Sieve of Eratosthenes

Algorithm 1: Sieve of Eratosthenes

Data: A postive integer $n \geq 2$

Result: An array $M[2 \mathinner{..} n]$ such that $M[i] = 0$ if i is prime and 1 if i is composite

```
begin
    Let M[2 .. n] be initialized with all elements = 0;
    for i ← 2 to n do
        if M[i] ≠ 1 then
            for j ← 2i and j ≤ n do
                M[j] ← 1;
                j ← j + i;
            end
        end
        i ← i + 1;
    end
    return M;
end
```

1 Proof of Correctness (By Induction)

1.1 Inductive Hypothesis

Let $P(i)$:= At the beginning of the outer for loop, all prime numbers $< i$ have been found (set to 0 in M) and the multiples of all these primes have been marked (set to 1) in M.

1.2 Base Case

Initially, $i = 2$. As there are no prime numbers less than 2 and our indexing for M begins from 2, P(2) is trivially true.

1.3 Inductive Step

Assume the $P(k)$ to be true for some $k \geq 2$. When $i = k+1$, we have two cases. If k is composite, it can expressed as the product of primes i.e $k = p_1^{\alpha_1} p_2^{\alpha_2} \ \ldots \ p_n^{\alpha_n}$ where p_j is a prime number $< k$. According to our assumption, this would mean that k has already been marked (set to 1 in M). The inner loop will not execute.

If k is indeed prime, then none of the previous marking procedures would have affected $M[k]$. As $M[k]$ was initially set 0, it will continue to remain 0. In addition to this, the inner loop will execute successfully and mark all multiples of k.

In both the cases, we have now found all prime numbers less than $k+1$ and marked their multiples i.e $P(k+1)$ holds true.

1.4 Termination

The procedure terminates when $i > n$. As i is always incremented by 1, i will always be equal to $n+1$ when the procedure terminates. $\therefore P(n+1)$ is true i.e all prime numbers $< n+1$ have been found. $\blacksquare$