COLLOQUIUM MATHEMATICUM

VOL. 135 2014 NO. 1

MODIFICATIONS OF THE ERATOSTHENES SIEVE

BY

JERZY BROWKIN (Warszawa) and HUI-QIN CAO (Nanjing)

Abstract. We discuss some cancellation algorithms such that the first non-cancelled number is a prime number p or a number of some specific type. We investigate which numbers in the interval $(p, 2p)$ are non-cancelled.

1. Introduction. In the present paper we discuss some analogs of the Eratosthenes sieve, which give many prime numbers.

The well known sieve of Eratosthenes ([1]) gives all prime numbers less than a given integer. It can be stated in the following form:

THE ALGORITHM. For a fixed integer $n \geq 2$ cancel in the set $\{2, 3, 4, \ldots\}$ all multiples of 2, of $3, \ldots,$ and of n. In particular, the numbers $2, 3, \ldots, n$ are cancelled.

THEOREM 1. *After applying this algorithm:*

(i) *The least non-cancelled number is the least prime number p greater than n.*
(ii) *In the interval (p, p^2), where p is defined in* (i), *all prime numbers are non-cancelled and all composite ones are cancelled. The least non-cancelled composite number is p^2.*

Proof. (i) Let p be the least prime greater than n. Then every number t, $2 \leq t < p$, has a prime factor q less than p, so $q \leq n$, by the minimality of p. Consequently, t is cancelled.

On the other hand, p is not cancelled, since p does not have any factor in the interval $[2, n]$.

(ii) Let m be the least non-cancelled composite number. Then m has at least two prime factors, and each of them is $\geq p$. Consequently, $m \geq p^2$. Thus in (p, p^2) all composite numbers are cancelled.

Every prime number in this interval is non-cancelled, since it does not have a factor in $[2, n]$.

2010 *Mathematics Subject Classification*: Primary 11A41; Secondary 11N32, 11N36.
Key words and phrases: prime number algorithms.

([1]) Eratosthenes of Cyrene (c. 276 BC–c. 194 BC) became director of the great library in Alexandria.

DOI: 10.4064/cm135-1-10

Similarly, p^2 does not have any factor in this interval, so it is not cancelled. ∎

In the following we discuss other cancellation algorithms, which give numbers of some kind, in particular, prime numbers.

2. The first generalization. Let $g : \mathbb{N} \to \mathbb{N}$ be an injective mapping. Then for $n \in \mathbb{N}$ we define $b(n)$ as the least number in the set

$$B_n := \{m \in \mathbb{N} : g(1), \ldots, g(n) \text{ are distinct modulo } m\}.$$

This can be stated equivalently as the following cancellation algorithm. For $n \geq 2$ define the set

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

and the set of divisors of numbers in A_n:

$$D_n := \{d \in \mathbb{N} : d \,|\, a \text{ for some } a \in A_n\}.$$

Finally, let $D'_n := \mathbb{N} \setminus D_n$.

If we cancel in $\mathbb{N}$ all divisors of all numbers in A_n, i.e. all numbers in D_n, then D'_n will be the set of non-cancelled numbers.

LEMMA 2. *In the above notation we have $B_n = D'_n$ for $n \geq 2$.*

Proof. The following equivalences hold: $d \notin B_n$ if and only if $g(r) \equiv g(s) \pmod{d}$ for some r, s with $1 \leq r < s \leq n$, if and only if $d \,|\, g(s) - g(r)$ for some r, s as above. This divisibility holds if and only if $d \in D_n$. Consequently, $d \notin B_n$ if and only if $d \in D_n$. Hence $B_n = D'_n$. ∎

From Lemma 2 it follows that $b(n)$ is the least number in D'_n, so it is the least non-cancelled number.

3. The case of $g(n) = kn$ for some $k \in \mathbb{N}$. We apply the above algorithm to the linear function $g(n) = kn + l$, where $k \in \mathbb{N}$ and $l \in \mathbb{Z}$. From the definition of A_n it follows that we can assume that $l = 0$.

