On some cancellation algorithms

Maciej Zakarczemny

Politechnika Krakowska

21 listopada 2015

Zhi-Wei Sun w swojej pracy [5] zdefiniował liczbę
$b(n) := \min\{m \in \mathbb{N} : \ g(1), g(2), \ldots, g(n)$ są parami różne modulo $m\}$
gdzie $g : \mathbb{N} \to \mathbb{N}$ jest funkcją różnowartościową.

Browkin and Cao w [1] opisali następujący algorytm:

Dla $n \geqslant 2$ definiujemy zbiór

$$A_n := \{g(s) - g(r) : 1 \leqslant r < s \leqslant n;\ r, s \in \mathbb{N}\}$$

$$= \{g(k+l) - g(l) : k + l \leqslant n;\ k, l \in \mathbb{N}\}$$

oraz zbiór dzielników elementów A_n:

$$D_n := \{d \in \mathbb{N} : d|a \text{ dla pewnego } a \in A_n\}.$$

Następnie wykreślamy z $\mathbb{N}$ wszystkie elementy D_n.
Definiujemy $b(n)$ jako najmniejszą liczbę w zbiorze $\mathbb{N} \setminus D_n$, czyli najmniejszą niewykreśloną liczbę.

Ogólniej rozważmy dowolną funkcję $f : \mathbb{N}^m \to \mathbb{N}$, $m \geqslant 1$ i zbór

$$D_n = \{d \in \mathbb{N} : \ d | f(n_1, n_2, \ldots, n_m), \ n_1 + n_2 + \ldots + n_m \leqslant n\}.$$

Definiujemy znów $b(n)$ jako najmniejszą liczbę w zbiorze liczb niewykreślonych

$$D'(n) = \mathbb{N} \setminus D_n.$$

Naszym celem jest opisanie zbioru najmiejszych niewykreślonych liczb $\{b(n) : n \in \mathbb{N}\}$ dla szczególnych przypadków funkcji f.

Dla przykładu Browkin i Cao badali funkcję

$$f(k,l) = k^2 + l^2,\ (k,l) \in \mathbb{N}^2$$

i pokazali, że w tym przypadku zbiór $\{b(n) : n \geqslant 2\}$ jest równy $Q \setminus \{1\}$, gdzie Q jest podzbiorem liczb naturalnych, złożonym z liczb bezkwadratowych, które są iloczynami liczb pierwszych $\equiv\ 3 \pmod 4$.

$$Q = \{3, 7, 11, 19, 21, 23, 31, 33, 43, 47, 57, 59, 67, 69, 71, 77, 79, 83, \ldots\}.$$

Mówimy, że liczba naturalna jest bezkwadratowa jeśli nie jest podzielna przez żaden kwadrat liczby naturalnej większej od jeden.

Policzmy

Z definicji

$$D_n = \{d \in \mathbb{N} : \ d | k^2 + l^2, \ k + l \leqslant n, \ k, l \in \mathbb{N}\},$$

zatem

$\mathrm{D}_2 = \{1, 2\}$	b(2)=3,
$\mathrm{D}_3 = \{1, 2, 5\}$	b(3)=3,
$\mathrm{D}_4 = \{1, 2, 4, 5, 8, 10\}$	b(4)=3,
$\mathrm{D}_5 = \{1, 2, 4, 5, 8, 10, 13, 17\}$	b(5)=3,
$\mathrm{D}_6 = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 13, 17, 20, 26\}$	b(6)=7,
...	...

Twierdzenie 1

Niech $(r_s)_{s=1}^{\infty}$ to rosnący ciąg liczb bezkwadratowych.

Dla funkcji $f : \mathbb{N} \to \mathbb{N}$ zadanej wzorem $f(n) = n^k$, gdzie $k \geqslant 2$ jest liczbą naturalną, oznaczamy jak wyżej

$$D_n = \{d \in \mathbb{N} : \ d | r^k, \ r \leqslant n, \ r \in \mathbb{N}\}.$$

Niech $b(n)$ będzie najmniejszą liczbą w $D'(n) = \mathbb{N} \setminus D_n$.
Dla $s > 1$ mamy

$$b(n) = r_s \text{ dla } r_{s-1} \leqslant n < r_s.$$

Zatem $\{b(n) : n \in \mathbb{N}\}$ to jest zbiór wszystkich liczb bezkwadratowych z wyłączeniem 1.

