REVISTA MATEMÁTICA de la
Universidad Complutense de Madrid
Volumen 9, número 1: 1996
http://dx.doi.org/10.5209/rev_REMA.1996.v9.n1.17611

A Note on the Extensions of Eratosthenes' Sieve

A.R. QUESADA and B. VAN PELT

ABSTRACT. Given $k \in \mathbb{N}$, let S_k denote the set of natural numbers relatively prime to the first k primes. The k-extension of the Sieve of Eratosthenes, recently found, provides a set of rules that govern the positions in S_k of the multiples of the elements of S_k. In this paper we provide an alternative approach to the k-extension which yields an easier implementation in parallel processing. In addition it is shown that, with an appropriate layout of the set S_k, the rules governing the sieving process can be made similar to those in the original sieve.

Keywords and Phrases. Prime numbers, sieve, tables of primes, algorithms.

1. INTRODUCTION

The needs of modern cryptography, fueled by an increase in electronic transmission of information, and the need for computer-testing

1991 Mathematics Subject Classification: 11A41, 11-04, 11Y16

algorithms, explains in part the resurgence of activity in the area of primality that we have witnessed in the last twenty five years. The search for efficient algorithms to generate large tables of prime numbers has produced excellent new results from, among others, Mairson [3], Pritchard [4] and Bengelloun [1]. It has also produced noticeable improvements of traditional algorithms like Eratosthenes' Sieve.

The Sieve of Eratosthenes is probably the best known way to generate the table of all prime numbers less than a given natural number N. The reason for this is that, despite its simplicity, the Sieve is reasonably efficient. The primes on an initial set of candidates $S = \{2, 3, \ldots, N\}$ are 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 (larger than p) in S, not previously considered, are crossed out. Marking the multiples of p can be accomplished simply by counting, since they are located p units apart starting at p. This process, of "sieving" the composite numbers in S, continues until $p^2 > N$.

This classic algorithm, as described above, can be readly improved by first letting the initial set be the subset S_1 of all the odd numbers in S; in addition, we can mark the multiples of p, still p units apart in S_1, starting at p^2. We call this the first extension of the Sieve of Eratosthenes; and we remark that, quite often, the modern-day Sieve of Eratosthenes is identified with this first extension [2].

In 1988, X. Luo [7] achieved the second extension by sieving an initial set S_2, obtained from S, that was devoid of both the multiples of 2 and 3. In 1991, A. Quesada [5] obtained the third extension by further removing the multiples of 5 from the sieving set S. Finally, in 1993, Quesada [6] developed the generalized k-th extension where the initial set of candidates S_k is obtained from S by removing the multiples of the first k primes in S. In each subsequent extension, the reduction of the size of the new initial set produces a change in the position of the remaining elements in the set. As a result, the positions of consecutive multiples of any given number $p \in S_k$ are no longer p units apart. Instead, for each p in S_k a constant finite set of differences between consecutive multiples of p was found. Then the positions of the multiples of p in S_k were easily obtained by adding cyclically the elements of this finite set to the position of p. As the size of k increases, so does the size of this set of differences, making the calculations needed

for sieving the k-extension too cumbersome to be done by hand. In this paper we provide an alternative approach to the k-extension which yields an easier implementation in parallel processing. In addition it is shown that, with the proper layout of the sieving set, the rules governing the sieving process can be made almost as simple as those in the original sieve.

2. NOTATION AND BASIC DEFINITIONS

Let $p_1, p_2, \ldots p_i, \ldots$, denote the sequence of prime numbers, and let $\pi_k = \prod_{i=1}^{k} p_i$, $k \in \mathbb{N}$. The initial set is defined as $S_k = \{x \in \mathbb{N} : (x, \pi_k) = 1\}$. We denote by C_k the subset of elements of S_k less than π_k; that is, $C_k = \{c \in \mathbb{N}: c < \pi_k, (c, \pi_k) = 1\}$. We let m_k stand for the cardinality of C_k which can be easily obtained from the Euler totient function of π_k; i.e., $m_k = |C_k| = \phi(\pi_k) = \prod_{i=1}^{k} (p_i - 1)$.

