathematics, Cracow University of Technology
Warszawska 24, 31-155 Kraków, Poland
e-mail: mzakarczemny@pk.edu.pl

Received: 17 September 2016 **Accepted:** 31 January 2017

Abstract: Let f be a natural-valued function defined on the Cartesian product of finitely many copies of $\mathbb{N}$ (positive integers). Here we will discuss some modifications of the sieve of Eratosthenes in the sense that we cancel the divisors of all possible values of f in the points whose sum of coordinates is less or equal to n. By applying similar arguments to those used in the paper [J. Browkin, H-Q. Cao, *Modifications of the Eratosthenes sieve*, Colloq. Math. 135, (2014)], but also in the companion papers, we investigate new problems for the values of some polynomial functions or quadratic and cubic forms.
Keywords: Cancellation algorithms, Primes in arithmetic progression, Quadratic and cubic forms.
AMS Classification: Primary 11A41; Secondary 11N32, 11N36.

1 Introduction

Suppose that

$$D_f(n) := \min\{m \in \mathbb{N} : \ g(1), g(2), \ldots, g(n) \text{ are distinct modulo } m\} \tag{1.1}$$

for some special injective mapping $g : \mathbb{N} \to \mathbb{N}$, see [8] and [9].

The $D_f(n)$ is generally known as the discriminator and was involved in determining an efficient algorithm for computing the square roots of a long sequence of integers for a problem in computer simulation (see [1]).

Arnold, Benkoski, and McCabe [1] defined, for natural number n, the smallest natural number m such that $1^2, 2^2, \ldots, n^2$ are all distinct modulo m. In this case, the value $D_f(n)$ for $n > 4$ is the smallest $m \geq 2n$ such that m is a prime or twice a prime. Later authors tried to generalize it to the cyclic polynomials $g(x) = x^j$, where j is any natural number, see [2]. Zhi-Wei Sun made a modification to get only the primes. The characterization of the discriminator by permutation polynomials was made in papers [6] and [10].

Here we compute some generalization of the discriminator using methods from the elementary number theory.

Browkin and Cao in the paper [3] stated (1.1) equivalently in terms of the following cancellation algorithm. For $n \geq 2$ define the set

$$A_n := \{g(s) - g(r) : 1 \leq r < s \leq n\} = \{g(k+l) - g(l) : k + l \leq n\}.$$

Cancel in $\mathbb{N}$ all numbers from the set $\{d \in \mathbb{N} : d|a \,\text{for some}\, a \in A_n\}$,
then $D_f(n)$ is the least non-cancelled number.

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

$$V_n = \{f(n_1, n_2, \ldots, n_m) : \, n_1 + n_2 + \ldots + n_m \leq n\}.$$

Definition 1.1. We define $b_f(n)$ as the least number in the set

$$\mathbb{N} \setminus \{d \in \mathbb{N} : d|a \,\text{for some}\, a \in V_n\},$$

being called the set of all non-cancelled numbers.

Our aim is to describe the set $\{b_f(n) : n \in \mathbb{N}\}$ of the least non-cancelled numbers for some special cases of the function f. In the next sections of this paper, we will discuss a few examples of f and find the formulas for the set $\{b_f(n) : n \in \mathbb{N}\}$.

Such modifications of the Eratosthenes sieve and the discriminator are of certain interest, since they develop a way to characterize the primes or a numbers of some special kind, for example those square-free numbers which are the products of primes from some arithmetic progression. Authors of the paper [3] give some details for the function $f(k, l) = k^2 + l^2$ and they obtained that the set $\{b_f(n) : n \geq 2\}$ is equal to $Q \setminus \{1\}$, where Q is the set of all square-free positive integers, which are the products of prime numbers $\equiv 3 \pmod 4$.

2 $f(n) = n^k$ for some natural $k \geq 2$

Let $(r_s)_{s=1}^{\infty}$ be the increasing sequence of all positive square free numbers.

Theorem 2.1. *Let $f : \mathbb{N} \to \mathbb{N}$, $f(n) = n^k$, where $k \geq 2$ is a natural number. If $s > 1$ and $r_{s-1} \leq n < r_s$ then*

$$b_f(n) = r_s.$$

Hence, $\{b_f(n) : n \in \mathbb{N}\}$ is the set of all square-free numbers with the exception of 1.

We will prove this theorem by demonstrating the crucial lemma.

Lemma 2.2. *For $s > 1$ the following inequality holds:*

$$r_s \leq 2r_{s-1}. \tag{2.1}$$

Proof. Follows from the Bertrand's Postulate which states that for every $x \geq 1$ the interval $[x, 2x]$ contains at least one prime, see also [3]. □

Now we can prove our theorem.

Proof. For a given $n \in \mathbb{N}$ we take $s > 1$ such that $r_{s-1} \leq n < r_s$.

We have to prove that r_s is non-cancelled, but every natural number $h < r_s$ is cancelled.

