MODULE *SieveOfEratosthenes*

EXTENDS *Naturals*

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 $sqrt(n)$ 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 input: an integer $n > 1$

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

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

VARIABLES $numbers$, $iterator$
$vars \triangleq \langle numbers,\ iterator \rangle$

$Init \triangleq$
$\land\ numbers = 0 \,..\, N$ output: all prime number from 2 through n
$\land\ iterator = 2 \,..\, SquareRoot(N)$ let A be an array of Boolean values, indexed by integers 2 to n, initially all set to tru
$\land\ SquareRootForNExists$

$TypeOK \triangleq$
$\land\quad numbers \subseteq Nat$
$\land\quad iterator \subseteq Nat$

$GetCurrentNumberFromIterator \triangleq$ CHOOSE $i \in iterator : i = i$ trick to choose fixed number instead of iterating all p

$RemoveNonPrimesByMultiplesOf(i) \triangleq$
LET $non\_primes \triangleq \{(i * 2) + (i * j) : j \in 0 \,..\, N\}$ for $j = i2,\ i2 + i,\ i2 + 2i,\ i2 + 3i,\ \ldots$
        $non\_primes\_not\_larger\_n \triangleq \{x \in non\_primes : x \leq N\}$ for $j = i2,\ i2 + i,\ i2 + 2i,\ i2 + 3i,\ \ldots$, not exc
IN $numbers' = numbers \setminus non\_primes\_not\_larger\_n$

$HandleCurrentNumberBasedOnPresenceinNumbers(i) \triangleq$
$\lor\ \land\ i \in numbers$ if $A[i]$ is true
    $\land\ RemoveNonPrimesByMultiplesOf(i)$
$\lor\ numbers' = numbers$

$Next \triangleq$ LET $i \triangleq GetCurrentNumberFromIterator$ for $i = 2, 3, 4, \ldots,$ not exceeding $sqrt(n)$ do
IN $\land\ iterator' = iterator \setminus \{i\}$
$\land\ RemoveNonPrimesByMultiplesOf(i)$

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

THEOREM $Spec \Rightarrow \Box\, TypeOK$

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

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

Invariant that gets false when numbers does only contain Primes
$NumbersContainsNotOnlyPrimes \triangleq \exists\, n \in numbers : isNoPrime(n)$ return all i such that $A[i]$ is true.

---

* Modification History
* Last modified *Wed Mar* 06 10:18:51 *CET* 2024 by *JUFIGGE*
* Created *Fri Mar* 05 13:15:02 *CET* 2024 by *JeuJeus*