EXAMPLE 3. If $k = 1$, i.e. $g(n) = n$ for $n \in \mathbb{N}$, then for $n \geq 2$ we have

$$A_n = \{s - r : 1 \leq r < s \leq n\} = \{1, \ldots, n-1\}.$$

Then $D_n = A_n$, hence m is not cancelled iff $m \geq n$, so $b(n) = n$ for every $n \geq 2$.

The following theorem concerns the case $k \geq 2$.

THEOREM 4. *For a fixed $k \geq 2$ let $g(n) = kn$, where $n \in \mathbb{N}$. Assume that $n \geq k$. Then:*

(i) *All integers in the interval* $[1, n-1]$ *are cancelled.*
(ii) *The set of non-cancelled numbers in the interval* $[n, 2n)$ *equals*

$$S_n := \{t \in \mathbb{N} : n \le t < 2n,\ (t,k) = 1\}.$$

(iii) *The least non-cancelled number* $b(n)$ *is the least number in* S_n, *i.e. the least integer* $\ge n$ *which is relatively prime to* k.
(iv) $\{b(n) : n \in \mathbb{N},\ n \ge k\}$ *is the set of all integers* $\ge k$ *relatively prime to* k.

Proof. We cancel all divisors of all numbers $g(s)-g(r) = k(s-r)$, where $1 \le r < s \le n$, so all divisors of the form d_1d_2, where $d_1 \mid k$ and $d_2 \mid s-r$. Thus d_2 takes every value in $[1, n-1]$ and no others. Hence taking $d_1 = 1$ we get all integers in the interval $[1, n-1]$. This proves (i).

Observe that the set S_n is not empty, because from $k \le n$ it follows that the numbers $n, n+1, \ldots, n+k-1$ belong to $[n, 2n)$. They give all residues modulo k, in particular those relatively prime to k.

Assume that $t \in S_n$ is cancelled. Then $t = d_1d_2$, where d_1, d_2 are as above. From $(t,k) = 1$ and $d_1 \mid k$ it follows that $d_1 = 1$. Hence $t = d_2 \ge n$, which is impossible. Therefore no number in S_n is cancelled.

It remains to prove that all numbers $t \in [n, 2n)$ such that $d := (t,k) > 1$ are cancelled. We have $t = dt'$, where $d \mid k$ and $t' = t/d < 2n/d$. Since $d \ge 2$, we get $t' \le n-1$. Therefore t is cancelled. This proves (ii).

Now (iii) follows from (i), (ii) and the definition of $b(n)$, and (iv) follows from (iii). ■

4. The case of $g(n) = n^2$. Above we have discussed all linear polynomials; now we shall consider quadratic ones, starting with the simplest quadratic polynomial $g(n) = n^2$.

This case was investigated in [ABM], where parts (i) and (iii) of the theorem below are proved.

Let us recall that now for a given $n \ge 2$ we cancel all divisors of all numbers $g(s) - g(r) = s^2 - r^2$, where $1 \le r < s \le n$.

THEOREM 5.

(i) *For* $n > 2$, *all integers in the interval* $[1, 2n)$ *are cancelled.*
(ii) *For* $n \ge 2$ *all numbers in the set*

$$T_n := \{t \in \mathbb{N} : 2n \le t < 4n,\ t = p \text{ or } 2p,\ \text{where } p \text{ is a prime}\}$$

are non-cancelled. For $n \ge 15$ *all numbers in* $[2n, 4n] \setminus T_n$ *are cancelled.*
(iii) *For* $n > 4$ *the least non-cancelled number* $b(n)$ *is the least number in* T_n.

(iv) $b(2) = 2$, $b(4) = 9$, *and the set of other values of the function* $b(n)$ *equals*

$$\{b(n) : n \in \mathbb{N},\, n \neq 2, 4\} = \{2p : p \text{ is an odd prime}\} \\ \cup \{p : p = 2q + 1 \text{ is a prime and } q \text{ is composite}\}.$$

Thus $b(n)$ *is never equal to a Sophie Germain prime, i.e. to a prime* $p = 2q + 1$ *with* q *prime.*

Proof. For the proof of (i) and (iii) see [ABM]. The proof of (ii) goes along the same lines as the proof of Lemma 4 in [ABM]. We proceed as follows.

