Elementary Number Theory Part 1

Divisibility – Number Representation in Base b

MZI

School of Computing
Telkom University

SoC Tel-U

June 2023

Acknowledgements

This slide is composed based on the following materials:

1. *Discrete Mathematics and Its Applications*, 8th Edition, 2019, by K. H. Rosen (main).
2. *Discrete Mathematics with Applications*, 5th Edition, 2018, by S. S. Epp.
3. *Mathematics for Computer Science*. MIT, 2010, by E. Lehman, F. T. Leighton, A. R. Meyer.
4. Slide for Matematika Diskret 2 (2012). Fasilkom UI, by B. H. Widjaja.
5. Slide for Matematika Diskret 2 at Fasilkom UI by Team of Lecturers.
6. Slide for Matematika Diskret. Telkom University, by B. Purnama.

Some of the pictures are taken from the above resources. This slide is intended for academic purpose at FIF Telkom University. If you have any suggestions/comments/questions related to the material on this slide, send an email to <pleasedontspam>@telkomuniversity.ac.id.

Contents

Contents

Why Do We Need to Learn about Number Theory?

Number theory is prevalently used in many research areas in computer science, for example:

Why Do We Need to Learn about Number Theory?

Number theory is prevalently used in many research areas in computer science, for example:

1. methods to develop algorithms for generating random numbers in computer (pseudo-random number generation),

Why Do We Need to Learn about Number Theory?

Number theory is prevalently used in many research areas in computer science, for example:

1. methods to develop algorithms for generating random numbers in computer (pseudo-random number generation),
2. methods to develop a cryptosystem or key exchange protocol,

Why Do We Need to Learn about Number Theory?

Number theory is prevalently used in many research areas in computer science, for example:

1. methods to develop algorithms for generating random numbers in computer (pseudo-random number generation),
2. methods to develop a cryptosystem or key exchange protocol,
3. methods to formulate algorithms pertaining to integers (i.e., the greatest common divisor ($\gcd$) and the least common multiple (lcm)).

Example of Number Theory Application: Diffie-Hellman Protocol

Number Theory in Competitive Programming

Inti Sets

by *IEEEXtreme*

Problem | Submissions | Leaderboard | Discussions

In order to motivate his Peruvian students, a teacher includes words in the Quechua language in his math class.

Today, he defined a curious set for a given positive integer *N*. He called this set, an ***Inti set***, and defined it as the set of all positive integer numbers that have the number *1* as their single common positive divisor with number *N*.

The math class about Inti sets was amazing. After class, the students try to challenge to teacher. They each ask questions like this: "Could you tell me the sum of all numbers, between *A* and *B* (inclusive), that are in the Inti set of *N*?"

Since the teacher is tired and he's sure that you are the best in class, he wants to know if you can help him.

Input Format

The first line of input contains an integer *Q*, $1 \le Q \le 20$, representing the number of students. Each of the next *Q* lines contain three space-separated integers *N*, *A* and *B*, which represent a query.

Constraints

$1 \le A \le B \le N \le 10^{12}$

Output Format

The output is exactly Q lines, one per student query. For each query you need to find the sum of all numbers between A and B, that are in the Inti set of N, and print the sum modulo 1000000007.

Number Theory in Competitive Programming

2013 World Finals
acm International Collegiate Programming Contest
IBM event sponsor
ICPC 2013 St. Petersburg HOSTED BY ITMO

Problem D
Factors
Time Limit: 2 seconds

The fundamental theorem of arithmetic states that every integer greater than 1 can be uniquely represented as a product of one or more primes. While unique, several arrangements of the prime factors may be possible. For example:

$$10 = 2 \cdot 5 \qquad 20 = 2 \cdot 2 \cdot 5$$
$$= 5 \cdot 2 \qquad = 2 \cdot 5 \cdot 2$$
$$= 5 \cdot 2 \cdot 2$$

Let $f(k)$ be the number of different arrangements of the prime factors of k. So $f(10) = 2$ and $f(20) = 3$.

Given a positive number n, there always exists at least one number k such that $f(k) = n$. We want to know the smallest such k.

Contents

Divisibility in $\mathbb{Z}$

We have $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. The set of all *positive* integers is denoted by $\mathbb{Z}^+$. Suppose a and b are two integers. The result of a/b *is not always* an integer. For example $12/6 = 2 \in \mathbb{Z}$ but $12/5 = 2.4 \notin \mathbb{Z}$.

Definition (Divisibility)

Given two integers a and b with $a \neq 0$, then:

Divisibility in $\mathbb{Z}$

We have $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. The set of all *positive* integers is denoted by $\mathbb{Z}^+$. Suppose a and b are two integers. The result of a/b *is not always* an integer. For example $12/6 = 2 \in \mathbb{Z}$ but $12/5 = 2.4 \notin \mathbb{Z}$.