To prove that r_s is non-cancelled, let $r_s | b^k$ for some $b \in \mathbb{N}$. Since r_s is a square-free number, $r_s | b$.

Therefore $b \geq r_s > n$ and r_s is non-cancelled.

Now we assume that $h < r_s$. Let u^2 be the greatest square of some natural number, which is the divisor of h. Clearly, $\frac{h}{u^2}$ is a square-free number. Hence, we may find $j \in \mathbb{N}$ such that

$$h = r_j u^2, \text{ where } 1 \leq j \leq s-1.$$

We put $b = r_j u$ and thus obtain $h | b^k$, since $k \geq 2$. We consider two cases. If $u = 1$ then $b = r_j \leq r_{s-1} \leq n$.

If $u \geq 2$ then $b = \frac{h}{u} \leq \frac{h}{2} < \frac{r_s}{2} \leq r_{s-1} \leq n$, by Lemma 2.2.

Hence, in each case h is cancelled and this is what we need to prove. □

3 $f(n) = n(n+t)$ for some positive square-free number t

Let t be a square-free natural number. We define Q_t as the set of all natural numbers in the form ap^k, where p is a prime number which does not divide t; a is a positive square-free number which divide t and k is the non-negative integer. Let $(q_s)_{s=1}^{\infty}$ be the increasing sequence of all elements of Q_t.

Theorem 3.1. *Let $f : \mathbb{N} \to \mathbb{N}$, $f(n) = n(n+t)$.*
For $n \in \mathbb{N}$, where $n \geq t^2 - t$ we define $s > 1$ such that

$$q_{s-1} \leq n + t \leq q_s - 1. \tag{3.1}$$

Under these conditions, we obtain $b_f(n) = q_s$ and

$$\{b_f(n) : n \geq t^2 - t,\ n \in \mathbb{N}\} = \{q_s \in Q_t :\ q_s > \max\{t^2, t+1\},\ s > 1\}.$$

Remark 3.2. If we take $t = 1$, then $Q_1 = \{p^k : p \text{ is a prime number},\ k \geq 0\}$ and

$$\{b_f(n) : n \in \mathbb{N}\} = \{p^k : p \text{ is a prime number}, k \geq 0\} \backslash \{1, 2\}.$$

Remark 3.3. If we take $t = 2$, then $Q_2 = \{p^k : k \geq 0\} \cup \{2p^k : k \geq 0\}$ and

$$\{b_f(n) : n \geq 2,\ n \in \mathbb{N}\} = (\{p^k : k \geq 0\} \cup \{2p^k : k \geq 0\})\backslash\{1, 2, 3\},$$

where p is an odd prime number.

To prove Theorem 3.1, we need the following lemmas.

Lemma 3.4. *Let $(q_s)_{s=1}^{\infty}$ be the increasing sequence of all elements of Q_t then*

$$q_1 = 1,\ q_2 = 2,\ q_3 = 3 \tag{3.2}$$

and

$$q_s < 2q_{s-1} \text{ for } s > 2. \tag{3.3}$$

Proof. Since $\{1, 2, 3\} \subset Q_t$, we have that (3.2) holds. Moreover, the sequence $(p_n)_{n=1}^{\infty}$ of all prime numbers is a subsequence of $(q_s)_{s=1}^{\infty}$.

Hence, the rest of the proof is the same as in the proof of Lemma 2.2. □

Lemma 3.5. *If for any $q \in Q_t$ there exists $b \in \mathbb{N}$ such that $q|b(b + t)$, then $b + t \geq q$.*

Proof. For any $q \in Q_t,\ q = ap^k$ we take $b \in \mathbb{N}$ such that $q|b(b + t)$.

Let $a = p_1p_2 \cdot \ldots \cdot p_s$, where all $p_1, ..., p_s$ are prime numbers which divide t. We note that if $a = 1$ then $s = 0$. We may assume that

$p_1p_2 \cdot \ldots \cdot p_{s'}|b$ and $p_{s'+1}p_{s'+2} \cdot \ldots \cdot p_s|(b + t)$, where $0 \leq s' \leq s$ since $a|b(b + t)$.

Using the fact that $a \mid t$, we obtain that $a \mid b$ and $a \mid b + t$.

We also have $p^k|b$ or $p^k|(b + t)$ since $p^k|b(b + t)$ and $(t, p) = 1$ from the definition of q. Hence, either $q|b$ or $q|b + t$. Now, it follows that $b + t \geq q$. □

Lemma 3.6. *Let $t \in \mathbb{N}$. For all the numbers in the form $c = c_1c_2 > t^2$ such that both $c_1,\ c_2 \in \mathbb{N}, c_1, c_2 > 1,\ (c_1, c_2) = 1,\ c_1, c_2 \nmid t$, there exists $b \in \mathbb{N}$ satisfying $b + t \leq \frac{c}{2}$ and $c|b(b + t)$.*

Proof. Obviously, we have $\max\{c_1, c_2\} > t$ and $\min\{c_1, c_2\} > 1$, thus $c > 2t$.