Let $n \geq 2$. Assume that a prime p belongs to T_n and is cancelled. Then $p \mid s^2 - r^2$ for some $1 \leq r < s \leq n$. Hence $p \mid s \pm r < 2s \leq 2n$. Thus $p < 2n$, which is impossible for $p \in T_n$.

Assume that $2p \in T_n$, where p is a prime, is cancelled. Then $2p \mid s^2 - r^2$ for some $1 \leq r < s \leq n$. It follows that s, r are of the same parity. Consequently, $n \geq 3$ and p is odd. Hence $2p \mid s \pm r < 2s \leq 2n$. This is impossible since $2p \in T_n$.

Thus we have proved that all numbers in T_n are non-cancelled. It remains to prove that for $n \geq 15$ all other numbers t in the interval $[2n, 4n)$ are cancelled.

For $n = 15, 16, 17$ this can be verified directly. We assume in the following that $n \geq 18$.

Since $t \notin T_n$, t is not equal to p or $2p$, where p is a prime. Therefore there are four possibilities for t, shown in Table 1 below. In each case we give r, s such that $1 \leq r < s \leq n$ and $t \mid s^2 - r^2$. This will prove that such a t is cancelled.

Table 1

No.	t	r	s	$s^2 - r^2$	Conditions
1.	a^2	a	$2a$	$3a^2$	
2.	$2a^2$	a	$3a$	$8a^2$	
3.	ab	$\frac{a-b}{2}$	$\frac{a+b}{2}$	ab	$2 \mid a - b$, $a > b > 1$
4.	$2ab$	$a - b$	$a + b$	$4ab$	ab odd, $a > b > 1$

From this table it is clear that in each case we have $1 \leq r < s$ and $t \mid s^2 - r^2$. It remains to prove that $s \leq n$ in each case. We proceed as follows.

By assumption, $2n \leq t < 4n$.

1. We have $s = 2a = 2\sqrt{t} < 2\sqrt{4n} \leq n$ for $n \geq 16$.
2. We have $s = 3a = 3\sqrt{t/2} < 3\sqrt{2n} \leq n$ for $n \geq 18$.

3. If a, b are odd, then $a > b \geq 3$. Hence

$$(a-3)(b-3) \geq 0, \quad \text{which gives} \quad ab+9 \geq 3(a+b).$$

Therefore

$$s = \frac{a+b}{2} \leq \frac{ab+9}{6} = \frac{t+9}{6} < \frac{4n+9}{6} < n$$

for $n \geq 5$.

If a, b are even, then $a > b \geq 2$. Hence

$$(a-2)(b-2) \geq 0, \quad \text{which gives} \quad ab+4 \geq 2(a+b).$$

Therefore

$$s = \frac{a+b}{2} \leq \frac{ab+4}{4} = \frac{t}{4} + 1 < n+1,$$

so $s \leq n$.

4. Since a, b are odd, we get, as above, $ab + 9 \geq 3(a + b)$. Hence

$$s = a + b \leq \frac{ab+9}{3} = \frac{t}{6} + 3 < \frac{4n}{6} + 3 \leq n$$

for $n \geq 9$.

Thus we have proved that $s \leq n$ for $n \geq 18$, which gives (ii).

(iv) From (iii) it follows that $b(n+1) \geq b(n)$ for $n \geq 15$. The same holds for $2 \leq n \leq 14$ (see [ABM]).

For a prime p, by the definition of T_n, it follows that the least number in T_p is $2p$. Then (iii) implies that $b(p) = 2p$ for every odd prime p, including $p = 3$, since $b(3) = 6$.

If $p = 2q + 1$ where q is composite, then the least number in T_q is $2q + 1 = p$.

If $p = 2q + 1$ where $q \geq 5$ is a prime, i.e. if p is a Sophie Germain prime, then $b(q) = 2q$ and $b(q + 1) \geq 2(q + 1) > p$. Since $b(n)$ is a non-decreasing function, it follows that $b(n) \neq p$ for every $n \geq 2$ and each Sophie Germain prime p. ∎

5. The case of $g(n) = 2n(n-1)$. For a fixed $n \geq 2$ we cancel all divisors of all numbers $g(s) - g(r) = 2(s - r)(s + r - 1)$, where $1 \leq r < s \leq n$. Equivalently, substituting $k = s - r$ and $m = r$ we get $g(s) - g(r) = 2k(k+2m-1) =: f(m, k)$. Thus we cancel all divisors of all numbers $f(m, k)$ where $k, m \in \mathbb{N}$, $k + m \leq n$.