Lemat 1

Dla $s > 1$ następująca nierówność zachodzi:

$$r_s \leqslant 2r_{s-1}.$$

Dowód twierdzenia 1

Dla danego $n \in \mathbb{N}$ bierzemy $s > 1$ takie, że $r_{s-1} \leqslant n < r_s$.
Trzeba pokazać, że r_s nie jest wykreślona,
ale każda liczba naturalna $h < r_s$ jest wykreślona.

Dowód twierdzenia 1

Aby pokazać, że r_s nie jest wykreślona, niech $r_s | b^k$ dla pewnego $b \in \mathbb{N}$.
Ponieważ r_s jest bezkwadratowa, zatem $r_s | b$.
Dlatego $b \geqslant r_s > n$ i r_s nie jest wykreślone.

Dowód twierdzenia 1

Teraz załóżmy, że $h < r_s$.
Niech u^2 to maksymalny kwadrat liczby naturalnej dzielący h.
Wtedy $\frac{h}{u^2}$ jest bezkwadratowa.
Zatem, możemy znaleźć $j \in \mathbb{N}$ takie, że

$$h = r_j u^2,\ 1 \leqslant j \leqslant s-1.$$

Biorąc $b = r_j u$ otrzymujemy $h | b^k$, ponieważ $k \geqslant 2$.
Rozważmy dwa przypadki. Jeśli $u = 1$ to $b = r_j \leqslant r_{s-1} \leqslant n$.
Jeśli $u \geqslant 2$ to $b = \frac{h}{u} \leqslant \frac{h}{2} < \frac{r_s}{2} \leqslant r_{s-1} \leqslant n$, z Lematu 1.
Zatem, w każdym przypadku h jest wykreślone i to było do pokazania.

Niech t to liczba bezkwadratowa. Definiujemy Q_t jako zbór liczb naturalnych w postaci ap^k, gdzie p to liczba pierwsza, która nie dzieli t; a jest liczbą bezkwadratową dzielącą t oraz k jest nieujemną liczbą całkowitą.
Niech $(q_s)_{s=1}^{\infty}$ to rosnący ciąg elementów Q_t.

Twierdzenie 2

Niech $f : \mathbb{N} \to \mathbb{N}$ będzie zadana wzorem $f(n) = n(n+t)$.
Dla $n \in \mathbb{N}$, gdzie $n \geqslant \max\{t^2 - t, 1\}$ definiujemy $s > 1$ takie, że

$$q_{s-1} \leqslant n + t \leqslant q_s - 1.$$

Wtedy

$$b(n) = q_s$$

oraz

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

Uwaga 1

Jeśli weźmiemy $t = 1$, czyli $f(n) = n(n+1)$ to

$$\{b(n) : n \in \mathbb{N}\} = \{p^k : p \text{ jest liczbą pierwszą, } k \geqslant 0\} \setminus \{1, 2\}.$$

Uwaga 2

Jeśli weźmiemy $t = 2$, czyli $f(n) = n(n+2)$ to

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

gdzie p to nieparzysta liczba pierwsza.

Oznaczmy, przez T zbiór liczb bezkwadratowych będących iloczynami liczb pierwszych, które nie są przystające do 1 modulo 6.
Niech $(t_s)_{s=1}^{\infty}$ to rosnący ciąg elementów T.
Przyjmujemy, że $t_1 = 1$, co odpowiada iloczynowi pustemu.
Zatem:

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

Twierdzenie 3

Niech $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ będzie zadana wzorem $f(k, l) = k^3 + l^3$. Wtedy

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

$$b(n) = t_s$$

gdzie $n \geqslant 4$ oraz s jest wybrane tak aby $t_{s-1} \leqslant n < t_s$.

Lemat 2

Dla naturalnego $s > 4$ mamy

$$t_s \leqslant \frac{151}{100} \cdot t_{s-1}.$$

Lemat 3

Dla $s > 0$ oraz $a, b \in \mathbb{N}$ jeśli $t_s|(a^3 + b^3)$ to $t_s|(a + b)$.

Kolejny typ algorytmu

Rozważmy dowolną funkcję $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ i zbiór

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

Wykreślmy z $\mathbb{N}$ wszystkie liczby $d \in \mathbb{N}$ takie, że d^2 jest dzielnikiem pewnej liczby w A_n i definiujemy $b(n)$ jako najmniejszą nie wykreśloną liczbą.

