Internat. J. Math. & Math. Sci.
VOL. 18 NO. 3 (1995) 539-544

ON THE K-th EXTENSION OF THE SIEVE OF ERATOSTHENES

ANTONIO R. QUESADA

Department of Mathematical Sciences,
The University of Akron, Akron, OH 44325-4002
R1quesa@VM1.cc.UAkron.edu

(Received November 19, 1993 and in revised form March 28, 1994)

ABSTRACT. The Sieve of Eratosthenes has been recently extended by excluding the multiples of 2, 3, and 5 from the initial set, and finding the additive rules that give the positions of the multiples of the remaining primes. We generalize these results. For a given k we let the initial set S_k consists of natural numbers relatively prime to the first k primes, and find the rules governing the positions of the multiples of the remaining elements.

KEY WORDS AND PHRASES. Prime numbers, sieve, tables of primes, algorithms.
1992 AMS SUBJECT CLASSIFICATION CODES. 11A41, 11-04, 11Y16.

1. INTRODUCTION.

One of several algorithms from the Greeks that, has survived the test of time, due to its simplicity and efficiency, is the Sieve of Eratosthenes. Given an initial set of positive integers $S = \{2, 3, 4, \cdots, N\}$, the prime numbers in S can be found iteratively by first crossing out all the multiples of 2 larger than 2 in S; then, in each subsequent step, the multiples of the smallest remaining number p not previously considered are crossed out. The process continues while $p^2 < N$. It should be noted that only prime numbers are used to sieve, and that the multiples of any number p are p units apart.

The advent of computers and the electronic transmission of information, with encrypting and testing techniques based on large primes, explains the enormous attention that the prime numbers have received during the last twenty-five years. The search for efficient algorithms to generate large tables of primes have produced impressive results such as Benelloum [1], Mairson [2], and Pritchard [3]. Several improvements have been made to the Sieve by reducing the size of the initial set and by avoiding some duplication in the removal process. In this paper, we will justify and generalize these simplifications of the Sieve, which may prove to be of particular interest in parallel processing.

The original algorithm can be readily improved, to what we will call the first extension, by first letting the initial set, denoted S_1, consist of only odd numbers, and then crossing out the multiples of p from p^2 on, starting with $p = 3$. We remark that, in this first extension, the multiples of any number p can still be found by counting, since their positions in S_1 are still p units apart. In the oldest reference to the Sieve commonly available in English, Nichomacus [4] states that Eratosthenes was aware of this idea of starting with only odd numbers, and made use of it. In general, no distinction is found in the literature between the original Sieve and the first extension (cf Knuth [5]).

In 1989, Xuedong Luo [6] obtained a second extension of the Sieve by also removing the multiples of three from the initial set, denoted S_2. Three years later, a third extension was found by Quesada [7] by further removing the multiples of five from the set S_3. In each extension, the reduction in size of the new initial set produces a change in the position of the remaining elements; thus, for example 29 changes from being the fourteenth element in S_1 to the ninth element of S_2, and the seventh in S_3. As a result, the positions of consecutive multiples of any given number p are no longer p units apart. Instead, they can be obtained by adding cyclically the elements of a predetermined finite set of differences, depending on p, whose size varies from one extension to another. For instance, the positions of the multiples of 7 can be obtained in S_2 by successively adding the elements of the set $\{9,5\}$, while in S_3 the corresponding set of differences between the remaining multiples of 7 is $\{12,7,4,7,4,7,12,3\}$.

2. NOTATION AND BASIC DEFINITIONS.

We now generalize this process for obtaining the prime numbers less than or equal to a given N. First we denote the initial set by S_k, that is, the set obtained from S by removing the multiples of the first k prime numbers. Then, for any p in S_k we determine the rules that govern the positions of the multiples of p in S_k.

Let $p_1, p_2, \cdots, p_n, \cdots$ denote the sequence of prime numbers, and let $\pi_k = \prod_{i=1}^{k} p_i$, $k \geq 1$. We denote by C_k the set of positive integers relatively prime and less than π_k, i.e., we let $C_k = \{c \in \mathbb{Z}^+ | \; c < \pi_k, \; (c,\pi_k) = 1\}$. The cardinality m_k of C_k is given by the Euler totient function, that is we let $m_k = |C_k| = \phi(\pi_k) = \prod_{i=1}^{k} (p_i - 1)$.