Definition (Divisibility)

Given two integers a and b with $a \neq 0$, then:

1. We say that b is *divisible* by a, denoted by $a|b$, if there is $k \in \mathbb{Z}$ that satisfies $b = k \cdot a$.

Divisibility in $\mathbb{Z}$

We have $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. The set of all *positive* integers is denoted by $\mathbb{Z}^+$. Suppose a and b are two integers. The result of a/b *is not always* an integer. For example $12/6 = 2 \in \mathbb{Z}$ but $12/5 = 2.4 \notin \mathbb{Z}$.

Definition (Divisibility)

Given two integers a and b with $a \neq 0$, then:

1. We say that b is *divisible* by a, denoted by $a|b$, if there is $k \in \mathbb{Z}$ that satisfies $b = k \cdot a$.
2. If $a|b$, then a is called as a factor or divisor of b, and b is called as a dividend (or multiple) of a.

Divisibility in $\mathbb{Z}$

We have $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. The set of all *positive* integers is denoted by $\mathbb{Z}^+$. Suppose a and b are two integers. The result of a/b *is not always* an integer. For example $12/6 = 2 \in \mathbb{Z}$ but $12/5 = 2.4 \notin \mathbb{Z}$.

Definition (Divisibility)

Given two integers a and b with $a \neq 0$, then:

1. We say that b is *divisible* by a, denoted by $a|b$, if there is $k \in \mathbb{Z}$ that satisfies $b = k \cdot a$.
2. If $a|b$, then a is called as a factor or divisor of b, and b is called as a dividend (or multiple) of a.
3. Notation $a \nmid b$ denotes that b is not divisible by a.

Notice that the condition $a|b$ is equivalent with the predicate logic formula $\exists k\,(ka = b)$ where its universe of discourse is the set of all integers.

Example

We have

Example

We have

1. $2|4$ because there is $k = 2$ such that $4 = 2 \cdot (2)$

Example

We have

1. $2|4$ because there is $k = 2$ such that $4 = 2 \cdot (2)$
2. $4|-8$ because there is $k = -2$ such that $-8 = 4 \cdot (-2)$

Example

We have

1. $2|4$ because there is $k = 2$ such that $4 = 2 \cdot (2)$
2. $4| - 8$ because there is $k = -2$ such that $-8 = 4 \cdot (-2)$
3. $7|0$ because there is $k = 0$ such that $0 = 7 \cdot (0)$

Example

We have

1. $2|4$ because there is $k = 2$ such that $4 = 2 \cdot (2)$
2. $4|-8$ because there is $k = -2$ such that $-8 = 4 \cdot (-2)$
3. $7|0$ because there is $k = 0$ such that $0 = 7 \cdot (0)$
4. $2 \nmid 1$ because there is no integer k such that $1 = 2k$

Example

We have

1. $2|4$ because there is $k = 2$ such that $4 = 2 \cdot (2)$
2. $4| - 8$ because there is $k = -2$ such that $-8 = 4 \cdot (-2)$
3. $7|0$ because there is $k = 0$ such that $0 = 7 \cdot (0)$
4. $2 \nmid 1$ because there is no integer k such that $1 = 2k$
5. $4 \nmid 7$ because there is no integer k such that $7 = 4k$

Example

We have

1. $2|4$ because there is $k = 2$ such that $4 = 2 \cdot (2)$
2. $4| - 8$ because there is $k = -2$ such that $-8 = 4 \cdot (-2)$
3. $7|0$ because there is $k = 0$ such that $0 = 7 \cdot (0)$
4. $2 \nmid 1$ because there is no integer k such that $1 = 2k$
5. $4 \nmid 7$ because there is no integer k such that $7 = 4k$
6. $8 \nmid -4$ because there is no integer k such that $-4 = 8k$

Exercise: Divisibility

Exercise

Check whether the following statements are correct or not:

1. 6 is a divisor of 54
2. -27 is a multiple of 3
3. 3 is a divisor of 91
4. 17 is a multiple of -3
5. 4 is a divisor of 0

Solution:

Exercise: Divisibility

Exercise

Check whether the following statements are correct or not:

1. 6 is a divisor of 54
2. -27 is a multiple of 3
3. 3 is a divisor of 91
4. 17 is a multiple of -3
5. 4 is a divisor of 0

Solution:

1. True, because there is $k = 9$ such that $6 \cdot 9 = 54$.

Exercise: Divisibility

Exercise

Check whether the following statements are correct or not:

1. 6 is a divisor of 54
2. -27 is a multiple of 3
3. 3 is a divisor of 91
4. 17 is a multiple of -3
5. 4 is a divisor of 0

Solution:

1. True, because there is $k = 9$ such that $6 \cdot 9 = 54$.
2. True, because there is $k = -9$ such that $3 \cdot (-9) = -27$.