Oznaczmy, przez F zbiór wszystkich liczb naturalnych, które są iloczynami liczb pierwszych $\not\equiv 1 (mod\, 4)$.
Niech $(f_s)_{s=1}^{\infty}$ to rosnący ciąg wszystkich elementów F.
W szczególności $f_1 = 1$ co odpowiada iloczynowi pustemu. Zatem

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

Twierdzenie 4

Dla funkcji $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ zadanej wzorem $f(k, l) = k^2 + l^2$ oznaczmy

$$D_n = \{d \in \mathbb{N} : \exists_{k,l \in \mathbb{N}}\, k + l \leqslant n,\ d^2 | k^2 + l^2\}.$$

Niech $b(n)$ najmniejsza liczba w zbiorze $D'(n) = \mathbb{N} \setminus D_n$.
Wtedy $b(1) = 1$.
Ponadto jeśli $n \geqslant 2$ oraz $2f_{s-1} \leqslant n < 2f_s$ gdzie $s \geqslant 2$ to

$$b(n) = f_s.$$

Zatem, zbiór $\{b(n) : n \in \mathbb{N}\}$ jest równy F.

Przypuszczenie 1

Rozważmy funkcję $f : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ zadaną wzorem

$$f(k, l, m) = k^2 + l^2 + m^2,$$

oznaczmy

$$D_n = \{d \in \mathbb{N} : \exists_{k,l,m \in \mathbb{N}} \ k + l + m \leqslant n, \ d | k^2 + l^2 + m^2\}.$$

Niech $b(n)$ najmniejsza liczba w zbiorze $D'(n) = \mathbb{N} \setminus D_n$.
Wtedy $b(1) = b(2) = 1$, $b(3) = 2$
oraz dla naturalnego s mamy

- Jeśli $2 \cdot 2^s \leqslant \mathrm{n} < 3 \cdot 2^s$ to $b(n) = 4^s$,
- Jeśli $3 \cdot 2^s \leqslant n < 2 \cdot 2^{s+1}$ to $b(n) = 5 \cdot 4^{s-1}$.

Zatem możemy opisać zbiór

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

Przypuszczenie 2

Rozważmy funkcję $f : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ zadaną wzorem

$$f(k, l, m) = k^2 + l^2 + m^2,$$

oznaczmy

$$D_n = \{d \in \mathbb{N} : \exists_{k,l,m \in \mathbb{N}}\, k + l + m \leqslant n,\ d^2 | k^2 + l^2 + m^2\}.$$

Niech $b(n)$ zdefiniowana jak wyżej, wtedy $b(1) = 1$ oraz $n \geqslant 2$

$$b(n) = 2^{s-1}, \text{ jeśli } 3 \cdot 2^{s-2} \leqslant n < 3 \cdot 2^{s-1},$$

gdzie $s \geqslant 2$.
Zatem możemy opisać zbiór

$$\{b(n) : n \in \mathbb{N}\} = \{2^{s-1} :\ s \geqslant 1\}.$$

Bibliografia

1. J. Browkin, H-Q. Cao, *Modifications of the Eratosthenes sieve*, Colloq. Math. 135, (2014), pp. 127-138.
2. W. Sierpiński, *Elementary Theory of numbers*, Ed. by A. Schinzel, North-Holland (1988)
3. K. Molsen, *Zur Verallgemeinerung des Bertrandschen Postulates*, Deutsche Math. 6 (1941), 248-256
4. P. Moree, *Bertrand's postulate for primes in arithmetical progressions*, Comput. Math. Appl. 26 (1993), 35-43.
5. Z.W. Sun, *On functions taking only prime values*, J. Number Theory 133 (2013), pp. 2794-2812.
6. Z.W. Sun, *On primes in arithmetic progressions* (2013), available at arXiv:1304.5988v4.

Twierdzenie Gaussa

Każda liczba naturalna, która nie jest w postaci $4^l(8k+7)$, gdzie k, l to nieujemne liczby całkowite jest sumą kwadratów trzech liczb całkowitych.

Twierdzenie Hurwitza

Jedyne liczby naturalne n, dla których n^2 nie jest sumą kwadratów trzech liczb naturalnych to liczby $n = 2^h$ oraz $n = 5 \cdot 2^h$, gdzie $h = 0, 1, 2, \ldots$.

Twierdzenie Lagrange

Każda nie ujemna liczba całkowita jest reprzentowalna jako suma czterech kwadratów liczb całkowitych.