International Journal of Mathematical Archive-7(9), 2016, 132-134
IJMA Available online through www.ijma.info ISSN 2229 – 5046

# GENERATING SEQUENCE OF RELATIVELY PRIMES USING SIEVE TECHNIQUE

B. N. PRASAD RAO[1]*, Dr. M. RANGAMMA[1]

[1]Department of Mathematics, Osmania University, Hyderabad, Telangana, India.

*(Received On: 14-09-16; Revised & Accepted On: 30-09-16)*

*ABSTRACT*

*Sieve of Eratosthenes is a technique used to find sequence of primes below a given integer $n$. This technique is adaptable to digital computers on slight modification. The modification essentially involves a sieve process. In this paper we have generated the sequence of relatively prime numbers to an integer $N \neq p, 2^k$ where $k \in \mathbb{N}$ and $p$ is a prime number.*

***Keywords:*** *Algorithm for Generating Sequence of Relatively Primes using Sieve Technique.*

***AMS Subject Classification:*** *10A.*

## INTRODUCTION

Sieve technique is modified to generate sequence of prime numbers less than a given positive integer $n$ and some Number Theoretic Functions (see [2]). We have generated sequence of relatively prime numbers to a given integer $N \neq p, 2^k$ where $k \in \mathbb{N}$ and $p$ is a prime number. We have used some criterions under which a prime below a given integer becomes relatively prime (see [1]). These criterions have been mentioned in preliminaries section. We have used these criterions to stop the iteration process in generating sequence of relatively primes.

## PRELIMINARIES

**Theorem 1:** Let $N \neq 2q, 3q$ where $q$ is a prime number, be a composite integer. The prime numbers greater than $\frac{N}{4}$ are relatively prime to $N$.

**Theorem 2:** Let $N = 3q$ where $q$ is an odd prime number, be a composite integer. The prime numbers greater than $\frac{N}{3}$ are relatively prime to $N$.

**3. Definition:** The characteristic function on the set of positive integers less than $N$ and relatively prime to $N$, denoted by $\chi^N{}_{rp}$ is defined as

$$\chi^N{}_{rp}(n) = \begin{cases} 1 \; if \; n < N, \gcd(n, N) = 1 \\ 0 \; otherwise \end{cases}$$

**Modification 1:** The modification to sieve process in generating the sequence of relatively primes to a given integer $N \neq 2^k, p$ where $k \in \mathbb{N}, p$ a prime number is illustrated for the case $N = 28$. Table 1 shows the construction of sequence of relatively prime numbers below $N$. This table is headed by the sequence of natural numbers in natural order, which will thus indicate the position numbers for the elements of the sequences. The entries in table 1 are prepared as follows. For the sequence $A^{(0)}$, we enter 1 in the first row for $n \leq N$. In order to begin the process of sieving, we locate 1 appearing at 2$^{nd}$ position of the first row and denote this position by $a_1$ (from table 1, $a_1$ has value 2) and then convert the entries in position $ma_1$, $m = 1,2,...$(every 2$^{nd}$ entry starting from 2) from 1 to 0. If the process of conversion results 0 at the $N^{th}$ position then it indicates that $a_1$ is not relatively prime to $N$. We sieve out $a_1$and its multiples. The resulting sequence is denoted by sequence $A^{(1)}$. If the process of conversion does not results 0 at the $N^{th}$ position then it indicates that $a_1$ is relatively prime to $N$. In this case, we take the new sequence $A^{(1)}$ to be same as the preceding sequence $A^{(0)}$. In Table 1, the entry 1 at position $N = 28$ is converted to 0 and hence, the new sequence $A^{(1)}$ is the sequence with the converted entries.

***Corresponding Author: B. N. Prasad Rao[1]****

The position number of the first non-zero entry beyond position $a_1$ in sequence $A^{(1)}$ is denoted by $a_2$ (from table 1, $a_2$ has value 3). Every entry in position $ma_2$, for $ma_2 \leq N$ where $m = 1,2, ...$ (i,e. every 3rd entry starting from 3) is converted from 1 to 0, if the entry is not already 0. The conversion process leading to an entry 0 at the $N^{th}$ position is checked. In this case the resulting sequence is denoted by $A^{(2)}$ which is a sequence taken to be same as the sequence $A^{(1)}$.

In general, in the sequence $A^{(k-1)}$ we locate the position of the first non-zero entry beyond position $a_{k-1}$ and denote this position by $a_k$. we now convert the entries in position $ma_k, m = 1,2, ...$(every $a_k$-th entry starting from $a_k$) from 1 to 0, if they are not already 0. If the conversion process leads to an entry 0 at $N^{th}$ position then the new sequence $A^{(k)}$ is the sequence with subtracted entries. Otherwise the sequence $A^{(k)}$ is taken to be same as sequence $A^{(k-1)}$.

The process of termination depends on $N$. The process is terminated at the sequence $A^{(k-1)}$ if $a_k > \frac{N}{4}$ where $N \neq 2q, 3q$ and $q$ is a prime [since by Theorem 1 the primes greater than $\frac{N}{4}$ are relatively prime to $N$]. The process is terminated at the sequence $A^{(k-1)}$ if $a_k > \frac{N}{2}$ where $N = 2q$ and $q$ is a prime. [Since all primes greater than $\frac{N}{2}$ are relatively prime to $N$]. The process is terminated at the sequence $A^{(k-1)}$ if $a_k > \frac{N}{3}$ where $N = 3q$ and $q$ is an odd prime [since by Theorem 2 the primes greater than $\frac{N}{3}$ are relatively prime to $N$].