This case was investigated by Zhi-Wei Sun, who proved the following

THEOREM 6 ([Sun1, Theorem 1.1(i)]). *For $n \geq 2$ the least non-cancelled number $b(n)$ is the least prime $p \geq 2n-1$. Therefore the set of numbers $b(n)$ is the set of all odd prime numbers.*

Theorem 7. *For $n \geq 9$ let p be the least prime $\geq 2n-1$.*

(i) *All prime numbers in the interval $[p, 2p)$ are non-cancelled.*
(ii) *All composite numbers in the interval $[p, 2p)$ are cancelled with at most one exception: If $2^{s-1} < n \leq 2^s$, then 2^{s+2} is not cancelled. $2^{s+2} \in (p, 2p)$ iff there is no prime in $[2n-1, 2^{s+1}-1]$; equivalently, iff $p > 2^{s+1}-1$.*

Proof. For $9 \leq n \leq 19$ the theorem can be verified directly. In what follows we assume that $n \geq 20$.

(i) If a prime $q \in (p, 2p)$ is cancelled, then $q \,|\, 2k(k+2m-1)$ for some $k, m \in \mathbb{N},\ k+m \leq n$.

If $q \,|\, k$, then $q \leq k < n < p$, contradicting $q \in (p, 2p)$.

If $q \,|\, k+2m-1$, then, from $k+2m-1 < 2(k+m)-1 \leq 2n-1 \leq p$, we get the same contradiction.

Therefore q is not cancelled, so (i) follows.

(ii) The proof will be divided in several steps.

Let $2^{s-1} < n \leq 2^s$. By Chebyshev's theorem we get $2^s < 2n-1 \leq p < 2(2n-1) < 4n \leq 2^{s+2}$. Thus $2p < 2^{s+3}$. It follows that if a power of 2 is in the interval $(p, 2p)$ then it must be 2^{s+1} or 2^{s+2}.

(1) We claim that 2^{s+1} is cancelled, and 2^{s+2} is not. Indeed, we have $f(2^{s-1}, 1) = 2(1 + 2^s - 1) = 2^{s+1}$ and $2^{s-1}+1 \leq n$, so 2^{s+1} is cancelled. If 2^{s+2} were cancelled, then $2^{s+2} \,|\, 2k(k+2m-1)$ for some $k, m \in \mathbb{N},\ k+m \leq n$.

If k is even, then $2^{s+1} \,|\, k < n \leq 2^s$, contradiction.

If k is odd, then $2^{s+1} \,|\, k+2m-1 < 2n-1 \leq 2^{s+1}-1$, contradiction.
Thus the claim is proved.

(2) Now we shall consider the exceptional case. It remains to investigate when $2^{s+2} < 2p$, or equivalently, when $2^{s+1}-1 < p$, because p is odd. Since p is the least prime $\geq 2n-1$, the inequality $2^{s+1}-1 < p$ holds iff there is no prime in the interval $[2n-1, 2^{s+1}-1]$.

This proves the exceptional case.

(3) It remains to prove that every composite number $t \in (p, 2p)$ which is not a power of 2, is cancelled. Therefore it is sufficient to prove that $t \,|\, f(m, k)$ for some $m, k \in \mathbb{N}$ such that $m+k \leq n$.

We shall use the following strong effective version of Chebyshev's theorem.

Lemma 8 ([Sun1, proof of Lemma 3.1]). *For $n \geq 2$ there is a prime number $p \in [2n-1, 2.4n]$.*

From this lemma it follows that the least prime $p \geq 2n-1$ satisfies $p \leq 2.4n$. Consequently, $t < 2p \leq 4.8n$. We shall use this inequality several times.

Since t is not a power of 2, it has an odd prime factor. Let q be the least odd prime factor of t. Then $t = qv$, where $v > 1$, since t is not a prime.

Case 1: $q \le 7$, that is, $q = 3, 5$ or 7.