Exercise: Divisibility

Exercise

Check whether the following statements are correct or not:

1. 6 is a divisor of 54
2. -27 is a multiple of 3
3. 3 is a divisor of 91
4. 17 is a multiple of -3
5. 4 is a divisor of 0

Solution:

1. True, because there is $k = 9$ such that $6 \cdot 9 = 54$.
2. True, because there is $k = -9$ such that $3 \cdot (-9) = -27$.
3. False, because there is no $k \in \mathbb{Z}$ such that $3 \cdot k = 91$ (because $91/3 = 30\frac{1}{3} \notin \mathbb{Z}$).

Exercise: Divisibility

Exercise

Check whether the following statements are correct or not:

1. 6 is a divisor of 54
2. -27 is a multiple of 3
3. 3 is a divisor of 91
4. 17 is a multiple of -3
5. 4 is a divisor of 0

Solution:

1. True, because there is $k = 9$ such that $6 \cdot 9 = 54$.
2. True, because there is $k = -9$ such that $3 \cdot (-9) = -27$.
3. False, because there is no $k \in \mathbb{Z}$ such that $3 \cdot k = 91$ (because $91/3 = 30\frac{1}{3} \notin \mathbb{Z}$).
4. False, because there is no $k \in \mathbb{Z}$ such that $-3 \cdot k = 17$ (because $17/-3 = -5\frac{2}{3} \notin \mathbb{Z}$).

Exercise: Divisibility

Exercise

Check whether the following statements are correct or not:

1. 6 is a divisor of 54
2. -27 is a multiple of 3
3. 3 is a divisor of 91
4. 17 is a multiple of -3
5. 4 is a divisor of 0

Solution:

1. True, because there is $k = 9$ such that $6 \cdot 9 = 54$.
2. True, because there is $k = -9$ such that $3 \cdot (-9) = -27$.
3. False, because there is no $k \in \mathbb{Z}$ such that $3 \cdot k = 91$ (because $91/3 = 30\frac{1}{3} \notin \mathbb{Z}$).
4. False, because there is no $k \in \mathbb{Z}$ such that $-3 \cdot k = 17$ (because $17/-3 = -5\frac{2}{3} \notin \mathbb{Z}$).
5. True, because there is $k = 0$ such that $4 \cdot 0 = 0$.

Theorem of Divisibility

Theorem

Suppose $a, b, c \in \mathbb{Z}$, then

1. if $a|b$ and $a|c$, then $a|\,(b+c)$
2. if $a|b$, then $a|bd$, for *every* $d \in \mathbb{Z}$
3. if $a|b$ and $b|c$, then $a|c$

Proof

The proof is left for the reader as exercises, proof for property no. 3 has been discussed in transitive relation topic, because divisibility is a transitive relation.

Theorem

If $a, b, c \in \mathbb{Z}$ with properties $a|b$ and $a|c$, then for *every* $m, n \in \mathbb{Z}$ we have $a|mb + nc$.

Proof

The proof is left for the reader as an exercise (hint: use properties no. 2 and no. 1 from the previous theorem).

Properties of Divisibility Relation

Suppose $a, b \in \mathbb{Z}$ and we have a relation R that is defined as $aRb \Leftrightarrow a|b$, then

1. Relation $|$ is reflexive because $a|a$ for every $a \in \mathbb{Z}$
2. Relation $|$ is transitive because if $a|b$ and $b|c$, then $a|c$, for every $a, b, c \in \mathbb{Z}$.

Do you think $|$ is symmetric? (Relation R is symmetric if we have: $\forall a \forall b \, (aRb \rightarrow bRa)$.)

Division Theorem

Theorem (Division Theorem)

If a is an integer and d is a positive integer, then there are unique integers q and r where $0 \leq r < d$ that satisfy $a = dq + r$, furthermore:

- q is called as the quotient of a divided by d, and is denoted as $a \operatorname{div} d$,
- r is called as the remainder of a divided by d, and is denoted as $a \bmod d$.

Example

Notice that

1. if $a = 17$ and $d = 8$, then $q =$

Division Theorem

Theorem (Division Theorem)

If a is an integer and d is a positive integer, then there are unique integers q and r where $0 \leq r < d$ that satisfy $a = dq + r$, furthermore:

- q is called as the quotient of a divided by d, and is denoted as $a \operatorname{div} d$,
- r is called as the remainder of a divided by d, and is denoted as $a \bmod d$.

Example

Notice that

1. if $a = 17$ and $d = 8$, then $q = 2$ and $r =$

Division Theorem

Theorem (Division Theorem)

If a is an integer and d is a positive integer, then there are unique integers q and r where $0 \leq r < d$ that satisfy $a = dq + r$, furthermore:

- q is called as the quotient of a divided by d, and is denoted as $a \operatorname{div} d$,
- r is called as the remainder of a divided by d, and is denoted as $a \bmod d$.