In order to obtain the k-th extension we choose the set of candidates S_k so that it contains just those positive integers less than or equal to N and relatively prime to π_k, thus we let $S_k = \{n \mid n = q\pi_k + c \leq N, \; q \in \mathbb{Z} - \mathbb{Z}^-, \; c \in C_k\}$. Moreover, we will consider both sets S_k and C_k to be ordered in ascending order. Notice that to simplify our notation we have included 1 in S_k and we place it in position 0. We remark that $\forall n \in S_k$ the multiples on n in S_k are obtained as ns_i, where $s_i \in S_k$.

EXAMPLE 1. Let's consider for instance the third extension. In this case $\pi_3 = 2 \cdot 3 \cdot 5 = 30$, $m_3 = \phi(30) = 8$, $C_3 = \{1, 7, 11, 13, 17, 19, 23, 29\}$ and $S_3 = \{1, 7, 11, \cdots, 29, 31, 37, \cdots, 59, \cdots, 30q + c_i, \cdots, N\}$. The multiples of any element of S_3, say 7, are $\{7, 49, 77, \cdots, 203, 217, \cdots\}$ whith corresponding ordinal positions $\{1, 13, 20, 24, 31, 35, 42, 54, 57, 69, \cdots\}$.

In any extension of the Sieve, we need to know for any given element $n \in S_k$ its position, the position of its square and of subsequent multiples of n in S_k.

We start by defining a function that maps each element of S_k to its ordinal position in S_k.

LEMMA 2. Let $C_k = \{c_i \mid c_0 < c_1 < c_2 < \cdots < c_{m_{k-1}}\}$. The position of any element of S_k is given by the injection Pos: $S_k \rightarrow \mathbb{Z}^+$ defined by

$$\mathrm{Pos}(n) = m_k q + i, \quad \text{for } n = q\pi_k + c_i. \qquad (2.1)$$

PROOF. If $n \in C_k$, then $n = c_i$ for some i, and Pos (n) = i. Otherwise, we can write Pos $(n) = \left\lfloor \frac{n}{\pi_k} \right\rfloor m_k + i$. Hence Pos is a well defined function.

To see that Pos is one-to-one, let $n_r = q_r\pi_k + c_r$ and $n_t = q_t\pi_k + c_t$. Assume that $\text{Pos}(n_r) = \text{Pos}(n_t)$. If $q_r < q_t$ then $m_kq_r+r = m_kq_t+t$ implies that $m_k < m_k(q_t - q_r) = r - t < m_k$ since $0 < r,t < m_k$. This contradiction shows that $q_r \geq q_t$. Symmetrically, $q_r > q_t$ yields a similar contradiction, hence $q_r = q_t$. It follows that $c_r = c_t$ and therefore $n_r = n_t$.

LEMMA 3. Let $n, t \in S_k$ where $n = q_n\pi_k+c_n$ and $t = q_t\pi_k+c_t$. Then

$$\text{Pos}(nt) = m_k(q_nt+c_nq_t)+\text{Pos}(c_nc_t) \tag{2.2}$$

PROOF.

$$\begin{aligned}\text{Pos}(nt) &= \text{Pos}((q_n\pi_k+c_n)t) = m_kq_nt+\text{Pos}(c_n(q_t\pi_k+c_t))\\ &= m_k(q_nt+c_nq_t)+\text{Pos}(c_nc_t).\end{aligned}$$

The congruence relation modulo π_k partitions S_k into m_k equivalent classes, where the elements of C_k are the canonical representatives, that is,

$$S_k = \bigcup_{c \in C_k} [c], \text{ where } [c] = \{x \in S_k \mid x \equiv c(\text{mod } \pi_k)\}.$$

We will see that for any $n \in [c]$ the positions of the multiples of n in S_k can be obtained by adding cyclically the elements of a predetermined finite set of differences, which in turn depend upon c. First, to determine the positions of the multiples of any element $c \in C_k$ in S_k, we need the following.

DEFINITION 4. Let c_i and c_{i+1} be consecutive elements of C_k. Then for each $n \in S_k$ we let

$$d_{n,i} = \begin{cases} \text{Pos}(nc_{i+1})-\text{Pos}(nc_i), & 1 \leq i < m_k \\ \text{Pos}(n(\pi_k+1))-\text{Pos}(nc_{m_k}), & i = m_k \end{cases}, \text{ and define } D_k^n = \{d_{n,i} \mid 1 \leq i \leq m_k\}.$$

That is, D_k^n is the set of differences of positions of the successive m_k+1 multiples of n in S_k .

3. MAIN RESULTS

LEMMA 5. Let $c \in C_k$. The set D_k^c contains all possible differences of positions between consecutive multiples of c in S_k, and repeats cyclically.