If $(c_1, c_2) = 1$ then the numbers in the form

$$f_1c_1 - f_2c_2,$$

where $0 \leq f_1 < c_2,\ 0 \leq f_2 < c_1,\ f_1, f_2 \in \mathbb{Z}$, are pairwise distinct modulo c.

The cardinality of this set is c. Hence they form a complete set of residues modulo c.

In particular, there exist specific $0 \leq f_1 < c_2$ and $0 \leq f_2 < c_1$,
such that $f_1c_1 - f_2c_2 \equiv t\,(mod\, c)$.

From the inequalities $-c < f_1c_1 - f_2c_2 < c$ and $0 \leq t \leq t^2 < c$, there exist $0 \leq f_1 < c_2$ and $0 \leq f_2 < c_1$, such that

$$f_1c_1 - f_2c_2 = t \text{ or } f_1c_1 - f_2c_2 = t - c. \tag{3.4}$$

We have that both $c_1, c_2 \nmid t$, thus in both cases $f_1, f_2 > 0$.

If the second equality of (3.4) holds, then we have $t = f_1c_1 + c - f_2c_2$, hence $t \geq c_1 + c - (c_1 - 1)c_2 = c_1 + c_2$ and $t^2 \geq (c_1 + c_2)^2 > c$, thus we obtain a contradiction. Therefore, we have

$$f_1c_1 - f_2c_2 = t,$$

where $0 < f_1 < c_2$ and $0 < f_2 < c_1$.

Now, taking such f_1 and f_2 we have:

$$b = \begin{cases} (c_2 - f_1)c_1, & \frac{c_2}{2} < f_1 < c_2 \\ f_2c_2, & 0 < f_1 \leq \frac{c_2}{2} \end{cases}$$

and

$$b + t = \begin{cases} (c_1 - f_2)c_2, & \frac{c_2}{2} < f_1 < c_2 \\ f_1c_1, & 0 < f_1 \leq \frac{c_2}{2} \end{cases},$$

hence we obtain $b > 0$.

In the first case of the definition of b we get $b < \frac{c}{2}$.

In the second case of the definition of b we get $b + t \leq \frac{c}{2}$.

Moreover, if in the first case we had $b + t > \frac{c}{2}$, then

$$c - 2b > 0 \text{ and } 2b + 2t - c > 0.$$

From the definition of b we get

$$c_1|c - 2b \text{ and } c_2|(2b + 2t - c).$$

Thus

$$1 \leq c_1 \leq c - 2b \text{ and } 1 \leq c_2 \leq 2b + 2t - c.$$

By the inequality between arithmetic and geometric mean we obtain

$$c \leq (c - 2b)(2b + 2t - c) \leq t^2,$$

which leads to a contradiction.

Therefore, in the first case we also have $b + t \leq \frac{c}{2}$.

We also have

$$b(b + t) = \begin{cases} c_1c_2(c_2 - f_1)(c_1 - f_2), & \frac{c_2}{2} < f_1 < c_2 \\ c_1c_2f_1f_2, & 0 < f_1 \leq \frac{c_2}{2} \end{cases},$$

thus $c|b(b + t)$. □

Lemma 3.7. *Let P denote the set of all prime numbers and t be a square-free number. We have the following decomposition of the set of all natural numbers:*

$$\begin{aligned} \mathbb{N} = \{h :\ & h \leq t^2,\ h \in \mathbb{N}\} \cup \{h : \exists\, p \in P,\ p|t,\ p^2|h,\ h \in \mathbb{N}\} \\ & \cup \{h : h = ap^k, p \in P,\ p \nmid t,\ a|t,\ k \geq 0,\ h \in \mathbb{N}\} \\ & \cup \{h : h = c_1c_2,\ (c_1, c_2) = 1, c_1, c_2 \nmid t,\ c > t^2,\ c_1, c_2 \in \mathbb{N}\}. \end{aligned}$$

Proof. Since t is a square-free number, we get the following partition of $\mathbb{N}$:

$$\begin{aligned}\mathbb{N} = \{h : \exists\, p \in P,\, p|t,\, p^2|h \in \mathbb{N}\} \cup \\ \{h :\, h|t,\, h \in \mathbb{N}\} \cup \{h :\, (h,t) = 1,\, h > 1,\, h \in \mathbb{N}\} \\ \cup\, \{h : h = c_1c_2,\, c_1 = (h,t),\, (c_2,t) = 1,\, c_1, c_2 > 1,\, c_1, c_2 \in \mathbb{N}\}. \quad (3.5)\end{aligned}$$