Example

Notice that

1. if $a = 17$ and $d = 8$, then $q = 2$ and $r = 1$, this is because $17 = 8 \cdot 2 + 1$.
2. if $a = 8$ and $d = 17$, then $q =$

Division Theorem

Theorem (Division Theorem)

If a is an integer and d is a positive integer, then there are unique integers q and r where $0 \leq r < d$ that satisfy $a = dq + r$, furthermore:

- q is called as the quotient of a divided by d, and is denoted as $a \operatorname{div} d$,
- r is called as the remainder of a divided by d, and is denoted as $a \bmod d$.

Example

Notice that

1. if $a = 17$ and $d = 8$, then $q = 2$ and $r = 1$, this is because $17 = 8 \cdot 2 + 1$.
2. if $a = 8$ and $d = 17$, then $q = 0$ and $r =$

Division Theorem

Theorem (Division Theorem)

If a is an integer and d is a positive integer, then there are unique integers q and r where $0 \leq r < d$ that satisfy $a = dq + r$, furthermore:

- q is called as the quotient of a divided by d, and is denoted as $a \operatorname{div} d$,
- r is called as the remainder of a divided by d, and is denoted as $a \bmod d$.

Example

Notice that

1. if $a = 17$ and $d = 8$, then $q = 2$ and $r = 1$, this is because $17 = 8 \cdot 2 + 1$.
2. if $a = 8$ and $d = 17$, then $q = 0$ and $r = 8$, this is because $8 = 17 \cdot 0 + 8$.

Remark

The value of remainder a divided by d ($a \bmod d$) is always non negative.
A programming language may have more than one modular arithmetic operator:

- mod is used in Prolog, BASIC, Maple, Mathematica, EXCEL, and SQL,
- $\%$ is used in C, C++, Java, and Python,
- rem is used in Ada and Lisp,

Some modular arithmetic operators in the above programming languages can give a negative value. Be careful when using them.

Exercise

Exercise

Determine the value of

1. $11 \operatorname{div} 3$ and $11 \bmod 3$
2. $-11 \operatorname{div} 3$ and $-11 \bmod 3$

Solution:

Exercise

Exercise

Determine the value of

1. $11 \operatorname{div} 3$ and $11 \bmod 3$
2. $-11 \operatorname{div} 3$ and $-11 \bmod 3$

Solution:

1. $11 = 3(3) + 2$, therefore $11 \operatorname{div} 3 = 3$ and $11 \bmod 3 = 2$

Exercise

Exercise

Determine the value of

1. $11 \operatorname{div} 3$ and $11 \bmod 3$
2. $-11 \operatorname{div} 3$ and $-11 \bmod 3$

Solution:

1. $11 = 3\,(3) + 2$, therefore $11 \operatorname{div} 3 = 3$ and $11 \bmod 3 = 2$
2. $-11 = 3\,(-4) + 1$, therefore $-11 \operatorname{div} 3 = -4$ and $-11 \bmod 3 = 1$. Remember that although $-11 = 3\,(-3) + (-2)$, it is not true that $-11 \bmod 3 = -2$, because a remainder must be nonnegative.

Exercise

Exercise

Determine the value of

1. $22 \operatorname{div} 3$ and $22 \bmod 3$
2. $-22 \operatorname{div} 3$ and $-22 \bmod 3$
3. $97 \operatorname{div} 4$ and $97 \bmod 4$
4. $-97 \operatorname{div} 4$ and $-97 \bmod 4$

Solution:

Exercise

Exercise

Determine the value of

1. $22 \operatorname{div} 3$ and $22 \bmod 3$
2. $-22 \operatorname{div} 3$ and $-22 \bmod 3$
3. $97 \operatorname{div} 4$ and $97 \bmod 4$
4. $-97 \operatorname{div} 4$ and $-97 \bmod 4$

Solution:

1. $22 = 3(7) + 1$, therefore $22 \operatorname{div} 3 = 7$ and $22 \bmod 3 = 1$.

Exercise

Exercise

Determine the value of

1. $22 \operatorname{div} 3$ and $22 \bmod 3$
2. $-22 \operatorname{div} 3$ and $-22 \bmod 3$
3. $97 \operatorname{div} 4$ and $97 \bmod 4$
4. $-97 \operatorname{div} 4$ and $-97 \bmod 4$

Solution:

1. $22 = 3(7) + 1$, therefore $22 \operatorname{div} 3 = 7$ and $22 \bmod 3 = 1$.
2. $-22 = 3(-8) + 2$, therefore $-22 \operatorname{div} 3 = -8$ and $-22 \bmod 3 = 2$.

Exercise

Exercise

Determine the value of

1. $22 \operatorname{div} 3$ and $22 \bmod 3$
2. $-22 \operatorname{div} 3$ and $-22 \bmod 3$
3. $97 \operatorname{div} 4$ and $97 \bmod 4$
4. $-97 \operatorname{div} 4$ and $-97 \bmod 4$

Solution:

1. $22 = 3(7) + 1$, therefore $22 \operatorname{div} 3 = 7$ and $22 \bmod 3 = 1$.
2. $-22 = 3(-8) + 2$, therefore $-22 \operatorname{div} 3 = -8$ and $-22 \bmod 3 = 2$.
3. $97 = 4(24) + 1$, therefore $97 \operatorname{div} 4 = 24$ and $97 \bmod 4 = 1$.

