Number Theory Algorithms

Ervin Gegprifti

gegprifti.ervin@gmail.com

Abstract

This paper is the documentation for the Calculator module in Number Theory Algorithms mobile application.

Calculator operations

Addition: $a + b$

Description: Add b to a.
Input: a, b, where $a, b \in \mathbb{Z}$
Output: $a + b$

Subtraction: $a - b$

Description: Subtract b from a.
Input: a, b, where $a, b \in \mathbb{Z}$
Output: $a - b$

Multiplication: $a \times b$

Description: Multiply a with b.
Input: a, b, where $a, b \in \mathbb{Z}$
Output: $a \times b$

Division: a/b

Description: Divide a with b.
Input: a, b, where $a \in \mathbb{Z}$, $b \in \mathbb{Z}_{\neq 0}$
Output: quotient as $\lfloor a/b \rfloor$, remainder as $a - (\lfloor a/b \rfloor b)$

Power: a^b

Description: Raise a to the power of b.
Input: a, b, where $a \in \mathbb{Z}$, $b = \{0, \ldots, 2147483647\}$
Output: a^b

Root: $\sqrt[b]{a}$

Description: The b root of a.
Input: a, b, where $a \in \mathbb{Z}$, $b = \{1, \ldots, 2147483647\}$
Output: $\sqrt[b]{a}$

Greatest Common Divisor: $GCD(|a|, |b|)$

Description: The largest number that divides both a and b without leaving a remainder.
Input: a, b, where $a, b \in \mathbb{Z}$
Output: $GCD(|a|, |b|)$

Lowest Common Multiple: $LCM(a, b)$

Description: The smallest integer that is evenly divisible by both a and b.
Input: a, b, where $a, b \in \mathbb{Z}$, not both 0
Output: $LCM(a, b) = (ab)/GCD(a, b)$ since $(ab) = GCD(a, b)LCM(a, b)$

Modulo: $a \pmod b$

Description: The remainder when a is divided by b.
Input: a, b, where $a \in \mathbb{Z}$, $b \in \mathbb{Z}_{\geq 1}$
Output: $a \pmod b$, output is always a non-negative number

Modulo Inverse: $a^{-1} \pmod b$

Description: Modular inverse of $a \pmod b$ is a^{-1}. If $a \equiv c \pmod b$, then $aa^{-1} \equiv 1 \pmod b$.
Input: a, where $a \in \mathbb{Z}$, $b \in \mathbb{Z}_{\geq 1}$
Output: $a^{-1} \pmod b$

Is probable prime:

Description: Check if a number is probable prime within a certain certainty.
Input: a, where $a \in \mathbb{Z}$ with $a \geq 2$, $b = \{1, \ldots, 2147483647\}$
Output: 1 if a is probably prime with probability $1 - 1/2^b$, 0 if a is definitely composite

Euler's phi-function: $\phi(a)$

Relatively prime definition. The integers d and e, with $d \neq 0$ and $e \neq 0$, are relatively prime if d and e have greatest common divisor $(d, e) = 1$. Because $(25, 42) = 1$, then 25 and 42 are relatively prime.
Euler's phi-function $\phi(a)$ definition. Let a be a positive integer. The $\phi(a)$ is defined to be the number of positive integers not exceeding a that are relatively prime to a.
Example.
$\phi(1) = 1$ because $\left\{ \begin{array}{l} \text{(1,1)=1} \longrightarrow counter = 1 \end{array} \right.$

$\phi(2) = 1$ because $\left\{ \begin{array}{l} \text{(1,2)=1} \longrightarrow counter = 1 \\ \text{(2,2)=2} \end{array} \right.$

$\phi(3) = 2$ because $\left\{ \begin{array}{l} \text{(1,3)=1} \longrightarrow counter = 1 \\ \text{(2,3)=1} \longrightarrow counter = 2 \\ \text{(3,3)=3} \end{array} \right.$

$\phi(4) = 2$ because $\left\{ \begin{array}{l} \text{(1,4)=1} \longrightarrow counter = 1 \\ \text{(2,4)=2} \\ \text{(3,4)=1} \longrightarrow counter = 2 \\ \text{(4,4)=4} \end{array} \right.$

$$\phi(5) = 4 \text{ because } \begin{cases} (1,5)=1 \longrightarrow counter = 1 \\ (2,5)=1 \longrightarrow counter = 2 \\ (3,5)=1 \longrightarrow counter = 3 \\ (4,5)=1 \longrightarrow counter = 4 \\ (5,5)=5 \end{cases}$$

Factorial: $a!$

Description: Calculates the $a! = 1 \times 2 \times 3 \times \cdots \times a$.
Input: a, where $a \in \mathbb{Z}$ with $a > 0$
Output: $a!$

Next probable prime:

Description: The next probable prime to a number.
Input: a, where $a \in \mathbb{Z}$ with $a \geq 2$
Output: next probable prime to a

Next twin prime to a:

Description: The next probable twin prime pair to a.
Input: a, where $a \in \mathbb{Z}$ with $a > 2$
Output: next probable twin prime pair to a

References

[1] "Class BigInteger." java.math.BigInteger