We have also

$$\begin{aligned}\{h :\, (h,t) = 1,\, h > 1,\, h \in \mathbb{N}\} = \{h : h = p^k,\, p \in P,\, k \geq 1,\, p \nmid t\} \\ \cup\, \{h :\, h = c_1c_2, (c_1,t) = 1,\, (c_2,t) = 1,\, (c_1,c_2) = 1,\, c_1, c_2 > 1\} \quad (3.6)\end{aligned}$$

and

$$\begin{aligned}\{h : h = c_1c_2,\, c_1 = (h,t),\, (c_2,t) = 1,\, c_1, c_2 > 1,\, c_1, c_2 \in \mathbb{N}\} = \quad (3.7) \\ =\, \{h : c_1p^k,\, c_1 = (h,t),\, p \nmid t,\, k \geq 1,\, c_1 > 1,\, p \in P,\, c_1 \in \mathbb{N}\} \\ \cup \{h :\, h = c_1ab,\, c_1 = (h,t),\, (ab,t) = 1,\, (a,b) = 1,\, c_1, a, b > 1, c_1, a, b \in \mathbb{N}\} \\ \subseteq \{h : c_1p^k,\, c_1 = (h,t),\, p \nmid t,\, k \geq 1,\, c_1 > 1,\, p \in P,\, c_1 \in \mathbb{N}\} \\ \cup \{h : h = e_1e_2,\, (e_1,e_2) = 1, e_1, e_2 \nmid t,\, e_1 = c_1a, e_2 = b,\, c_1, a, b \in \mathbb{N}\}.\end{aligned}$$

From (3.5), (3.6) and (3.7) we obtain

$$\begin{aligned}\mathbb{N} \subseteq \{h :\, h \leq t^2,\, h \in \mathbb{N}\} \,\cup\, \{h : \exists\, p \in P,\, p|t,\, p^2|h,\, h \in \mathbb{N}\} \\ \cup \{h : h = ap^k, p \in P,\, p \nmid t,\, a|t,\, k \geq 0\} \\ \cup \{h : h = c_1c_2,\, (c_1,c_2) = 1, c_1, c_2 \nmid t,\, c > t^2,\, c_1, c_2 \in \mathbb{N}\}\end{aligned}$$

and the lemma follows. □

Now we will prove the main theorem in this section.

Proof. We have to prove that every number $q_s \in Q_t,\, q_s > \max\{t^2, t+1\},\, s > 1$ is non-cancelled, but every $h < q_s$ is cancelled.

Let $s > 1$ and $q_s|b(b+t)$ for some $b \in \mathbb{N}$. By Lemma (3.5) combined with the inequality (3.1) we have $b \geq q_s - t > n$. Therefore, q_s is non-cancelled.

Let $h < q_s$. By Lemma 3.7, h satisfies one of the following conditions. We shall prove that in each case h is cancelled.

a) If $h = 1$, then put $b = 1$ and get $h|b(b+t)$, where $b = 1 \leq n$.

b) If $h \leq t^2$, where $t > 1$, then we consider a few subcases:

1) If $h = 2, \ldots, t^2 - t, t > 1$, then put $b = h$ and get $h|b(b+t)$, where $0 < b = h \leq t^2 - t \leq n$.

2) If $h = t^2 - (t-1), \ldots, t^2, t > 1$, then put $b + t = h$ and get $h|b(b+t)$, where $0 < b = h - t \leq t^2 - t \leq n$.

c) If $h = q_j$, where $1 \leq j \leq s-1,\ q_j > t^2$, then put $b = q_j - t > 0$ and get $h|b(b+t)$, where $b = q_j - t \leq q_{s-1} - t \leq n$, by (3.1).

d) If $h = p^2c > t^2$, where p is a prime number such that $p|t$ and $c \in \mathbb{N}$, then put $b = pc - t = \frac{1}{p}p^2c - t > \frac{t^2}{p} - t \geq 0$. We have also $b = pc - t = \frac{h}{p} - t \leq \frac{h}{2} - t \leq \frac{1}{2}(q_s - 1) - t \leq q_{s-1} - 1 - t < n$, by Lemma 3.4 and inequality (3.1). We get $b(b+t) = (pc-t)pc$, but $p|t$, thus $h|b(b+t)$.

e) If $h = c$, where $c = c_1c_2,\ (c_1, c_2) = 1, c_1, c_2 \nmid t,\ c > t^2$ and $c_1, c_2 \in \mathbb{N}$, then by Lemma (3.6) we may find $b \in \mathbb{N}$ such that $b + t \leq \frac{c}{2}$ and $h|b(b+t)$. We obtain $b + t \leq \frac{h}{2} \leq \frac{1}{2}(q_s - 1) \leq q_{s-1} - 1$, by Lemma 3.4, thus $b < q_{s-1} - t \leq n$, by (3.1).

In each case we have proved that $b \leq n$, so h is cancelled.

To summarize, we have shown that every $h < q_s$ is cancelled and this is precisely what we want to prove. □

4 $f(n_1, n_2) = n_1n_2$

Our aim in this chapter is to find and algorithm which gives only prime numbers p_s.

Theorem 4.1. *Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N},\ f(k,l) = kl$. We have*

$$b_f(1) = 1,\ b_f(2) = 2$$

and if $n > 2$ then $b_f(n) = p_s$, where $s > 1$ is chosen in the way that $p_{s-1} < n \leq p_s$.

