Number Theory Algorithms

Ervin Gegprifti

gegprifti.ervin@gmail.com

Abstract

Nothing to claim here. This paper is the documentation for the Calculator module in Number Theory Algorithms mobile application.

Calculator operations

Addition: $+$

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

Subtraction: $-$

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

Multiplication: $\times$

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

Division: $\div$

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: $\sqrt{}$

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

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

Description: The smallest integer that is evenly divisible by both a and b.
Input: a, b, where $a, b \in \mathbb{Z}$, $b \in \mathbb{Z}$
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 $a \in \mathbb{Z}_{\geq 2}$, $b = \{1, \ldots, 2147483647\}$
Output: 1 if a is probably prime with probability $1 - 1/2^b$, 0 if a is definitely composite

Next probable prime:

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

References

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