1.1: v is even, $v = 2v_1$. We look for $m \in \mathbb{N}$ such that $t \mid f(m,q)$ and $m + q \le n$. We have $f(m,q) = 2q(q + 2m - 1) = 4q\bigl(m + \frac{q-1}{2}\bigr)$. There is $m \in [1, v_1]$ such that $m + \frac{q-1}{2} \equiv 0 \pmod{v_1}$. Then $t \mid f(m,q)$ and

$$m + q \le v_1 + q = \frac{t}{2q} + q \le \frac{4.8}{2q} n + q.$$

For $q = 3, 5, 7$ and $n \ge 15$ the last expression is $\le n$.

1.2: v is odd.

1.2.1: $v \le 2q - 1$. We have as before $f(m,q) = 4q\bigl(m + \frac{q-1}{2}\bigr)$. There is $m \in [1, v]$ such that $v \mid m + \frac{q-1}{2}$. Then $t = qv \mid f(m,q)$, and

$$m + q \le v + q \le 3q - 1 \le 20 \le n$$

for $q \le 7$ and $n \ge 20$.

1.2.2: $v > 2q - 1$. Now consider $f(m, 2q) = 4q(2q + 2m - 1)$. Take $m := \frac{v+1}{2} - q$. By assumption, $m \ge 1$, and $f(m, 2q) = 4qv = 4t$. Moreover,

$$m + 2q = \frac{v+1}{2} + q < \frac{t}{2q} + q + 1 \le \frac{2.4}{q} n + q + 1.$$

The last expression is $\le n$ for $q = 3, 5, 7$ and $n \ge 20$.

Case 2. $q \ge 11$.

2.1: $v = 2$ or 4. From $t = qv$ we get $q = t/v \le t/2 < p$, where p is the least prime $\ge 2n - 1$. Hence $q \le 2n - 3$. We have

$$f\left(\frac{q-1}{2}, 2\right) = 4(2 + (q-1) - 1) = 4q \equiv 0 \pmod{t}$$

and $\frac{q-1}{2} + 2 \le (n-2) + 2 = n$.

2.2: $v = 8$. As above we have $f(m,q) = 4q\bigl(m + \frac{q-1}{2}\bigr)$. We choose $m \in \{1, 2\}$ such that $m + \frac{q-1}{2} \equiv 0 \pmod 2$. Then $t = 8q \mid f(m,q)$ and

$$m + q \le 2 + \frac{t}{8} \le 2 + \frac{4.8}{8} n \le n \quad \text{for } n \ge 5.$$

2.3: $v \notin \{2, 4, 8\}$. Then $v \ge 11$, since v does not have an odd prime factor ≤ 7. We have $f(m,q) = 4q\bigl(m + \frac{q-1}{2}\bigr)$. Take $m \in [1, v]$ such that $m + \frac{q-1}{2} \equiv 0 \pmod{v}$. Then $t = qv \mid f(m,q)$ and

$$m + q \le v + q \le t\left(\frac{1}{q} + \frac{1}{v}\right) \le \frac{2}{11} t \le \frac{2}{11} \cdot 4.8n \le n \quad \text{for } n \ge 1. \ \blacksquare$$

6. The second generalization. Above we have considered functions $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by means of injective mappings $g : \mathbb{N} \to \mathbb{N}$ via $f(m,k) = g(m+k) - g(m)$ for $k, m \in \mathbb{N}$.

More generally, we can consider an arbitrary function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and use it in the same cancellation algorithm.

We give the details for the function

$$f(m,k) = m^2 + k^2. \tag{1}$$

It is easy to verify that it does not correspond to any injective mapping $g : \mathbb{N} \to \mathbb{N}$.

For a given $n \geq 2$, D_n is the set of all divisors of all numbers $f(m,k) = m^2 + k^2$, where $m, k \in \mathbb{N},\ m + k \leq n$. The numbers in D_n are cancelled, so the numbers in $D'_n = \mathbb{N} \setminus D_n$ remain non-cancelled.