Exercise

Exercise

Determine the value of

1. $22 \operatorname{div} 3$ and $22 \bmod 3$
2. $-22 \operatorname{div} 3$ and $-22 \bmod 3$
3. $97 \operatorname{div} 4$ and $97 \bmod 4$
4. $-97 \operatorname{div} 4$ and $-97 \bmod 4$

Solution:

1. $22 = 3\,(7) + 1$, therefore $22 \operatorname{div} 3 = 7$ and $22 \bmod 3 = 1$.
2. $-22 = 3\,(-8) + 2$, therefore $-22 \operatorname{div} 3 = -8$ and $-22 \bmod 3 = 2$.
3. $97 = 4\,(24) + 1$, therefore $97 \operatorname{div} 4 = 24$ and $97 \bmod 4 = 1$.
4. $-97 = 4\,(-25) + 3$, therefore $-97 \operatorname{div} 4 = -25$ and $-97 \bmod 4 = 3$.

Theorem

Suppose $a \in \mathbb{Z}$, a is divisible by $d \in \mathbb{Z}$ (or in other word $d|a$) if and only if $a \bmod d = 0$.

Contents

Prime Numbers

Prime numbers are usually discussed in the set $\mathbb{Z}^+$.

Definition

A positive integer $p > 1$ is called prime if it has exactly two positive divisors, namely 1 and p. A positive integer that is greater than 1 and is *not a prime* is called a composite.

In other words, a positive integer is a prime number iff the number is not divisible by any positive integers except 1 and itself.

Primality Testing

Problem

Given a positive integer n, construct an algorithm to determine whether n is a prime.

Approach 1: because n is prime iff factor of n are only 1 and n, then we can divide n with all numbers between 2 to $n-1$. If the value of $n \bmod i$ for $i = 2, \ldots, n-1$ is not zero, then n is a prime.

Primality Testing

Problem

Given a positive integer n, construct an algorithm to determine whether n is a prime.

Approach 1: because n is prime iff factor of n are only 1 and n, then we can divide n with all numbers between 2 to $n-1$. If the value of $n \bmod i$ for $i = 2, \ldots, n-1$ is not zero, then n is a prime.

Primality Testing: First Algorithm

```
function IsPrime(n)                          // n ∈ ℤ⁺
    prime := True; i := 2
    if n = 1
        prime := False                       // 1 is not a prime number
    while (prime = True) and (i < n)
        if n mod i = 0                       // n is divisible by i
            prime := False
        else
            i := i + 1
    return(prime)
```

Prime Factor Composite Number

The previous primality testing algorithm is not efficient because in the **worst case** the number of iteration that we need to check whether n is a prime is $n - 1$ iteration. To speed up the primality testing algorithm, we will see some theorems.

Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer can be written in a unique way, as

1. a prime, or
2. a multiplication of two or more prime numbers that is written in ascending order.

The above theorem says that every positive integer certainly has prime factor.

Example

The prime factorization of 100, 641, 999, and 1024 are

1. $100 =$

Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer can be written in a unique way, as

1. a prime, or
2. a multiplication of two or more prime numbers that is written in ascending order.

The above theorem says that every positive integer certainly has prime factor.

Example

The prime factorization of 100, 641, 999, and 1024 are

1. $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$,
2. $641 =$

Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer can be written in a unique way, as

1. a prime, or
2. a multiplication of two or more prime numbers that is written in ascending order.

The above theorem says that every positive integer certainly has prime factor.

Example

The prime factorization of 100, 641, 999, and 1024 are

1. $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$,
2. $641 = 641$,
3. $999 =$

Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer can be written in a unique way, as

1. a prime, or
2. a multiplication of two or more prime numbers that is written in ascending order.

The above theorem says that every positive integer certainly has prime factor.

Example

The prime factorization of 100, 641, 999, and 1024 are

1. $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$,
2. $641 = 641$,
3. $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 37$,
4. $1024 =$

Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic)

Every positive integer can be written in a unique way, as

1. a prime, or
2. a multiplication of two or more prime numbers that is written in ascending order.

The above theorem says that every positive integer certainly has prime factor.

Example

The prime factorization of 100, 641, 999, and 1024 are

1. $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$,
2. $641 = 641$,
3. $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 37$,
4. $1024 = 2^{10}$.

Prime Factors of a Composite Number

Theorem

Suppose n is a composite number, then n has a prime factor which is less than or equal to $\lfloor \sqrt{n} \rfloor$.

Proof

The proof is one of the *challenging problems*.