Proposition 1. *Let $C_k = \{e_1, e_2, \ldots, e_{m_k}\}$, where $e_i < e_j$ for $i < j$. The following statements hold:*

a) $S_k = [e_1] \cup [e_2] \cup \ldots \cup [e_{m_k}]$, where $[e_i] = \{x \in S_k : x \equiv e_i (mod \pi_k)\}$ for $1 \leq i \leq m_k$, and $[e_i] \cap [e_j] = \phi$ for $i \neq j$.

b) For $1 \leq i \leq m_k$, $[e_i] = \{e_i, e_i + \pi_k, \ldots, e_i + (n-1)\pi_k, \ldots\}$

c) $S_k = \{q\pi_k + e_i : e_i \in C_k, q \in \mathbb{N} \cup \{0\}\}$, and is closed under multiplication.

Proof. Part a) simply states that, by the Partition Theorem, the equivalence relation of "congruence mod π_k" partitions the initial set S_k into equivalence classes which have the elements of C_k as canonical representatives. Part b) follows from the definition of congruence mod π_k in S_k. Finally, from a) and b), we see that S_k can be obtained by adding successive multiples of π_k to the elements of C_k. Furthermore, $(x, \pi_k) = 1$ and $(y, \pi_k) = 1$ iff $(xy, \pi_k) = 1$ yields the closure of S_k under multiplication.

Definition 2. *If $x \in S_k$ and $t \in \mathbb{N}$, then the t-th multiple of x in S_k will be denoted by $\overset{(t)}{x}$. That is, $\overset{(t)}{x} = xs_t$, where s_t is the t-th element of S_k.*

From now on we will refer to a multiple of an element x in S_k, or to the t-th multiple of x in S_k by a simply saying a multiple of x or the t-th multiple of x.

MAIN RESULTS

Proposition 3. *Let $x \in S_k$. Any m_k consecutive multiples of x fall into different equivalent classes.*

Proof. Let $xs_i, xs_{i+1}, \ldots, xs_{i+m_k-1}$ be a set of m_k consecutive multiples of x. Proceeding by way of contradiction, suppose that xs_u, $xs_v \in [e_t]$ for some $e_t \in C_k$, and $u \neq v$, where $i \leq u, v \leq i + m_k - 1$. Thus we have that $xs_u = q_1\pi_k + e_t$ and $xs_v = q_2\pi_k + e_t$, for some $q_1, q_2 \in \mathbb{N} \cup \{0\}$. Without loss of generality, assume that $s_u > s_v$. Therefore,

$$x(s_u - s_v) = (q_1 - q_2)\pi_k.$$

Since x and π_k have no common factors, this implies that $\pi_k|(s_u - s_v)$, which is a contradiction since by construction $\pi_k > s_u - s_v > 0$.

Next we show that the multiples of any element $x \in S_k$ that appear within a given equivalence class can be found, like in the original Sieve, by counting every x positions starting from the first multiple of x in the class.

Theorem 4. *The difference between the positions of two consecutive multiples of any element $x \in S_k$ within a given equivalence class is x.*

Proof. If $x = 1$, then we are done. So let $x \in S_k$, $x > 1$, such that $\overset{(t)}{x} \in [e_j]$, for some $e_j \in C_k$ and $t \in \mathbb{N}$. We want to show that the next multiple of x in S_k that falls into the equivalence class $[e_j]$ is $\overset{(t)}{x} + x\pi_k$.

Let $\overset{(t)}{x} = q\pi_k + e_j$ for some $q \in \mathbb{N} \cup \{0\}$. Then,

$$\overset{(t)}{x} + x\pi_k = (q\pi_k + e_j) + x\pi_k = (q + x)\pi_k + e_j \in [e_j].$$

Thus $\overset{(t)}{x} + x\pi_k$ is a multiple of x in $[e_j]$. All that remains to be shown is that there does not exist a multiple of x, say $\overset{(m)}{x}$, such that $\overset{(m)}{x} \in [e_j]$

and $\overset{(t)}{x} < \overset{(m)}{x} < \overset{(t)}{x} + x\pi_k$. By way of contradiction, suppose that such an $\overset{(m)}{x}$ does exist in $[e_j]$. Thus, $\overset{(m)}{x} = u\pi_k + e_j$, for some $u \in \mathbb{N} \cup \{0\}$. Then from $\overset{(t)}{x} < \overset{(m)}{x} < \overset{(t)}{x} + x\pi_k$ it follows that

$$q\pi_k + e_j < u\pi_k + e_j < (q + x)\pi_k + e_j, \text{ and so } q < u < q + x.$$

