On some cancellation algorithms

Maciej Zakarczemny

Cracow University of Technology, Poland

Conference on Rings and Polynomials

Graz

July 05, 2016

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

$$D_g(n) := \min\{m \in \mathbb{N} :\ g(1), g(2), \ldots, g(n) \textit{ are distinct modulo } m\} \qquad (1)$$

The function D_g is commonly called the discriminator of the function g.

Remark: By $\mathbb{N}$ we denote the set of positive integers.

Arnold, Benkoski, and McCabe [1] defined, for a 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 $D_g(n)$ for $n > 4$ is the smallest $m \geq 2n$ such that m is a prime or twice a prime.

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

Later authors tried to generalize it to the cyclic polynomials $g(x) = x^j$, where j is any natural number, see [2],

Moree and Mullen [8] give the asymptotic characterization of $D_{g_j(x,a)}(n)$, where

$$g_j(x, a) = \sum_{i=0}^{\lfloor \frac{j}{2} \rfloor} \frac{j}{j-i} \binom{j-i}{i} (-a)^i x^{j-2i} \in \mathbb{Z}[x]$$

is the Dickson polynomial of degree $j \geq 1$ and parameter $a \in \mathbb{Z}$.

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

[8] P. Moree and G. L. Mullen, Dickson polynomial discriminators, J. Number Theory 59 (1996), 88-105.

The characterization of the discriminator for permutation polynomials was made in papers [6] and [11].

Let R be a finite commutative ring. A polynomial $f \in R[x]$ is said to be a permutation polynomial of R if it permutes the elements of R under the evaluation mapping $x \mapsto f(x)$.
In paper [6] author give conditions for f to have an asymptotic characterization of the form

$$D_f(n) = \min\{k \geq n : \ f \ permutes \ \mathbb{Z}/k\mathbb{Z}\}.$$

[6] P. Moree, *The incongruence of consecutive values of polynomials*, Finite Fields Appl. 2 (1996), no. 3, 321-335.

[11] M.Zieve, *A note on the discriminator*, J. Number Theory 73 (1998), no. 1, 122-138.

Here we generalize the notion of discriminator and compute some of its values using methods from the elementary number theory.

Browkin and Cao in the paper [3] stated (1) equivalently in terms of the following cancellation algorithm.

For $n \geq 2$ define the set

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

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

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

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

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

Definition

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

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

being called the set of all non-cancelled numbers.

Example

If $D_n = \{d \in \mathbb{N} : \exists_{n_1, n_2 \in \mathbb{N},\, n_1+n_2 \le n} \;\; d | (n_1+n_2)^2 - {n_2}^2\}$ and $b_f(n)$ is the least number in the set $\mathbb{N} \setminus D_n$ then

$V_1 = \emptyset$ $D_1 = \emptyset$	$b_f(1) = 1$,
$V_2 = \{3\}$ $D_2 = \{1, 3\}$	$b_f(2) = 2$,
$V_3 = \{3, 5, 8\}$ $D_3 = \{1, 2, 3, 4, 5, 8\}$	$b_f(3) = 6$,
$V_4 = \{3, 5, 7, 8, 12, 15\}$ $D_4 = \{1, 2, 3, 4, 5, 6, 7, 8, 12, 15\}$	$b_f(4) = 9$,
$V_5 = \{3, 5, 7, 8, 9, 12, 15, 16, 21, 24\}$ $D_5 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 15, 16, 21, 24\}$	$b_f(5) = 10$,
$V_6 = \{3, 5, 7, 8, 9, 11, 12, 15, 16, 20, 21, 24, 25, 27, 32, 35\}$ $D_6 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 15, 16, 20, 21, 24, 27, 32, 35\}$	$b_f(6) = 13$,
$V_7 = \{3, 5, 7, 8, 9, 11, 12, 13, 15, 16, 20, 21, 24, 25, 27, 32, 33, 35, 45, 48\}$ $D_7 = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16, 20, 21, 24, 25, 27, 32, 33, 35, 45, 48\}$	$b_f(7) = 14$,
...	...

Note that $V_n = \{g(s) - g(r) : 1 \le r < s \le n\}$, where $g : \mathbb{N} \ni r \to r^2 \in \mathbb{N}$.
In this case $f(n_1, n_2) = (n_1+n_2)^2 - n_1^2$ and $b_f(n)$ is equal to the discriminator $D_{r^2}(n)$.

Hence for $n > 4$ we get that $b_f(n)$ is the smallest $m \ge 2n$ such that m is a prime or twice a prime.

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.

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 squarefree numbers which are the products of primes from some arithmetic progression.

The authors of [3] gave 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 squarefree positive integers, which are the products of prime numbers $\equiv 3 \pmod 4$.

$$Q = \{1, 3, 7, 11, 19, 21, 23, 31, 33, 43, 47, 57, 59, \ldots\}.$$

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

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

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

Theorem

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 squarefree numbers with the exception of 1.