As a consequence of the previous theorem, we can modify the previous algorithm to be more efficient as follows.

Primality Testing: Second Algorithm

```
function IsPrime(n)                                  // n ∈ ℤ⁺
    prime := True; i := 2
    if n = 1
        prime := False                               // 1 is not a prime number
    while (prime = True) and (i ≤ ⌊√n⌋)
        if n mod i = 0                               // n is divisible by i
            prime := False
        else
            i := i + 1
    return(prime)
```

As a consequence of the previous theorem, we can modify the previous algorithm to be more efficient as follows.

Primality Testing: Second Algorithm

function IsPrime(n) // $n \in \mathbb{Z}^+$

  $prime :=$ True; $i := 2$

  if $n = 1$

    $prime :=$ False // 1 is not a prime number

  while ($prime =$ True) **and** ($i \leq \lfloor \sqrt{n} \rfloor$)

    if $n \bmod i = 0$ // n is divisible by i

      $prime :=$ False

    else

      $i := i + 1$

  return($prime$)

In the worst case, the primality testing algorithm above at most needs $\lfloor \sqrt{n} \rfloor - 1$ iteration to check whether n is a prime.

Exercise

Check whether the following numbers are prime or composite, if the number is composite, write down their prime factorization.

1. 101
2. 7007

Solution: notice that:

Exercise

Check whether the following numbers are prime or composite, if the number is composite, write down their prime factorization.

1. 101
2. 7007

Solution: notice that:

1. Suppose 101 is a composite. Because $\lfloor \sqrt{101} \rfloor = 10$, then possible prime factors of 101 are

Exercise

Check whether the following numbers are prime or composite, if the number is composite, write down their prime factorization.

1. 101
2. 7007

Solution: notice that:

1. Suppose 101 is a composite. Because $\lfloor\sqrt{101}\rfloor = 10$, then possible prime factors of 101 are $2, 3, 5, 7$.

Exercise

Check whether the following numbers are prime or composite, if the number is composite, write down their prime factorization.

1. 101
2. 7007

Solution: notice that:

1. Suppose 101 is a composite. Because $\lfloor\sqrt{101}\rfloor = 10$, then possible prime factors of 101 are $2, 3, 5, 7$. However, because all of the four numbers are not divisors of 101, then 101 must be a prime.

Exercise

Check whether the following numbers are prime or composite, if the number is composite, write down their prime factorization.

1. 101
2. 7007

Solution: notice that:

1. Suppose 101 is a composite. Because $\lfloor\sqrt{101}\rfloor = 10$, then possible prime factors of 101 are $2, 3, 5, 7$. However, because all of the four numbers are not divisors of 101, then 101 must be a prime.
2. Suppose 7007 is a composite. Because $\lfloor\sqrt{7007}\rfloor = 83$, then possible prime factors of 7007 are no more than 83.

Exercise

Check whether the following numbers are prime or composite, if the number is composite, write down their prime factorization.

1. 101
2. 7007

Solution: notice that:

1. Suppose 101 is a composite. Because $\lfloor\sqrt{101}\rfloor = 10$, then possible prime factors of 101 are $2, 3, 5, 7$. However, because all of the four numbers are not divisors of 101, then 101 must be a prime.
2. Suppose 7007 is a composite. Because $\lfloor\sqrt{7007}\rfloor = 83$, then possible prime factors of 7007 are no more than 83. Furthermore, we have

$$\begin{aligned} 7007 &= 7 \cdot 1001 \\ 1001 &= 7 \cdot 143 \\ 143 &= 11 \cdot 13, \end{aligned}$$

therefore $7007 = 7^2 \cdot 11 \cdot 13$.

Challenging Problem

Challenging Problem

Develop a program in C, C++, Java, or Python with the following input and output:

1. input: two different positive integers a and b (a may be greater than b)
2. output: all prime numbers between a and b (inclusive, including a and b).

Example:

1. `input: 2, 13`
   `output: 2, 3, 5, 7, 11, 13`
2. `input: 101, 80`
   `output: 83, 89, 97, 101`

Contents

Which type are you?

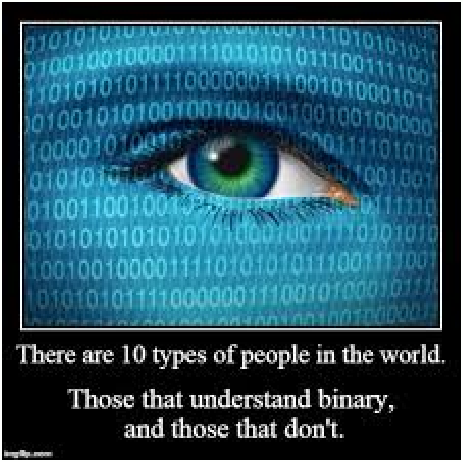

Image is taken from imgflip.com.

