Number Theory I

Ulises Méndez Martínez

Algorist Weekly Talks

ulisesmdzmtz@gmail.com

March 14, 2016

Mathematics

NUMB3RS

We all use math every day; to predict weather, to tell time, to handle money. Math is more than formulas or equations; it's logic, it's rationality, it's using your mind to solve the biggest mysteries we know.

What is number theory?

Number theory is the study of the set of positive whole numbers: 1,2,3,... which are often called the set of natural numbers. We will especially want to study the relationships between different sorts of numbers.

What is number theory?

Number theory is the study of the set of positive whole numbers: 1,2,3,... which are often called the set of natural numbers. We will especially want to study the relationships between different sorts of numbers.

Source: https://www.math.brown.edu

- odd $1, 3, 5, 7, 9, 11, \ldots$
- even $2, 4, 6, 8, 10, \ldots$
- square $1, 4, 9, 16, 25, 36, \ldots$
- cube $1, 8, 27, 64, 125, \ldots$
- prime $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$
- 1 (modulo 4) $1, 5, 9, 13, 17, 21, 25, \ldots$
- triangular $1, 3, 6, 10, 15, 21, \ldots$
- perfect $6, 28, 496, \ldots$
- Fibonacci $1, 1, 2, 3, 5, 8, 13, 21, \ldots$

Divisibility

Divisor

In mathematics a divisor of an integer **n**, also called a factor of **n**, is an integer that can be multiplied by some other integer to produce **n**. An integer **n** is divisible by another integer **m** if **m** is a factor of **n**, so that dividing **n** by **m** leaves no remainder.

Divisibility

Divisor

In mathematics a divisor of an integer **n**, also called a factor of **n**, is an integer that can be multiplied by some other integer to produce **n**. An integer **n** is divisible by another integer **m** if **m** is a factor of **n**, so that dividing **n** by **m** leaves no remainder.

Definition

A **prime** number (or a prime) is a natural number greater than **1** that has no positive divisors other than **1** and itself. A natural number greater than **1** that is not a prime number is called a **composite** number.

Divisibility

Divisor

In mathematics a divisor of an integer **n**, also called a factor of **n**, is an integer that can be multiplied by some other integer to produce **n**. An integer **n** is divisible by another integer **m** if **m** is a factor of **n**, so that dividing **n** by **m** leaves no remainder.

Definition

A **prime** number (or a prime) is a natural number greater than **1** that has no positive divisors other than **1** and itself. A natural number greater than **1** that is not a prime number is called a **composite** number.

Fundamental theorem of arithmetic

It states that every integer greater than **1** either is prime itself or is the product of prime numbers, and that this product is unique, up to the order of the factors.

Question?

Which is fastest algorithm to find prime numbers?

Question?

Which is fastest algorithm to find prime numbers?

- Sieve of Eratosthenes

Question?

Which is fastest algorithm to find prime numbers?

- Sieve of Eratosthenes
- Sieve of Atkin

Question?

Which is fastest algorithm to find prime numbers?

- Sieve of Eratosthenes
- Sieve of Atkin
- Linear Prime Sieve

GCD & LCM

Greatest common divisor

In mathematics, the greatest common divisor (*gcd*) of two or more integers, when at least one of them **is not zero**, is the largest positive integer that divides the numbers without a remainder.

GCD & LCM

Greatest common divisor

In mathematics, the greatest common divisor (*gcd*) of two or more integers, when at least one of them **is not zero**, is the largest positive integer that divides the numbers without a remainder.

Coprime numbers

Two numbers are called relatively prime, or coprime, if their greatest common divisor equals **1**. For example, 9 and 28 are relatively prime.

GCD & LCM

Greatest common divisor

In mathematics, the greatest common divisor (*gcd*) of two or more integers, when at least one of them **is not zero**, is the largest positive integer that divides the numbers without a remainder.

Coprime numbers

Two numbers are called relatively prime, or coprime, if their greatest common divisor equals **1**. For example, 9 and 28 are relatively prime.

Least common multiple

The lowest common multiple of two integers **a** and **b**, Is the smallest positive integer that is divisible by both **a** and **b**. Since division of integers by zero is undefined, this definition has meaning **only if a and b are both different from zero**.

Calculation

Calculation

Prime factorizations

Greatest common divisors can in principle be computed by determining the prime factorizations of the two numbers and comparing factors; $\mathbf{gcd(18, 84)}$, $18 = 2 \times 3^2$ and $84 = 2^2 \times 3 \times 7$, then $gcd(18, 84) = 6$

Calculation

Prime factorizations

Greatest common divisors can in principle be computed by determining the prime factorizations of the two numbers and comparing factors; $\mathbf{gcd(18, 84)}$, $18 = 2 \times 3^2$ and $84 = 2^2 \times 3 \times 7$, then $gcd(18, 84) = 6$

Binary method

Also known as Stein's algorithm. It uses simpler arithmetic operations than the conventional Euclidean algorithm; it replaces division with arithmetic shifts, comparisons, and subtraction.