Proof. By a straightforward verification we get

$$b_f(1) = 1,\ b_f(2) = 2.$$

Let $n > 2$. We assume that $p_{s-1} < n \leq p_s,\ s > 1$.

We have to prove that p_s is non-cancelled, but any natural number $h < p_s$ is cancelled.

First, let $p_s|ab$ for some $a, b \in \mathbb{N}$. Thus $p_s|a$ or $p_s|b$ and $a + b > p_s \geq n$. Therefore, a number p_s is non-cancelled.

We assume now that $h < p_s$. To show that h is cancelled, we need to consider two cases separately.

a) If $h = p_j$, where $j \in \mathbb{N}$ and $j \leq s-1$, then we take $a = 1,\ b = p_j$ and get $h|ab$ with $a + b = 1 + p_j \leq 1 + p_{s-1} \leq n$, thus such h is cancelled.

b) If $h = kl$, where $k, l > 1,\ k, l \in \mathbb{N}$, we have $(k-2)(l-2) \geq 0$, hence $k + l \leq \frac{1}{2}kl + 2$. We take $a = k,\ b = l$ and get $h|ab$.

From Chebyshev's theorem we have $p_s < 2p_{s-1}$ for $s > 1$. Hence,

$$a + b = k + l \leq \tfrac{1}{2}kl + 2 = \tfrac{1}{2}h + 2 \leq \tfrac{1}{2}(p_s - 1) + 2 = \tfrac{1}{2}(p_s + 1) + 1 \leq p_{s-1} + 1 \leq n,$$

thus such h is cancelled.

To summarize, we have shown that every $h < p_s$ is cancelled and this is the end of the proof. □

Remark 4.2. The set $\{b_f(n) : n > 1,\ n \in \mathbb{N}\}$ is the set of all prime numbers.

5 $f(n_1, n_2) = n_1^3 + n_2^3$

We denote by T the set of all square-free positive integers being the products of arbitrarily many prime numbers, which are not congruent to 1 modulo 6.

Let $(t_s)_{s=1}^{\infty}$ be the increasing sequence of all elements of T.

We notice that $t_1 = 1$, which corresponds to the empty product.

Thus:

$$T = \{1, 2, 3, 5, 6, 10, 11, 15, 17, 22, \ldots\}.$$

Theorem 5.1. *Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(k, l) = k^3 + l^3$. We have*

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

$b_f(n) = t_s$ if $n \geq 4$ and s is chosen in the way that

$$t_{s-1} \leq n < t_s. \tag{5.1}$$

Again, to prove our theorem, we need to prove a few lemmas. The following lemma gives us some estimates on the growth rate of the sequence $(t_s)_{s=1}^{\infty}$.

Lemma 5.2. *For a positive integer $s > 4$ we have that*

$$t_s \leq \tfrac{151}{100} \cdot t_{s-1}. \tag{5.2}$$

Proof. Follows from the fact that for every $x > 21$ the interval $(x, \frac{151}{100}x)$ contains at least one prime $\equiv 5 \pmod 6$, see [10]. □

Lemma 5.3. *For $s > 0$ and $a, b \in \mathbb{N}$ if $t_s | (a^3 + b^3)$, then $t_s | (a + b)$.*

Proof. Let $t_s | (a^3 + b^3)$ for some $a, b \in \mathbb{N}$.

We fix a prime number p. If $p | t_s$, then $p | (a^3 + b^3)$.

Moreover, for $p = 2$ and $p = 3$ if $p | (a^3 + b^3)$, then $p | (a + b)$.

We now assume that $p \nmid (a + b)$. We have $p | (a^2 - ab + b^2)$.

However, if $p | b$, then $p | a$ and hence $p | (a + b)$, what leads to a contradiction.

We may assume that $p \nmid b$, hence we can find an integer c such that

$$cb \equiv 1 \pmod p. \tag{5.3}$$

The following equality holds:

$$(2ac - bc)^2 + 3(bc)^2 = 4c^2(a^2 - ab + b^2),$$

thus

$$p | (2ac - bc)^2 + 3(bc)^2.$$

From (5.3) we have

$$-3 \equiv (2ac - bc)^2 \pmod p,$$

we thus obtain that -3 is quadratic residue modulo p, where $p \neq 2, 3$.

As is known, this implies that $p \equiv 1 \pmod 6$ (see [7]). Hence, from the definition of t_s we have $p \nmid t_s$ and thus we get a contradiction. Therefore, $p | (a + b)$.

Since t_s is square-free, we also get $t_s | (a + b)$, which completes the proof. □

Now, we may prove the main theorem in this section.

Proof. If $n \in \{1, 2, 3, 4\}$, then by a straightforward verification we get

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

and thus our theorem holds.

Let $n \geq 5$. We assume that $t_{s-1} \leq n < t_s$, hence $t_s > 5$ and $s \geq 5$.

