MODULE *SieveOfEratosthenes*

EXTENDS *Naturals*, *Sequences*

algorithm Sieve of *Eratosthenes* is input: an integer $n > 1$. output: all prime number from 2 through n.

let A be an array of Boolean values, indexed by integers 2 to n, initially all set to true.

for $i = 2, 3, 4, \ldots$, not exceeding n do if $A[i]$ is true
    for $j = i2,\ i2 + i,\ i2 + 2i,\ i2 + 3i,\ \ldots$, not exceeding n do set $A[j] :=$ false

return all i such that $A[i]$ is true.

CONSTANT N

$SquareRootForNExists \triangleq \exists\, x \quad \in 1 \,..\, N : x^2 = N$

$SquareRoot(n) \triangleq$ CHOOSE $sqrt \in 1 \,..\, n \ : sqrt^2 = n$

VARIABLES *numbers*
$vars \triangleq \langle numbers \rangle$

$Init \triangleq$
    $\wedge\ numbers = 0 \,..\, N$
    $\wedge\ SquareRootForNExists$

$TypeOK \triangleq$
    $\wedge\quad numbers \subseteq Nat$

$RemoveIfPresent(i) \triangleq$
  $\wedge\ i \in numbers$
  $\wedge\ numbers' = numbers \setminus \{i\}$

$RemoveNonPrimesByMultiplesOf(i) \triangleq$
    LET $non\_primes \triangleq \{(i * 2) + (i * j) : j \in 0 \,..\, N\}$
        $non\_primes\_not\_lager\_n \triangleq \{x \in non\_primes : x \leq N\}$
    IN $\exists\, x \in non\_primes\_not\_lager\_n :$
        $RemoveIfPresent(x)$

$Next \triangleq \exists\, i \in 2 \,..\, SquareRoot(N) : RemoveNonPrimesByMultiplesOf(i)$

$Spec \triangleq Init \wedge \quad \Box[Next]_{vars}$

THEOREM $Spec \Rightarrow \Box TypeOK$

$Divides(k,\ number) \triangleq$
$\quad \lor \ k \% number = 0$
$\quad \lor \ number \% k = 0$

$isNoPrime(number) \triangleq \exists\, k \in 2\,..\,number - 1 : Divides(k,\ number)$

Invariant that gets false when numbers does only contain Primes
$NumbersContainsNotOnlyPrimes \triangleq \exists\, n \in numbers : isNoPrime(n)$

\ * Modification History
\ * Last modified *Tue Mar* 05 15:52:25 *CET* 2024 by *JUFIGGE*
\ * Created *Fri Mar* 05 13:15:02 *CET* 2024 by *JeuJeus*