Calculation

Prime factorizations

Greatest common divisors can in principle be computed by determining the prime factorizations of the two numbers and comparing factors; $\mathbf{gcd(18, 84)}$, $18 = 2 \times 3^2$ and $84 = 2^2 \times 3 \times 7$, then $gcd(18, 84) = 6$

Binary method

Also known as Stein's algorithm. It uses simpler arithmetic operations than the conventional Euclidean algorithm; it replaces division with arithmetic shifts, comparisons, and subtraction.

Euclid's algorithm

The Euclidean algorithm is based on the principle that the greatest common divisor of two numbers does not change if the larger number is replaced by its difference with the smaller number.

Implementation

Recursive version

```
int gcd(int a, int b) {return (b==0)?a:gcd(b,a%b);}
```

Implementation

Recursive version

```
int gcd(int a, int b) {return (b==0)?a:gcd(b,a%b);}
```

How to swap two numbers without using temp variables nor arithmetic operations?

Implementation

Recursive version

```
int gcd(int a, int b) {return (b==0)?a:gcd(b,a%b);}
```

How to swap two numbers without using temp variables nor arithmetic operations?

Iterative version

```
int gcd(int a, int b) {
    while(b) {
        a %= b;
        b ^= a;
        a ^= b;
        b ^= a;
    }
    return a;
}
```

Modular arithmetic

In mathematics, modular arithmetic is a system of arithmetic for integers, where numbers "wrap around" upon reaching a certain value (**the modulus**).

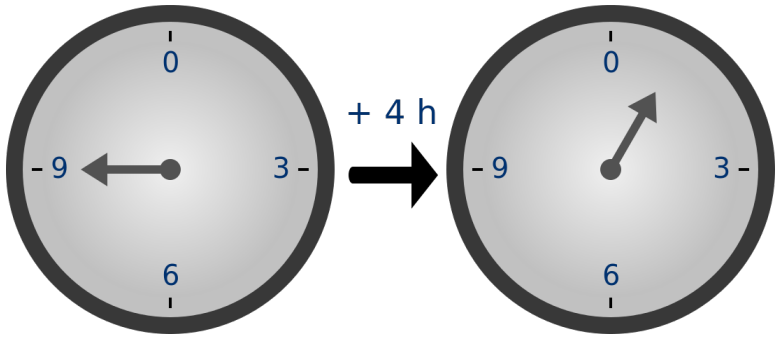

Figure : Time-keeping on this clock uses arithmetic modulo 12.

Modulo operator

Theorem (Euclidean division)

*Given two integers a and b ($b \neq 0$), there exist **unique** integers q and r such that:*

$$a = bq + r$$

$$0 \leq r < |b|$$

where $|b|$ denotes the absolute value of b.

Given two positive numbers, a (the dividend) and n (the divisor), a modulo n (abbreviated as $amodn$) is the remainder of the Euclidean division of a by n.

Equivalencies

Identity

- $(a \mod n) \mod n = a \mod n$.
- $n^x \mod n = 0$ for all positive integer values of x.
- If p is a prime number which is not a divisor of b, then $ab^{p-1} \mod p = a \mod p$, due to Fermat's little theorem.

Equivalencies

Identity

- $(a \mod n) \mod n = a \mod n$.
- $n^x \mod n = 0$ for all positive integer values of x.
- If p is a prime number which is not a divisor of b, then $ab^{p-1} \mod p = a \mod p$, due to Fermat's little theorem.

Inverse

- $[(-a \mod n) + (a \mod n)] \mod n = 0$.
- $b^{-1} \mod n$ denotes the modular multiplicative inverse, which is defined if and only if b and n are relatively prime, which is the case when the left hand side is defined: $[(b^{-1} \mod n)(b \mod n)] \mod n = 1$.

Equivalencies (cont)

Distributive

- $(a+b) \mod n = [(a \mod n) + (b \mod n)] \mod n$.
- $ab \mod n = [(a \mod n)(b \mod n)] \mod n$.

Equivalencies (cont)

Distributive

- $(a + b) \mod n = [(a \mod n) + (b \mod n)] \mod n$.
- $ab \mod n = [(a \mod n)(b \mod n)] \mod n$.

Example (Big Number Modulus Small One)

```
int mod(string s, int m) {
    int i, res = 0;
    for(i=0;i<s.length;i++) {
        res = res*10+(s[i]-'0');
        res %= m;
    }
    return res;
}
```

Q & A

References

- www.codechef.com/wiki/tutorial-number-theory
- www.hackerrank.com/domains/mathematics/number-theory
- oeis.org/A051193
- projecteuler.net/
- codeforces.com/problemset/tags/number_theory