We have to prove that t_s is non-cancelled, but any natural number $h < t_s$ is cancelled.

First, let $t_s|(a^3 + b^3)$ for some $a, b \in \mathbb{N}$. By Lemma 5.3 we obtain $t_s|(a + b)$, where $a + b \geq t_s > n$. Therefore, a number t_s is non-cancelled.

We now assume that $h < t_s$. To show that h is cancelled, we need to consider separately a few cases.

a) If $h = t_j > 1$, where $j \in \mathbb{N}$ and $j \leq s - 1$, then we take $a = 1$,

$b = t_j - 1 > 0$ and get $h|(a^3 + b^3)$ with $a + b = t_j \leq t_{s-1} \leq n$,

thus such h is cancelled.

b) If $h = k^2 l$, where $k, l \in \mathbb{N}$, then we consider few subcases:

1) If $h = k^2 l$, where $k, l \in \mathbb{N}$, $k > 3$, then we take $a = b = kl$ and get $h|(a^3 + b^3)$, where $a + b = 2kl \leq \frac{2}{k} k^2 l \leq \frac{2}{4} k^2 l = \frac{1}{2} h < \frac{1}{2} t_s < t_{s-1} \leq n$, thus such h is cancelled.

2) If $h = 9l$, where $l \in \mathbb{N}$, then we take $a = l, b = 2l$ and get $h|(a^3 + b^3)$. By inequalities (5.2) and (5.1) we obtain $a + b = 3l = \frac{h}{3} < \frac{t_s}{3} < t_{s-1} \leq n$, thus such h is cancelled.

3) If $h = 4l$, where $l \in \mathbb{N}$, $l > 1$ then we take $a = 2, b = 2l - 2$ and get $h|(a^3 + b^3)$. By inequalities (5.2) and (5.1) we obtain $a + b = 2l = \frac{h}{2} < \frac{t_s}{2} < t_{s-1} \leq n$, thus such h is cancelled.

4) If $h = 4$, then we take $a = 2, b = 2$ and get $h|(a^3 + b^3)$. By inequalities $s \geq 5$ and (5.1) we obtain $a + b = 4 < t_4 \leq t_{s-1} \leq n$, thus such h is cancelled.

5) If $h = 1$, then we take $a = b = 1$ and get $h|(a^3 + b^3)$, where $a + b = 2 < t_3 < t_{s-1} \leq n$, thus 1 is cancelled.

c) If h is a square-free number, which is divisible by a prime congruent to 1 modulo 6 then we consider few subcases:

1) If h is a square-free number and $7|h$ then $h = 7g$ for some $g \in \mathbb{N}$. We take $a = 3g$, $b = g$ and get $h|(a^3 + b^3)$. By inequalities (5.2) and (5.1) we obtain $a + b = 4g = \frac{4}{7} h < \frac{4}{7} t_s < t_{s-1} \leq n$, thus such h is cancelled.

2) If h is square-free number, which is divisible by a prime $p > 7$ congruent to 1 modulo 6, then $h = pg$, where $p \geq 13$, $g \in \mathbb{N}$.
By Theorem 5, Chapter 9.2 in [7] we may find $x, y \in \mathbb{N}$ such that $p = 3x^2 + y^2$.
Note that

$$3x + y \leq 2\sqrt{3x^2 + y^2} = 2\sqrt{p}. \tag{5.4}$$

We take $a = 2xg$, $b = (x+y)g$ and obtain $g|(a+b)$, $p|g^2(3x^2+y^2) = (a^2-ab+b^2)$. Hence $h|(a+b)(a^2-ab+b^2) = a^3+b^3$.

By inequalities (5.2), (5.1) and (5.4) and we obtain

$$a+b = (3x+y)g < 2\sqrt{p}g = 2\frac{h}{\sqrt{p}} < 2\frac{t_s}{\sqrt{p}} \leq 2\frac{t_s}{\sqrt{13}} < t_{s-1} \leq n,$$

thus such h is cancelled.

To summarize, we have shown that every $h < t_s$ is cancelled and now our proof is over. □

6 A modification of the second generalization

In this section we introduce and investigate certain modification of the second generalization case [3].

Consider an arbitrary function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and the set

$$A_n := \{f(k,l) : k+l \leq n,\ k,l \in \mathbb{N}\}$$

Cancel in $\mathbb{N}$ all numbers $d \in \mathbb{N}$ such that d^2 is a divisor of some number in A_n and define $b_f^{(2)}(n)$ as the least non-cancelled number. Here we give the details for the function $f(k,l) = k^2+l^2$.

Denote by F the set of all positive integers which are the products of prime numbers $\not\equiv 1 \pmod 4$.

Let $(q_s)_{s=1}^{\infty}$ be the increasing sequence of all elements of F.