Q_t

Let t be a squarefree 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 squarefree number which divide t and k is the non-negative integer.

Example

$Q_1 = \{1, 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, \ldots\}$,
$Q_2 = \{1, 2, 3, 5, 6, 7, 9, 10, 11, 13, 14, 17, 18, 19, \ldots\}$,
$Q_3 = \{1, 2, 3, 4, 5, 6, 7, 8, 11, 12, 13, 15, 16, 17, 19, \ldots\}$,
$Q_5 = \{1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 13, 15, 16, 17, 19, \ldots\}$,
$Q_6 = \{1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, \ldots\}$.

$f(n) = n(n+t)$ for some positive squarefree number t

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

Theorem

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

$$q_{s-1} \leq n + t \leq q_s - 1. \tag{2}$$

Then $b_f(n) = q_s$ and

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

$f(n) = n(n+1)$ or $f(n) = n(n+2)$

Remark

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

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

$$= \{3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, \ldots\}.$$

Remark

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

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

$$= \{5, 6, 7, 9, 10, 11, 13, 14, 17, 18, 19, \ldots\}.$$

where p is an odd prime number.

$f(n_1, n_2) = n_1 n_2$

Our aim in this theorem is to find an algorithm which gives only prime numbers p_s.

Theorem

Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(n_1, n_2) = n_1 n_2$. *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* $p_{s-1} < n \leq p_s$.

Remark

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

We give a short and simple proof of the above theorem.

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 the Bertrand's Postulate (Chebyshev's theorem) we have $p_s < 2p_{s-1}$ for $s > 1$. Hence,

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

thus such h is cancelled.

To summarize, we have shown that every $h < p_s$ is cancelled. □

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

We denote by T the set of all squarefree 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.

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

(In another words $t \in T$ if t is squarefree positive integer and $(3, \varphi(t)) = 1$.).

Furthermore $\varphi(k)$ denotes Euler's totient function and (a, b) denotes the greatest common divisor of a and b.

Theorem

Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(n_1, n_2) = {n_1}^3 + {n_2}^3$. *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*

$$t_{s-1} \leq n < t_s. \quad (3)$$

$f(n_1, n_2) = n_1^j + n_2^j$

Theorem

For $j > 1$ odd, let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(n_1, n_2) = {n_1}^j + {n_2}^j$. Then

$$b_f(n) \leq \min\{k : k > n,\ k \textit{ is squarefree},\ (j, \varphi(k)) = 1\}.$$

Remark

Let $j > 1$ be an odd number. We conjecture that for sufficiently large $n \geq 4$ we have

$$b_f(n) = \min\{k : k > n,\ k \textit{ is squarefree},\ (j, \varphi(k)) = 1\}$$

.

$f(n_1, n_2, n_3) = {n_1}^2 + {n_2}^2 + {n_3}^2$

Theorem

For the function $f : \mathbb{N}^3 \to \mathbb{N}$ *given by the formula* $f(n_1, n_2, n_3) = {n_1}^2 + {n_2}^2 + {n_3}^2$*, we have* $b_f(1) = b_f(2) = 1$*,* $b_f(3) = 2$ *and for any integer* $s \geq 1$ *we obtain:*

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

Remark

We conjecture that for any integer $s \geq 1$:

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

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

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

Cancel in $\mathbb{N}$ all numbers $d \in \mathbb{N}$ such that d^2 is a divisor of some number in V_n and define $b_f^{(2)}(n)$ as the least non-canceled number.

$f(n_1, n_2) = {n_1}^2 + {n_2}^2$ and $b_f^{(2)}$

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.

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

Theorem

Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $f(n_1, n_2) = {n_1}^2 + {n_2}^2$. 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.

$f(n_1, n_2, n_3) = {n_1}^2 + {n_2}^2 + {n_3}^2$ and $b_f^{(2)}$

Theorem

For the function $f : \mathbb{N}^3 \to \mathbb{N}$ given by the formula $f(n_1, n_2, n_3) = {n_1}^2 + {n_2}^2 + {n_3}^2$, we have $b_f^{(2)}(1) = 1$, $b_f^{(2)}(2) = 1$, and for $n \geq 3$

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

Remark

We conjecture that for any $n \geq 3$ we have $b_f^{(2)}(n) = 2^{\left\lceil \log_2 \frac{n}{3} \right\rceil}$.

$f(n_1, n_2, n_3) = {n_1}^3 + {n_2}^3 + {n_3}^3$

Problem

For the function $f : \mathbb{N}^3 \to \mathbb{N}$ *given by the formula* $f(n_1, n_2, n_3) = {n_1}^3 + {n_2}^3 + {n_3}^3$. *We have*

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

.

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

.

Find and prove an explicit formula for the above sequence.

First remark: Unfortunately, it is not always easy to come up with explicit formulas, when all you have is a list of the terms.