Denote by Q the set of all squarefree positive integers which are products of prime numbers $\equiv 3 \pmod 4$. Let $(q_s)_{s=0}^{\infty}$ be the increasing sequence of all elements of Q. In particular, $q_0 = 1$, which corresponds to the empty product. Thus

$$Q = \{1, 3, 7, 11, 19, 21, 23, 31, 33, 43, 47, 57, 59, 67, 69, 71, 77, 79, 83, 103, \ldots\}.$$

The following lemma gives estimates on the growth rate of the sequence (q_s).

Lemma 9. *We have*

$$\frac{q_1}{q_0} = 3, \quad \frac{q_2}{q_1} = \frac{7}{3} = 2.33, \quad \frac{q_3}{q_2} = \frac{11}{7} = 1.57, \quad \frac{q_4}{q_3} = \frac{19}{11} = 1.72,$$

and

$$\frac{q_s}{q_{s-1}} < 1.5 \quad \text{for all } s \geq 5.$$

It follows that

$$q_s \leq 2q_{s-1} + 1 \quad \text{for } s \geq 1. \tag{2}$$

Proof. The sequence (r_n) of all prime numbers $\equiv 3 \pmod 4$ is a subsequence of (q_s), and $r_1 = q_1 = 3$. Therefore for every $s \geq 2$ there is $n \in \mathbb{N}$ such that

$$r_{n-1} < q_s \leq r_n.$$

Then $r_{n-1} \leq q_{s-1}$, since (r_n) is a subsequence of (q_s). Hence

$$1 < \frac{q_s}{q_{s-1}} \leq \frac{r_n}{r_{n-1}}. \tag{3}$$

It is known that $r_n < 2r_{n-1}$ for $n \geq 3$ and $r_n < 1.5\, r_{n-1}$ for $n > 118$ (see [Mol] and [Mor]). Then from (3) the lemma follows, after the direct verification of the claim for small values of s. ∎

Lemma 10. *If $q \in Q$ satisfies $q \mid a^2 + b^2$ for some $a, b \in \mathbb{N}$, then $a \equiv b \equiv 0 \pmod q$. Hence $a + b \geq 2q$.*

Proof. For $q = 1$ the lemma holds, since $a+b \geq 2$ for $a, b \in \mathbb{N}$. Let $q > 1$. Since -1 is not a quadratic residue modulo any prime $p \equiv 3 \pmod 4$, the divisibility $p \mid a^2 + b^2$ implies that $a \equiv b \equiv 0 \pmod p$. The lemma follows, since q is the product of distinct primes $\equiv 3 \pmod 4$. ∎

For $n \geq 2$ define $s \in \mathbb{N}$ by

$$2q_{s-1} \leq n \leq 2q_s - 1. \tag{4}$$

THEOREM 11. *Assuming the above notation we have:*

(i) *For $n \geq 2$ the least non-cancelled number $b(n)$ is q_s.*
(ii) *For $n \geq 3$ in the interval $I_s := (q_s, 2q_s)$ the numbers*

1) $q_j \in Q \cap I_s$,
2) $4q_j$, *where $q_j \in Q$ satisfies $4q_j > n$,*

are non-cancelled. All other numbers in this interval are cancelled.
(iii) *The set $\{b(n) : n \geq 2\}$ is equal to $Q \setminus \{1\}$.*

Proof. (i) We have to prove that q_s is non-cancelled, and every $t < q_s$ is cancelled.

Let $q_s \mid k^2 + m^2$ for some $k, m \in \mathbb{N}$. By Lemma 10 and (4), we have $k + m \geq 2q_s > n$. Therefore q_s is non-cancelled.

Let $t < q_s$. Then t satisfies one of the following conditions, where q_j is an element of Q:

(a) $t = q_j$, where $j \leq s - 1$,
(b) $t = a^2 q_j$, where $a \geq 2$,
(c) $t = (a^2 + b^2)q_j$, where $a, b \in \mathbb{N}$.

We shall prove that in each case t is cancelled.

(a) Put $k = m = q_j$. Then $t = q_j \mid k^2 + m^2 = 2q_j^2$, and $k + m = 2q_j \leq 2q_{s-1} \leq n$, by (4).

(b) Put $k = m = aq_j$. Then $t = a^2 q_j \mid k^2 + m^2 = 2a^2 q_j^2$, and $k + m = 2aq_j \leq a^2 q_j = t \leq q_s - 1 \leq 2q_{s-1} \leq n$, by (2) and (4).