In particular, $q_1 = 1$, which corresponds to the empty product. Thus we obtain that

$$F = \{1,2,3,4,6,7,8,9,11,12,14,16,18,19,21,22,23,24,27,28,31,\ldots\}.$$

Lemma 6.1. *We have*

$$q_s < \tfrac{4}{3}q_{s-1} \text{ for } s > 5. \tag{6.1}$$

Proof. The sequence $(v_n)_{n=1}^{\infty}$ of all prime numbers $\equiv 7 \pmod{12}$ is a subsequence of $(q_s)_{s=1}^{\infty}$. We have $v_1 = q_6 = 7$. Hence, for every $q_s > 7$ there exists $n \in \mathbb{N}$ such that

$$v_{n-1} < q_s \leq v_n. \tag{6.2}$$

Therefore, $v_{n-1} \leq q_{s-1}$ and

$$1 < \frac{q_s}{q_{s-1}} \leq \frac{v_n}{v_{n-1}}. \tag{6.3}$$

It is known that

$$v_n < \tfrac{4}{3}v_{n-1} \tag{6.4}$$

for $n > 118$ (see [4] and [5]).

From direct computation we also get that

$$v_n < \tfrac{4}{3}v_{n-1} \tag{6.5}$$

for $118 \geq n > 5$ (note that $v_{118} = 3331$ and $v_5 = 67$).

Using (6.3), (6.4) and (6.5) we obtain

$$q_s < \tfrac{4}{3} q_{s-1} \text{ for } q_s > v_5 = 67.$$

Again, by calculation we get that

$$q_s < \tfrac{4}{3} q_{s-1} \text{ for } s > 5. \qquad \square$$

Lemma 6.2. *We assume that a, b and $t \geq 0$ are some integer numbers.*
If $p = 2$ or p is any prime number $\equiv 3 \pmod 4$, then

$$a^2 + b^2 \equiv 0 \pmod{p^{2t}} \text{ implies that } a \equiv b \equiv 0 \pmod{p^t}. \tag{6.6}$$

Proof. Our lemma is obvious for $t = 0$, so we may assume that $t \geq 1$.

Since -1 is not a quadratic residue modulo any prime $p \equiv 3 \pmod 4$, the divisibility $p^2 | a^2 + b^2$ implies that $a \equiv b \equiv 0 \pmod p$.

Moreover, if $2^2 | a^2 + b^2$, then $a \equiv b \equiv 0 \pmod 2$. Thus, the implication (6.6) holds for $t = 1$.

In consequence, the whole lemma follows by induction on t. $\square$

Lemma 6.3. *If $q \in F$ satisfies $q^2 | a^2 + b^2$ for some $a, b \in \mathbb{N}$, then $a + b \geq 2q$.*

Proof. We assume that there exist some natural numbers a, b such that

$$q^2 | a^2 + b^2. \tag{6.7}$$

Our lemma is obvious for $q = 1$, so we may assume that $q > 1$.

Using Lemma 6.2 to all prime divisors of q we get $a \equiv b \equiv 0 \pmod q$, since $q^2 | a^2 + b^2$.

Thus we have $a, b \geq q$, so $a + b \geq 2q$ and our lemma follows. $\square$

Theorem 6.4. *Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(k, l) = k^2 + l^2$. We have $b_f^{(2)}(1) = 1$ and for $n \geq 2$*

$$b_f^{(2)}(n) = q_s, \text{ if } 2q_{s-1} \leq n < 2q_s,$$

where $s \geq 2$. Hence, the set $\{b_f^{(2)}(n) : n \in \mathbb{N}\}$ is equal to F.

Proof. We fix $n \geq 2$. Let $s \geq 2$ be a natural number such that

$$2q_{s-1} \leq n < 2q_s. \tag{6.8}$$

We will show that q_s is non-cancelled. Let $q_s^2 | k^2 + l^2$ for some $k, l \in \mathbb{N}$.

By lemma 6.3 we have

$$k + l \geq 2q_s, \tag{6.9}$$

thus $k + l > n$ and q_s is non-cancelled.

We now assume that $h < q_s$. We will show that h is cancelled.

If $h < q_s$, then it fulfills one of the following conditions:

a) $h = q_j$, where $j \leq s - 1$ and $q_j \in F$,

b) h has at least one prime divisor $\equiv 1 \, (mod\, 4)$.

We will show that in both cases h is cancelled. Namely,
a) We take $k = l = q_j$, then $h^2|k^2 + l^2$ and $k + l = 2q_j \leq 2q_{s-1} \leq n$ by the inequalities (6.8).
b) By (Theorem 2, Chapter 11.3 in [7]) it follows that h^2 is the sum of the squares of two natural numbers, say k, l.

Moreover $h^2|k^2 + l^2$.

By the inequality between arithmetic mean and quadratic mean we get

$$k + l \leq \sqrt{2}\sqrt{k^2 + l^2} = \sqrt{2}h,$$

thus

$$k + l < \sqrt{2}q_s < \tfrac{4}{3}\sqrt{2}q_{s-1} < 2q_{s-1} \leq n,$$

by Lemma 6.1.