Integer Representation

In daily life, people almost certainly use base 10 number system for arithmetic operation. For example 965 can be written as $9 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0$. In computer science, we are required to convert numbers in base 10 to another base such as binary (base 2), octal (base 8), or hexadecimal (base 16).

Theorem

Suppose $b > 1$ is an integer. If n is a positive integer, then n can be expressed in a **unique** form of

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

where k is a nonnegative integer, $a_0, a_1, \ldots, a_k$ is a nonnegative number less than b, and $a_k \neq 0$.

- In the previous theorem, the expansion of n in base b is denoted as $(a_k a_{k-1} \ldots a_1 a_0)_b$. For example $(245)_8$ denotes the number $2 \cdot 8^2 + 4 \cdot 8 + 5 = 165$ in base 10.
- Generally, subscript 10 on number expansion in base 10 is not explicitly written because base 10 is already common as a representation of an integer.
- In hexadecimal numbers, the symbols used are: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \mathsf{A}, \mathsf{B}, \mathsf{C}, \mathsf{D}, \mathsf{E}, \mathsf{F}$. Here, A until F represents the number 10 until 15 in base 10.

Hexadecimal number systems can be seen on *blue screen of death* in Windows operating systems.

Exercise: Conversion to Decimal Systems

Exercise

Determine the number in base 10 that has binary, octal and hexadecimal representation as follows:

1. $(1\ 0101\ 1111)_2$
2. $(7016)_8$
3. $(2\text{AE}0\text{B})_{16}$

Solution: notice that:

1. $(1\ 0101\ 1111)_2 =$

Exercise: Conversion to Decimal Systems

Exercise

Determine the number in base 10 that has binary, octal and hexadecimal representation as follows:

1. $(1\ 0101\ 1111)_2$
2. $(7016)_8$
3. $(2\text{AE}0\text{B})_{16}$

Solution: notice that:

1. $(1\ 0101\ 1111)_2 =$
$1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = \mathbf{351}$.
2. $(7016)_8 =$

Exercise: Conversion to Decimal Systems

Exercise

Determine the number in base 10 that has binary, octal and hexadecimal representation as follows:

1. $(1\ 0101\ 1111)_2$
2. $(7016)_8$
3. $(2\mathsf{AE}0\mathsf{B})_{16}$

Solution: notice that:

1. $(1\ 0101\ 1111)_2 =$ $1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = \mathbf{351}$.
2. $(7016)_8 = 7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0 = \mathbf{3598}$.
3. $(2\mathsf{AE}0\mathsf{B})_{16} =$

Exercise: Conversion to Decimal Systems

Exercise

Determine the number in base 10 that has binary, octal and hexadecimal representation as follows:

1. $(1\ 0101\ 1111)_2$
2. $(7016)_8$
3. $(\mathsf{2AE0B})_{16}$

Solution: notice that:

1. $(1\ 0101\ 1111)_2 =$
$1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = \mathbf{351}$.
2. $(7016)_8 = 7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0 = \mathbf{3598}$.
3. $(\mathsf{2AE0B})_{16} = 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0 = \mathbf{175627}$.

Conversion from Decimal Systems

Given an integer n that will be converted into a number in base b, then conversion steps are explained as follows:

1. express n as $n = bq_0 + a_0$ with $0 \leq a_0 < b$, a_0 is the rightmost digit in the expansion of n in base b;
2. express q_0 as $q_0 = bq_1 + a_1$ with $0 \leq a_1 < b$, a_1 is the second rightmost digit in the expansion of n in base b;
3. do the following process iteratively until $q_r = 0$ for a $r \geq 0$: express q_{r-1} as $q_{r-1} = bq_r + a_r$ with $0 \leq a_r < b$, a_r is the $r + 1$ th digit from the right in the expansion of n in base b;
4. the result of this process is an expansion of n in base b with a_r is the leftmost digit and a_0 is the rightmost digit .

Examples

Octal representation (base 8) of 12345 can be obtained with the following steps

$$12345 \quad =$$

Examples

Octal representation (base 8) of 12345 can be obtained with the following steps

$$\begin{aligned} 12345 &= 8 \cdot 1543 + 1 \\ 1543 &= \end{aligned}$$

Examples

Octal representation (base 8) of 12345 can be obtained with the following steps

$$\begin{aligned} 12345 &= 8 \cdot 1543 + 1 \\ 1543 &= 8 \cdot 192 + 7 \\ 192 &= \end{aligned}$$

Examples

Octal representation (base 8) of 12345 can be obtained with the following steps

$$\begin{aligned} 12345 &= 8 \cdot 1543 + 1 \\ 1543 &= 8 \cdot 192 + 7 \\ 192 &= 8 \cdot 24 + 0 \\ 24 &= \end{aligned}$$

Examples

Octal representation (base 8) of 12345 can be obtained with the following steps

$$\begin{aligned} 12345 &= 8 \cdot 1543 + 1 \\ 1543 &= 8 \cdot 192 + 7 \\ 192 &= 8 \cdot 24 + 0 \\ 24 &= 8 \cdot 3 + 0 \\ 3 &= \end{aligned}$$

Examples

Octal representation (base 8) of 12345 can be obtained with the following steps

$$
\begin{aligned}
12345 &= 8 \cdot 1543 + 1 \\
1543 &= 8 \cdot 192 + 7 \\
192 &= 8 \cdot 24 + 0 \\
24 &= 8 \cdot 3 + 0 \\
3 &= 8 \cdot 0 + 3.
\end{aligned}
$$

Therefore, 12345 in base 8 is $(30071)_8$.