The sequence $A^{(k-1)}$ coincides with the function $\chi^N{}_{rp}$. In this construction the actual sieving out of the number $n \leq N$ is indicated by the conversion of an entry 1 to an entry 0 in position $n$ of the sequence. If a 0 has already appeared, this indicates that the number has been sieved out at a previous step.

**Verification:** The last sequence $A^{(4)}$ coincides with the characteristic function $\chi^N{}_{rp}$ for $N = 28$.

**Table-1**

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $A^{(0)}$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 |
| $A^{(1)}$ | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| | | | 0 | | | 0 | | | 0 | | | 0 | | | 0 | | | 0 | | | 0 | | | 0 | | | 0 | |
| $A^{(2)}$ | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| | | | | | 0 | | | | | 0 | | | | | 0 | | | | | 0 | | | | | 0 | | | |
| $A^{(3)}$ | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| | | | | | | | 0 | | | | | | | 0 | | | | | | | 0 | | | | | | | 0 |
| $A^{(4)}$ | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |

**Modification 2:** The above method has the disadvantage in that multiple sieving out of elements occur when ever the position number is composite. The following modification will eliminate this disadvantage.

The entries in Table 2 are prepared as follows. The initial sequence $A^{(0)}$, is the sequence with 1 for all $n \leq N$. In order to begin the process of sieving, we locate 1 appearing at 2nd position of the first row and denote this position by $a_1$ (from table 2, $a_1$ has value 2). We sieve out each second element by subtracting the entry at $m = 1,2, ...$ from the entry in position $ma_1$. If this process, upon subtraction leads to an entry 0 at the $N^{th}$ position then it indicates that $a_1$ is not relatively prime to $N$ and the new sequence $A^{(1)}$ is the sequence with subtracted entries. Otherwise, it indicates that $a_1$ is relatively prime to $N$. In this case, the new sequence $A^{(1)}$ is the same as the preceding sequence $A^{(0)}$. In Table 2, the entry 0 at position $N = 28$ results upon subtraction of entries and hence, the new sequence $A^{(1)}$ is the sequence with the subtracted entries.

The position number of the first non-zero entry beyond position $a_1$ in the sequence $A^{(1)}$ is denoted by $a_2$ (from table 2, $a_2$ has value 3). We use the sequence $A^{(1)}$ itself to generate the sequence $A^{(2)}$. we subtract the entry at position $m$ of $A^{(1)}$ from the entry in the position $ma_2, m = 1,2, ...$ for $ma_2 \leq N$. In this case; the entries are thus subtracted up to 27 leaving 28 without being subtracted. This indicates that 3 is relatively prime to 28. Thus, the new sequence $A^{(2)}$ is taken to be the same sequence $A^{(1)}$. We note that, the entry at position $m = 1,2, ...$ is subtracted from entry at position $ma_1$, thereby replacing the operation of leaving 0 as 0 as was done in the previous method.

In general, we locate the position of the first non-zero entry beyond position $a_{k-1}$ in the sequence $A^{(k-1)}$and denote this position by $a_k$. We subtract the entry at position $m = 1,2,\ldots$ from the entries at position $ma_k$ for $ma_k \leq N$. If the subtraction process leads to an entry 0 at the $N^{th}$ position then this would result in the new sequence $A^{(k)}$ of subtracted entries. Otherwise the sequence $A^{(k)}$ is taken to be same as sequence $A^{(k-1)}$. The process of termination of the sequence $A^{(k-1)}$ at position $a_k$ is similar to the one described in Modification 1. The sequence $A^{(k-1)}$ coincides with the function ${\chi^N}_{rp}$.

**Table-2**

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $A^{(0)}$ | 1 | $\underline{1}$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | | -1 | | -1 | | -1 | | -1 | | -1 | | -1 | | -1 | | -1 | | -1 | | -1 | | -1 | | -1 | | -1 | | -1 |
| $A^{(1)}$ | 1 | 0 | $\underline{1}$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| | | | -1 | | | -0 | | | -1 | | | -0 | | | -1 | | | -0 | | | -1 | | | -0 | | | -1 | |
| $A^{(2)}$ | 1 | 0 | 1 | 0 | $\underline{1}$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| | | | | | -1 | | | | | -0 | | | | | -1 | | | | | -0 | | | | | -1 | | | |
| $A^{(3)}$ | 1 | 0 | 1 | 0 | 1 | 0 | $\underline{1}$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| | | | | | | | -1 | | | | | | | -0 | | | | | | | -1 | | | | | | | -0 |
| $A^{(4)}$ | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |

## ACKNOWLEDGEMENTS

I thank MHRD, Govt. of India for supporting my research through UGC-BSR Fellowship.

## REFERENCE

1. B.N.Prasad Rao and M.Rangamma “Criterion for a prime below a given integer to be relatively prime”, Bulletin of mathematics and statistics research, October, 2015, pages 135-136.
2. R.G.Buschman “Some simple sieves”, Fibonacci Quarterly, October 1973, pages 247-254.

**Source of support: MHRD, Govt. of India, Conflict of interest: None Declared**