PROOF. Let n_i and n_j be consecutive elements of S_k such that $n_i = q_i\pi_k+c_i$ and $n_j = q_j\pi_k+c_j$. Then either (a) $q_i = q_j$ and $c_j = c_{i+1}$, or (b) $q_j = q_i+1$, $c_i = c_{m_k}$ and $c_j=1$.

In the first case, it follows from (2.1) that

$$\begin{aligned}\text{Pos}(cn_j)-\text{Pos}(cn_i) &= m_kc(q_j-q_j)+\text{Pos}(cc_j)-\text{Pos}(cc_i)\\ &= \text{Pos}(cc_j)-\text{Pos}(cc_i) = d_{c,i}.\end{aligned}$$

If (b) holds, then we can write $n_j = (q_i+1)\pi_k+1$. Hence,

$$\text{Pos}(cn_j)-\text{Pos}(cn_i) = [m_kcq_i + \text{Pos}(c(\pi_k+1))] - [m_kcq_i + \text{Pos}(cc_{m_k})] = d_{c,m_k}.$$

In either case $\mathrm{Pos}(cn_j)-\mathrm{Pos}(cn_i) \in D_k^c$.

Since, by construction, consecutive elements of S_k are congruent with consecutive elements of C_k modulo π_k, and we have seen that $\mathrm{Pos}(cn_j)-\mathrm{Pos}(cn_i) = d_{c,i}$, it follows that D_k^c contains all the differences of positions between successive multiples of c in S_k, and that they repeat cyclically.

Next we extend the previous result to any element n in S_k.

DEFINITION 6. Let

$$d_i = \begin{cases} c_{i+1}-c_i, & i < m_k \\ (\pi_k+1)-c_{m_k}, & i = m_k \end{cases} \quad \text{, and define } D_k = \{d_i \mid 1 \le i \le m_k\},$$

that is, D_k is the set of successive differences of the first m_k+1 elements of S_k.

THEOREM 7. Let $n= q\pi_k+c$ be an element of S_k. Then, the following statements hold.

(i) The set of differences of positions of consecutive multiples of n in S_k can be obtained as

$$D_k^n = D_k^c + m_kqD_k \tag{3.1}$$

where the sum is taken, as in the sum of m_k-tuples, over the i-th elements of the sets, $1 \le i \le m_k$.

(ii) The position of the first multiple of n to be sieved, i.e., n^2, is given by

$$\mathrm{Pos}(n^2) = m_kq(n+c)+\mathrm{Pos}(c^2). \tag{3.2}$$

(iii) The multiples of n that follow n^2 in S_k are obtained by cyclically adding the elements of D_k^n starting with $d_{n,r}$ for $c = c_r$.

PROOF. (i) Let $n_i = q_i\pi_k+c_i$ and $n_j = q_j\pi_k+c_j$ be consecutive elements of S_k. Then

$$\mathrm{Pos}(nn_j) - \mathrm{Pos}(nn_i) = q(n_j - n_i)m_k + \mathrm{Pos}(cn_j) - \mathrm{Pos}(cn_i). \tag{3.3}$$

From Lemma 5 we know that $\mathrm{Pos}(cn_j) - \mathrm{Pos}(cn_i) = d_{c,i}$, moreover, since $n_i \in [c_i]$ and $n_j \in [c_j]$ are consecutives, then it follows from Definition 6 that $n_j-n_i = d_i$, hence (3.3) yields

$$\mathrm{Pos}(nn_j)-\mathrm{Pos}(nn_i) = qd_im_k+d_{c,i}. \tag{3.4}$$

On the other hand,

$$d_{n,i}= \mathrm{Pos}(nc_j)-\mathrm{Pos}(nc_i) = q(c_j-c_i)m_k+\mathrm{Pos}(cc_j)-\mathrm{Pos}(cc_i) = qd_im_k+d_{c,i} \tag{3.5}$$

and the conclusion follows from (3.4) and (3.5).

(ii) This is a clear consequence of Lemma 2.