Now, $u = q + r$ for some $r \in \mathbb{N}$, where $1 \leq r < x$. Hence,

$$\overset{(m)}{x} = (q + r)\pi_k + e_j = (q\pi_k + e_j) + r\pi_k = \overset{(t)}{x} + r\pi_k.$$

Thus, $\overset{(m)}{x} - \overset{(t)}{x} = r\pi_k$ with $1 \leq r < x$. But $(x, \pi_k) = 1$ and $x | (\overset{(m)}{x} - \overset{(t)}{x})$. This implies that $x|r$, which is a contradiction.

We have seen in theorem 4 that for any element $x \in S_k$, once we find its first multiple in an equivalence class, the remaining multiples are found by constant addition. By proposition 3, the first m_k multiples of x fall each into a different equivalence class. Hence, we have reduced to m_k the number of products needed to determine all of the multiples of x. Our next result shows that the position within an equivalence class of any multiple of x is totally dependent on the canonical representative of the equivalence class containing x. More precisely, once we have found the first multiple of $e_j \in C_k$ in some equivalence class $[e_t]$, then we can find all the multiples of $x \in [e_j]$ that fall in $[e_t]$ by adding some constant to the first multiple of e_j in $[e_t]$.

Proposition 5. *Let $x \in S_k$ be the $(q + 1)$-th element in the equivalence class $[e_i]$, for some $e_i \in C_k$. If $\overset{(t)}{e_i}$ is the v-th element of some equivalence class $[e_j]$, then $\overset{(t)}{x}$ is the $(v + qs_t)$-th element of $[e_j]$, where s_t is the t-th element of S_k.*

Proof. Since x is the $(q + 1)$-th element in the equivalence class $[e_i]$, from Proposition 1 b), we can write $x = q\pi_k + e_i$. Hence,

$$\overset{(t)}{x} = (e_i + q\pi_k)s_t = e_i s_t + qs_t\pi_k = \overset{(t)}{e_i} + qs_t\pi_k = [(v - 1)\pi_k + e_j] + qs_t\pi_k.$$

But this says that $\overset{(t)}{x} = (v + qs_t - 1)\pi_k + e_j$, and this is precisely what we want.

Corollary 6. *If $x = (q+1)\pi_k + e_i$ and $e_ie_t \in [e_j]$ then xe_t, the first multiple of x in $[e_j]$, is the (qe_t)-th element from e_ie_t in $[e_j]$.*

Proof. This is just a restatement of the former proposition in the particular case when $s_t = e_t$.

We have seen that the first m_k multiples of the canonical representative of an equivalence class determines the positions of the first m_k multiples of any element in the class. This suggests that, before initiating the sieving process on S_k, we should have available a table containing the products e_ie_j for $i, j \in \{1, 2, \ldots, m_k\}$.

Definition 7. *We denote by A the $m_k \times m_k$ array containing the products e_ie_j for $1 \leq i, j \leq m_k$.*

Notice that A is symmetric, since both the i-th row and the i-th column of A consist of the first m_k multiples of e_i and that the first row (column) consists of the elements of C_k. Hence, we only need to calculate the elements a_{ij} for $2 \leq i \leq j \leq m_k$ of A. However, the number of calculations $m_k(m_k - 1)/2$ is still considerably large even for small values of k. Our next result shows that the number of calculations needed to obtain A can be further reduced.

Theorem 8. *Let $C_k = \{e_1, e_2, \ldots, e_{m_k}\}$ where $e_i < e_j$ for $i < j$. The following hold:*

a) $\pi_k - e_i \in C_k$, for each $e_i \in C_k$,

b) $e_i + e_j = \pi_k$ iff $i + j = m_k + 1$, and

c) $e_je_{m_k+1-t} = \pi_ke_j - e_je_t$ for $1 \leq j, t \leq m_k$.