In each case we have proved that $k + l \leq n$, so h is cancelled and the proof is over. □

7 Upper bounds for generalized discriminator

We finish our work with the following statements.

Theorem 7.1. *For the function $f : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ given by the formula $f(k, l, m) = k^2 + l^2 + m^2$, we have $b_f(1) = b_f(2) = 1$, $b_f(3) = 2$ and for any integer $s \geq 1$ we obtain:*

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

Proof. Note that $b_f(1) = 1$, $b_f(2) = 1$, $b_f(3) = 2$. We fix $n \geq 3$. Assume that the first case holds. Let $s \geq 1$ be a natural number such that

$$2 \cdot 2^s \leq n < 3 \cdot 2^s \tag{7.1}$$

It remains to show that 4^s is non-cancelled. Let $4^s|k^2 + l^2 + m^2$ for some $k, l, m \in \mathbb{N}$, thus $2^s|k$, $2^s|l$, $2^s|m$. Therefore $k + l + m \geq 3 \cdot 2^s > n$ and so 4^s is non-cancelled.

In the second case let $s \geq 1$ be a natural number such that

$$3 \cdot 2^s \leq n < 2 \cdot 2^{s+1} \tag{7.2}$$

It suffices to show that $5 \cdot 4^{s-1}$ is non-cancelled.

Let $5 \cdot 4^{s-1}|k^2 + l^2 + m^2$ for some $k, l, m \in \mathbb{N}$. Hence $2^{s-1}|k$, $2^{s-1}|l$, $2^{s-1}|m$.

We may write $5|\left(2^{1-s}k\right)^2 + \left(2^{1-s}l\right)^2 + \left(2^{1-s}m\right)^2$, where $2^{1-s}k, 2^{1-s}l, 2^{1-s}m \in \mathbb{N}$.

Therefore $2^{1-s}k + 2^{1-s}l + 2^{1-s}m \geq 8$.

Since $k + l + m \geq 2 \cdot 2^{s+1} > n$, we obtain that $5 \cdot 4^{s-1}$ is non-cancelled. □

Remark 7.2. We conjecture that in this case

$$\{b_f(n) : n \in \mathbb{N}\} = \{2\} \cup \{4^n : n \geq 0\} \cup \{5 \cdot 4^n : n \geq 0\}.$$

In the second theorem we consider squares of the divisors of the values of f.

Theorem 7.3. *For the function* $f : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *given by the formula* $f(k,l,m) = k^2 + l^2 + m^2$, *we have* $b_f^{(2)}(1) = 1$, $b_f^{(2)}(2) = 1$, *and for* $n \geq 3$

$$b_f^{(2)}(n) \leq 2^{\lceil \log_2 \frac{n}{3} \rceil}.$$

Proof. Note that $b_f^{(2)}(1) = 1$, $b_f^{(2)}(2) = 1$. We fix $n \geq 3$. Let $s \geq 2$ be a natural number such that

$$3 \cdot 2^{s-2} \leq n < 3 \cdot 2^{s-1}. \tag{7.3}$$

It remains to show that 2^{s-1} is non-cancelled. Let $\left(2^{s-1}\right)^2 | k^2 + l^2 + m^2$ for some $k, l, m \in \mathbb{N}$. Hence $4^{s-1} | k^2 + l^2 + m^2$ thus $2^{s-1} | k$, $2^{s-1} | l$, $2^{s-1} | m$.

Therefore $k + l + m \geq 3 \cdot 2^{s-1} > n$ and 2^{s-1} is non-cancelled. □

Remark 7.4. We conjecture that in this case $b_f^{(2)}(n) = 2^{\lceil \log_2 \frac{n}{3} \rceil}$ for $n \geq 3$ and that $\{b_f^{(2)}(n) : n \in \mathbb{N}\} = \{2^{s-1} : s \geq 1\}$.

Acknowledgements

We would like to thank Prof. Jerzy Browkin for inspiring discussions.

References

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

[2] Bremser, P. S., Schumer, P. D., & Washington, L.C. (1990) A note on the incongruence of consecutive integers to a fixed power, *J. Number Theory*, 35(1), 105–108.

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

[4] Molsen, K. (1941) Zur Verallgemeinerung des Bertrandschen Postulates, *Deutsche Math.*, 6, 248–256.

[5] Moree, P. (1993) Bertrand's postulate for primes in arithmetical progressions, *Comput. Math. Appl.*, 26, 35–43.

[6] Moree, P. (1996) The incongruence of consecutive values of polynomials, *Finite Fields Appl.*, 2(3), 321–335.

[7] Sierpiński, W. (1988) *Elementary Theory of Numbers*, Ed. by A. Schinzel, North-Holland

[8] Sun, Z. W. (2013) On functions taking only prime values, *J. Number Theory*, 133, 2794–2812.

[9] Sun, Z. W. (2013) On primes in arithmetic progressions, available at arXiv:1304.5988v4.

[10] Zieve, M. (1998) A note on the discriminator, *J. Number Theory*, 73(1), 122–138.