(c) Put $k = aq_j$, $m = bq_j$. Then $t = (a^2 + b^2)q_j \mid k^2 + m^2 = (a^2 + b^2)q_j^2$, and $k+m = (a+b)q_j \leq (a^2+b^2)q_j = t \leq q_s - 1 \leq 2q_{s-1} \leq n$, by (2) and (4).

In each case we have proved that $k + m \leq n$, so t is cancelled.

(ii) We have the following possibilities for numbers t in the interval $(q_s, 2q_s)$, where q_j is an element of Q:

1) q_j,	4) $2q_j$,
2) $4q_j$,	5) $5q_j$,
3) $a^2 q_j$, $a \geq 3$,	6) $(a^2 + b^2)q_j$, $a, b \in \mathbb{N}$, $a^2 + b^2 > 5$.

We shall prove that the numbers q_j and $4q_j$, where $4q_j > n$, are not cancelled, and all other numbers in the interval $(q_s, 2q_s)$ are cancelled.

1) From the assumption we have $q_s < q_j < 2q_s$. If $q_j \mid k^2 + m^2$ for some $k, m \in \mathbb{N}$, then, by Lemma 10 and (4), $k + m \geq 2q_j > 2q_s > n$. Hence q_j is non-cancelled.

2) Assume that $4q_j \mid k^2 + m^2$ for some $k, m \in \mathbb{N}$. Let $4q_j > n$. Then k and m are even, and, by Lemma 10, $k \equiv m \equiv 0 \pmod{q_j}$. Hence $2q_j \mid k$, $2q_j \mid m$, which implies that $k + m \geq 4q_j > n$, by assumption. Consequently, $4q_j$ is not cancelled.

If $4q_j \leq n$, take $k = m = 2q_j$. Then $t = 4q_j \mid k^2 + m^2 = 4q_j^2$ and $k + m = 4q_j \leq n$, by assumption. Therefore the number $4q_j$ is cancelled.

3) Let $t = a^2 q_j$ belong to $(q_s, 2q_s)$, where $a \geq 3$. First we assume that $s \leq 4$. In $(q_1, 2q_1) = (3, 6)$ there is no number of the form $a^2 q_j$, since $a \geq 3$. The cases $s = 2, 3, 4$ are described in the table below.

Table 2

s	$(q_s, 2q_s)$	$t = a^2 q_j$	$k = m$	$n \geq 2q_{s-1}$
2	$(7, 14)$	$9 = 3^2 \cdot 1$	3	6
3	$(11, 22)$	$16 = 4^2 \cdot 1$	4	14
4	$(19, 38)$	$25 = 5^2 \cdot 1$	5	22
4	$(19, 38)$	$27 = 3^2 \cdot 3$	5	22
4	$(19, 38)$	$36 = 6^2 \cdot 1$	5	22

We see that in all cases $k + m = 2k \leq n$, so $t = a^2 q_j$ is cancelled.

Assume that $s \geq 5$. For $t = a^2 q_j$ take $k = m = aq_j$. Then $t = a^2 q_j \mid k^2 + m^2 = 2a^2 q_j^2$. From $a \geq 3$ it follows that $a \leq a^2/3$. Therefore

$$k + m = 2aq_j \leq \frac{2}{3} a^2 q_j = \frac{2}{3} t \leq \frac{4}{3} q_s \leq \frac{4}{3} \cdot \frac{3}{2} q_{s-1} = 2q_{s-1} \leq n,$$

by Lemma 9 and (4). Consequently, $t = a^2 q_j$ is cancelled.

4) Let $t = 2q_j$. From $q_s < t < 2q_s$ it follows that $q_j < q_s$, so $j \leq s - 1$. Taking $k = m = q_j$ we get $t = 2q_j \mid k^2 + m^2 = 2q_j^2$ and $k + m = 2q_j \leq 2q_{s-1} \leq n$, by (4). It follows that $t = 2q_j$ is cancelled.