(iii) Let n_i and n_j be consecutive elements in S_k. Letting $n = n_i$ in (3.5), we can write

$$\mathrm{Pos}(n_in_j) - \mathrm{Pos}(n_in_i) = qd_im_k+d_{c_i,i} = d_{n_i,i}, \text{ thus } \mathrm{Pos}(n_in_j) = \mathrm{Pos}(n_i^2) + d_{n_i,i}.$$

We remark that this last theorem establishes that once the sets D_k and D_k^c are calculated, then for any $n \in [c]$ the set of diferences D_k^n and $\mathrm{Pos}(n^2)$ are readily known. Then, the multiples of n from n^2 on in S_k are found by cyclically adding the elements of D_k^n starting at $d_{n,j}$, for $c = c_j$. Is now clear, that sieving multiples of elements that belong to different equivalent classes are independent processes, and therefore the algorithm is particularly well suited for parallel processing.

COROLLARY 8. Let $t,n \in S_k$ be such that $t \equiv n \pmod{\pi_k}$. Then $D_k^t = D_k^n + m_k(q_t - q_n)D_k$, where the sum is taken over the i-th elements of the sets, $1 \leq i \leq m_k$.

PROOF. Since $t \equiv n \pmod{\pi_k}$, then $D_k^{c_t} = D_k^{c_n}$. Hence from the previous theorem, we obtain

$$D_k^t - D_k^n = (D_k^{c_t} + m_k q_t D_k) - (D_k^{c_n} + m_k q_n D_k) = m_k(q_t - q_n)D_k. \tag{3.6}$$

It is well known (see [5]) that the arithmetic complexity of the Sieve of Eratosthenes is O(n log n). Even though this remains unchanged in the k-th extension, the reduction in calculations is substantial, as the next Lemma shows.

LEMMA 9. The k-th extension of the Sieve of Eratosthenes produces a $\frac{100}{p_k}\%$ reduction on the size of S_{k-1}, and a $\frac{\pi_k - \phi(\pi_k)}{\pi_k}\%$ size reduction on S.

Proof. We know that $\phi(\pi_k) = (p_k - 1)\phi(\pi_{k-1})$. Moreover, in S_k each basic interval $[q\pi_k + 1, (q+1)\pi_k]$ contains $\phi(\pi_k)$ elements, while S_{k-1} has $p_k\phi(\pi_{k-1})$ elements in the same interval, hence

$$\frac{|S_{k-1}| - |S_k|}{|S_{k-1}|} = \frac{p_k\phi(\pi_{k-1}) - \phi(\pi_k)}{p_k\phi(\pi_{k-1})} = \frac{1}{p_k}. \tag{3.7}$$

That is, the reduction in size of S_k with respect to S_{k-1} is $\frac{100}{p_k}\%$.

From (3.6) we get $|S_k| = \frac{p_k - 1}{p_k}|S_{k-1}|$, from this we readily see that $|S_k| = \frac{\phi(\pi_k)}{\pi_k}|S|$ and the conclusion follows.

Table 1 below gives an idea of the size reduction of S_k with respect to S and S_{k-1} respectively. Notice that the reduction on the size of S_k is accompanied with an increase on the corresponding size of $\phi(\pi_k)$, and therefore on the number of the sets of differences as well as on the size of this sets. At the same time, once we pass the fourth extension, the reduction on the size of S_k seems to be rather small while $\phi(\pi_k)$ becomes too large. This suggests that even for relative large values of N, the third or the fourth extension may yield the faster results.

k	p_k	π	$\phi(\pi_k)$	$\frac{100}{p_k}\%$	$1 - \frac{\phi(\pi_k)}{\pi_k}\%$
1	2	2	1	50%	50%
2	3	6	2	33%	67%
3	5	30	8	20%	73%
4	7	210	48	14%	77%
5	11	2310	480	9%	79%
6	13	30030	5760	8%	81%

TABLE 1

REFERENCES

1. BENELLOUN, S.A., An incremental primal sieve, Acta Informatica 23, (1986), 119-125.

2. MAIRSON, H.G., Some new upper bounds on the generation of prime numbers, Commun. ACM 20, 9 (Sept. 1977), 664-669.

3. PRITCHARD, P., A sublinear additive sieve for finding prime numbers, Commun. ACM 24, 1 (Jan. 1981), 18-23.

4. D'OOGE, M. L. (translator), Nichomachus of Gerasa: Introduction to Arithmetic, Macmillan, New York, 1926.

5. KNUTH, D., The Art of Computer Programming, Vol. 2, 2nd ed., p. 394, Addison Wesley Publishing Company, Reading, Massachusetts, 1981.

6. XUEDONG LUO, A practical sieve algorithm for finding prime numbers, Commun. ACM 32, 3 (Mar. 1989), 344-346.

7. QUESADA A. R., Third Extension of Erathostenes' Sieve. Commun. ACM 35, 3 (Mar. 1992), pp. 11-13.