Proof. a) We need to show that $\pi_k - e_i$ and π_k are relatively prime. But if $p|(\pi_k - e_i)$ and $p|\pi_k$ for some prime p, then $p|[\pi_k - (\pi_k - e_i)] = e_i$, which is a contradiction to $e_i \in S_k$.

b) By hypothesis $e_i < e_j$ for $i < j$, thus it follows from a) that

$$\pi_k - e_{m_k} < \pi_k - e_{m_k-1} < \ldots < \pi_k - e_2 < \pi_k - e_1,$$

but this says that $e_i = \pi_k - e_{m_k - i}$ for $1 \leq i \leq m_k$, since $\pi_k - e_i \in C_k$.

c) Since $t + (m_k + 1 - t) = m_k + 1$, it follows from b) that $e_t + e_{m_k+1-t} = \pi_k$.

Corollary 9. *A is completely determined by the set*

$$T = \{e_i e_j : \ 2 \leq i \leq j \leq m_k/2\}.$$

Proof. Consider the four $\left(\frac{m_k}{2} \times \frac{m_k}{2}\right)$ submatrices B, C, D and E of the matrix A as depicted below. Clearly the first row of A consists of the elements of C_k, since $e_1 = 1$.

Once the set T is calculated, B is completely known by symmetry. Using Theorem 8 c) the submatrix C is immediately obtained from B. Moreover, the submatrix D is then the reflection of C upon the main diagonal of A. Finally, E is obtained from D by applying Theorem 8 c) again.

We remark that corollary 8 establishes that A is completely determined by less than $\frac{1}{8}$ of its elements.

$$\left[\begin{array}{cccc|ccc}
e_1e_1 & e_1e_2 & \cdots & e_1e_{\frac{m_k}{2}} & e_1e_{\frac{m_k}{2}+1} & \cdots & e_1e_{m_k} \\
e_2e_1 & e_2e_2 & \cdots & e_2e_{\frac{m_k}{2}} & e_2e_{\frac{m_k}{2}+1} & \cdots & e_2e_{m_k} \\
\vdots & \vdots & B & \vdots & \vdots & C & \vdots \\
e_{\frac{m_k}{2}}e_1 & e_{\frac{m_k}{2}}e_2 & \cdots & e_{\frac{m_k}{2}}e_{\frac{m_k}{2}} & e_{\frac{m_k}{2}}e_{\frac{m_k}{2}+1} & \cdots & e_{\frac{m_k}{2}}e_{m_k} \\
-- & -- & -- & -- & -- & -- & -- \\
e_{\frac{m_k}{2}+1}e_1 & e_{\frac{m_k}{2}+1}e_2 & \cdots & e_{\frac{m_k}{2}+1}e_{\frac{m_k}{2}} & e_{\frac{m_k}{2}+1}e_{\frac{m_k}{2}+1} & \cdots & e_{\frac{m_k}{2}+1}e_{m_k} \\
\vdots & \vdots & D & \vdots & \vdots & E & \vdots \\
\vdots & \vdots & & \vdots & \vdots & & \vdots \\
e_{m_k}e_1 & e_{m_k}e_2 & \cdots & e_{m_k}e_{\frac{m_k}{2}} & e_{m_k}e_{\frac{m_k}{2}+1} & \cdots & e_{m_k}e_{m_k}
\end{array}\right]$$

The following example illustrates our main results.

Example 10. Let $k = 3$. Then $\pi_3 = 2 \cdot 3 \cdot 5 = 30$, $C_3 = \{1, 7, 11, 13, 17, 19, 23, 29\}$, and $m_3 = \phi(30) = (2-1)(3-1)(5-1) = 8$.