5) Let $t = 5q_j$. First we assume that $s \leq 4$. There are the following cases:

Table 3

s	$(q_s, 2q_s)$	$t = 5q_j$	$k = q_j$	$m = 2q_j$	$n \geq 2q_{s-1}$
1	$(3, 6)$	$5 = 5 \cdot 1$	1	2	3
2	$(7, 14)$	$---$			
3	$(11, 22)$	$15 = 5 \cdot 3$	3	6	14
4	$(19, 38)$	$35 = 5 \cdot 7$	7	14	22

In the first line of the table we have $n \geq 3$, since in the theorem we have assumed that $n \geq 3$, so the case $n = 2$ is out of consideration.

In all cases in Table 3 we have $k + m \leq n$. Consequently, $t = 5q_j$ is cancelled.

Assume that $s \geq 5$. Take $k = q_j$ and $m = 2q_j$. Then $t = 5q_j \mid k^2 + m^2 = 5q_j^2$ and from $q_s < 5q_j < 2q_s$ we get

$$k + m = 3q_j < \frac{6}{5} q_s < \frac{6}{5} \cdot \frac{3}{2} q_{s-1} < 2q_{s-1} \leq n,$$

by Lemma 9 and (4). Consequently, $t = 5q_j$ is cancelled.

6) Let $t = (a^2 + b^2)q_j$, where $a, b \in \mathbb{N}$, $a^2 + b^2 > 5$. From the last inequality it follows easily that $a^2 + b^2 \geq 2(a + b)$.

Take $k = aq_j$ and $m = bq_j$. Then $t = (a^2 + b^2)q_j \mid k^2 + m^2 = (a^2 + b^2)q_j^2$, and

$$k + m = (a + b)q_j \leq \frac{1}{2}(a^2 + b^2)q_j = \frac{t}{2} < q_s \leq 2q_{s-1} + 1,$$

by (2). Consequently, $k + m \leq 2q_{s-1} \leq n$, by (4).

Therefore $t = (a^2 + b^2)q_j$ is cancelled.

(iii) The claim follows from (i). ∎

Remark. Zhi-Wei Sun (see [Sun1] and [Sun2]) has given many other cancellation algorithms such that the first non-cancelled number $b(n)$ is a prime (or conjecturally a prime). One may try to determine which numbers in the interval $(b(n), 2b(n))$ are non-cancelled by applying arguments similar to those in this paper. It turns out that for some of these algorithms also

Table 4

n	Non-cancelled numbers in $[q_s, 2q_s]$
2	3, **4**, 5, 6
3	3, **4**, 6
4—5	3, 6
7—11	7, 11, **12**, 14
12—13	7, 11, 14
14—21	11, 19, 21, 22
22—27	19, 21, 23, **28**, 31, 33, 38
28—37	19, 21, 23, 31, 33, 38
38—41	21, 23, 31, 33, 42
42—43	23, 31, 33, **44**, 46
44—45	23, 31, 33, 46
46—61	31, 33, 43, 47, 57, 59, 62
62—65	33, 43, 47, 57, 59, 66
66—75	43, 47, 57, 59, 67, 69, 71, **76**, 77, 79, 83, **84**, 86

some composite numbers in this interval are not cancelled. It would be interesting to describe them.

Table 4 illustrates Theorem 11. It lists the non-cancelled numbers in the interval $[q_s, 2q_s]$ corresponding to $n \in [2, 75]$ and the function $f(m,k) = m^2 + k^2$. The numbers of the form $4q_j$ are printed in bold. They satisfy $4q_j > n$ (see Theorem 11(ii) 2)).

Acknowledgements. The research of the second author has been supported by the National Natural Science Foundation (grant 11201233) of China.

REFERENCES

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

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

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

[Sun1] Z. W. Sun, *On functions taking only prime values*, J. Number Theory 133 (2013), 2794–2812.

[Sun2] Z. W. Sun, *On primes in arithmetic progressions*, arXiv:1304.5988v4.

Jerzy Browkin
Institute of Mathematics
Polish Academy of Sciences
Śniadeckich 8
00-656 Warszawa, Poland
E-mail: browkin@impan.pl

Hui-Qin Cao
Department of Applied Mathematics
Nanjing Audit University
211815, Nanjing, P.R. China
E-mail: caohq@nau.edu.cn

Received 20 February 2014 (6167)