Second remark: Can you prove the formula you conjectured?

$f(n_1, n_2, n_3, n_4) = {n_1}^2 + {n_2}^2 + {n_3}^2 + {n_4}^2$

Problem

For the function $f : \mathbb{N}^4 \to \mathbb{N}$ given by the formula $f(n_1, n_2, n_3, n_4) = {n_1}^2 + {n_2}^2 + {n_3}^2 + {n_4}^2$. We have

n	$1, 2, 3$	$4, 5$	$6, 7$	$8, 9$	$10, 11$	$12, \dots, 15$	16	$17, \dots, 23$
$b_f(n)$	1	3	8	17	24	32	89	96

.

n	$24, \dots, 31$	$32, \dots, 47$	$48, \dots, 63$
$b_f(n)$	128	384	512

.

We conjecture that for any integer $s \geq 3$:

1) *If $3 \cdot 2^s \leq n < 4 \cdot 2^s$, then $b_f(n) = 2 \cdot 4^s$,*

2) *If $4 \cdot 2^s \leq n < 3 \cdot 2^{s+1}$, then $b_f(n) = 6 \cdot 4^s$.*

$f(n_1, n_2, n_3, n_4, n_5) = {n_1}^2 + {n_2}^2 + {n_3}^2 + {n_4}^2 + {n_5}^2$

Problem

For the function $f : \mathbb{N}^5 \to \mathbb{N}$ *given by the formula* $f(n_1, n_2, n_3, n_4, n_5) = {n_1}^2 + {n_2}^2 + {n_3}^2 + {n_4}^2 + {n_5}^2$. *We have*

n	1, 2, 3, 4	5	6, 7, 8	9	10	11	12, 13, 14, 15	16	17	18, 19, 20	21	22	23, 24
$b_f(n)$	1	2	3	6	9	15	33	73	90	105	132	153	193

,

n	25	26	27	28	29	30	31, 32	33	34	35, 36	37	38, 39, 40	41	42
$b_f(n)$	210	225	288	297	318	321	353	432	441	513	570	585	732	793

.

n	43, 44, 45, 46	47, 48	49, 50	51	52	53, 54	55, 56	57	58	59, 60	61	
$b_f(n)$	825	1065	1185	1212	1257	1425	1473	1500	1617	1737	1860	

.

Find and prove an explicit formula for the above sequence.

$f(n_1, n_2, n_3) = \frac{n_1(n_1+1)}{2} + \frac{n_2(n_2+1)}{2} + \frac{n_3(n_3+1)}{2}$, sum of three triangular numbers

Problem

For the function $f : \mathbb{N}^3 \to \mathbb{N}$ *given by the formula* $f(n_1, n_2, n_3) = \frac{n_1(n_1+1)}{2} + \frac{n_2(n_2+1)}{2} + \frac{n_3(n_3+1)}{2}$. *We have*

n	$1, 2$	$3, 4$	5	$6, 7, 8$	$9, 10$	$11, \ldots, 14$	15	16	17	$18, 19$
$b_f(n)$	1	2	6	11	20	29	53	69	76	81

n	20	21	22	$23, 24$	25	$26, 27$	28	$29, 30$	$31, 32, 33$	34
$b_f(n)$	105	106	110	119	146	179	188	218	254	272

Find and prove an explicit formula for the above sequence.

- L.K. Arnold, S.J. Benkoski and B.J. McCabe, *The discriminator (a simple application of Bertrand's postulate)*, Amer. Math. Monthly (1985), 92, 275-277.
- P. S. Bremser, P.D. Schumer, L.C. Washington, *A note on the incongruence of consecutive integers to a fixed power*, J. Number Theory (1990), 35, no. 1, 105-108.
- J. Browkin, H-Q. Cao, *Modifications of the Eratosthenes sieve*, Colloq. Math. 135, (2014), pp. 127-138.
- K. Molsen, *Zur Verallgemeinerung des Bertrandschen Postulates*, Deutsche Math. 6 (1941), 248-256.
- P. Moree, *Bertrand's postulate for primes in arithmetical progressions*, Comput. Math. Appl. 26 (1993), 35-43.
- P. Moree, *The incongruence of consecutive values of polynomials*, Finite Fields Appl. 2 (1996), no. 3, 321-335.
- P. Moree and G. L. Mullen, Dickson polynomial discriminators, J. Number Theory 59 (1996), 88-105.
- W. Sierpiński, *Elementary Theory of numbers*, Ed. by A. Schinzel, North-Holland (1988).
- Z.W. Sun, *On functions taking only prime values*, J. Number Theory 133 (2013), pp. 2794-2812.
- Z.W. Sun, *On primes in arithmetic progressions* (2013), available at arXiv:1304.5988v4.
- M.Zieve, *A note on the discriminator*, J. Number Theory 73 (1998), no. 1, 122-138.