The set $T = \{7^2, 7 \cdot 11, 7 \cdot 13, 11^2, 11 \cdot 13, 13^2\}$ contains the elements b_{ij}, where $1 < i \leq j \leq 4$, of the submatrix B. The remaining elements of B are found by symmetry. Theorem 8 c) yields C, since $c_{ij} = 30b_{i1} - b_{i(5-j)}$, $1 \leq i, j \leq 4$.

$$B = \begin{bmatrix} 1 & 7 & 11 & 13 \\ 7 & 49 & 77 & 91 \\ 11 & 77 & 121 & 143 \\ 13 & 91 & 143 & 169 \end{bmatrix}, \quad C = \begin{bmatrix} 17 & 19 & 23 & 29 \\ 119 & 133 & 161 & 203 \\ 187 & 209 & 253 & 319 \\ 221 & 247 & 299 & 377 \end{bmatrix}$$

By symmetry on A we obtain D, i.e., $d_{ij} = c_{ji}$, $1 \leq i, j \leq 4$. Finally, E is obtained from D by applying Theorem 8 c) again.

$$A = \left[\begin{array}{cccc|cccc} 1 & 7 & 11 & 13 & 17 & 19 & 23 & 29 \\ 7 & 49 & 77 & 91 & 119 & 133 & 161 & 203 \\ 11 & 77 & 121 & 143 & 187 & 209 & 253 & 319 \\ 13 & 91 & 143 & 169 & 221 & 247 & 299 & 377 \\ \hline 17 & 119 & 187 & 221 & 289 & 323 & 391 & 493 \\ 19 & 133 & 209 & 247 & 323 & 361 & 437 & 551 \\ 23 & 161 & 253 & 299 & 391 & 437 & 529 & 667 \\ 29 & 203 & 319 & 377 & 493 & 551 & 667 & 841 \end{array}\right]$$

Using the characterization of Proposition 1 c) we obtain S_3 by adding multiples of 30 to C_3. Thus, as depicted in Table 1, we may express S_3 as an infinite array where each column is an equivalence class whose canonical representative is the corresponding element of C_3 in the first row.

The second row of A contains the first eight multiples of 7 in S_3, each in a different column, which we have parenthesized in the table. To delete the remaining multiples of 7 in an equivalence class, say those in [13], we locate the first multiple of 7 in [13] which is 133. Then we cancel every 7-th element after 133 in that column. The first eight multiples of

a prime number in the i-th row of table 1 and in the equivalence class [7], can be easily obtained by adding $30(i-1)e_{1j}$ to a_{2j}, $1 \leq j \leq 8$. Thus, the first eight multiples of 67 are $60+7, 420+49, \ldots, 1740+203$. We have also underlined the multiples of 11 in the table.

We remark that after A is obtained, the sieving of S_k becomes an additive process. Moreover, the deletion of the multiples of any prime in different columns can be done independently. Because of these two reasons, this is a fast algorithm particularly suited for parallel implementation.

[1]	[(7)]	[11]	[13]	[17]	[19]	[23]	[29]
31	37	41	43	47	(49)	53	59
61	67	71	73	(77)	79	83	89
(91)	97	101	103	107	109	113	(119)
121	127	131	(133)	137	139	143	149
151	157	(161)	163	167	169	173	179
181	187	191	193	197	199	(203)	209
211	(217)	221	223	227	229	233	239
241	247	251	253	257	(259)	263	269
271	277	281	283	(287)	289	293	299
(301)	307	311	313	317	319	323	(329)
331	337	341	(469)	347	349	353	359
361	367	(371)	373	377	379	383	389
391	397	401	403	407	409	(413)	419
421	(427)	431	433	437	439	443	449
451	457	461	463	467	(469)	473	479
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.

Table 1

References

[1] Bengelloun, 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] Knuth, D., *The Art of Computer Programming*, Vol. 2, 2nd ed., p. 394, Addison Wesley. Publishing Company, Reading, Massachusetts, 1981.

[4] Pritchard, P., A sublinear additive sieve for finding prime numbers, *Commun. ACM* **24, 1** (Jan. 1981), 18-23.

[5] Quesada, A.R., Third Extension of Erathostenes' Sieve. *Commun. ACM* **35, 3** (Mar. 1992), pp. 11-13.

[6] Quesada, A.R., On the k-th extension of the sieve of Eratosthenes. Int. J. of Math. and Math. Sci., Vol. 18, No. 3, pp. 539-544, 1995.

[7] Xuedong Luo, A practical sieve algorithm for finding prime numbers, *Commun. ACM* **32, 3** (Mar. 1989), 344-346.

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

Recibido: 30 de Septiembre, 1994