Hexadecimal representation (base 16) of 117130 can be obtained with the following steps:

$$177130 \quad =$$

Hexadecimal representation (base 16) of 117130 can be obtained with the following steps:

$$\begin{aligned} 177130 &= 16 \cdot 11070 + 10 \\ 11070 &= \end{aligned}$$

Hexadecimal representation (base 16) of 117130 can be obtained with the following steps:

$$\begin{aligned} 177130 &= 16 \cdot 11070 + 10 \\ 11070 &= 16 \cdot 691 + 14 \\ 691 &= \end{aligned}$$

Hexadecimal representation (base 16) of 117130 can be obtained with the following steps:

$$\begin{aligned} 177130 &= 16 \cdot 11070 + 10 \\ 11070 &= 16 \cdot 691 + 14 \\ 691 &= 16 \cdot 43 + 3 \\ 43 &= \end{aligned}$$

Hexadecimal representation (base 16) of 117130 can be obtained with the following steps:

$$\begin{aligned} 177130 &= 16 \cdot 11070 + 10 \\ 11070 &= 16 \cdot 691 + 14 \\ 691 &= 16 \cdot 43 + 3 \\ 43 &= 16 \cdot 2 + 11 \\ 2 &= \end{aligned}$$

Hexadecimal representation (base 16) of 117130 can be obtained with the following steps:

$$\begin{aligned}
177130 &= 16 \cdot 11070 + 10 \\
11070 &= 16 \cdot 691 + 14 \\
691 &= 16 \cdot 43 + 3 \\
43 &= 16 \cdot 2 + 11 \\
2 &= 16 \cdot 0 + 2.
\end{aligned}$$

Therefore, 117130 in base 16 is $(\text{2B3EA})_{16}$

Binary representation of 241 can be obtained with the following steps:

$$241 =$$

Binary representation of 241 can be obtained with the following steps:

$$\begin{aligned} 241 &= 2 \cdot 120 + 1 \\ 120 &= \end{aligned}$$

Binary representation of 241 can be obtained with the following steps:

$$\begin{aligned} 241 &= 2 \cdot 120 + 1 \\ 120 &= 2 \cdot 60 + 0 \\ 60 &= \end{aligned}$$

Binary representation of 241 can be obtained with the following steps:

$$\begin{aligned} 241 &= 2 \cdot 120 + 1 \\ 120 &= 2 \cdot 60 + 0 \\ 60 &= 2 \cdot 30 + 0 \\ 30 &= \end{aligned}$$

Binary representation of 241 can be obtained with the following steps:

$$\begin{aligned}
241 &= 2 \cdot 120 + 1 \\
120 &= 2 \cdot 60 + 0 \\
60 &= 2 \cdot 30 + 0 \\
30 &= 2 \cdot 15 + 0 \\
15 &=
\end{aligned}$$

Binary representation of 241 can be obtained with the following steps:

$$\begin{aligned}
241 &= 2 \cdot 120 + 1 \\
120 &= 2 \cdot 60 + 0 \\
60 &= 2 \cdot 30 + 0 \\
30 &= 2 \cdot 15 + 0 \\
15 &= 2 \cdot 7 + 1 \\
7 &=
\end{aligned}$$

Binary representation of 241 can be obtained with the following steps:

$$\begin{aligned}
241 &= 2 \cdot 120 + 1 \\
120 &= 2 \cdot 60 + 0 \\
60 &= 2 \cdot 30 + 0 \\
30 &= 2 \cdot 15 + 0 \\
15 &= 2 \cdot 7 + 1 \\
7 &= 2 \cdot 3 + 1 \\
3 &=
\end{aligned}$$

Binary representation of 241 can be obtained with the following steps:

$$\begin{aligned}
241 &= 2 \cdot 120 + 1 \\
120 &= 2 \cdot 60 + 0 \\
60 &= 2 \cdot 30 + 0 \\
30 &= 2 \cdot 15 + 0 \\
15 &= 2 \cdot 7 + 1 \\
7 &= 2 \cdot 3 + 1 \\
3 &= 2 \cdot 1 + 1 \\
1 &=
\end{aligned}$$

Binary representation of 241 can be obtained with the following steps:

$$\begin{aligned}
241 &= 2 \cdot 120 + 1 \\
120 &= 2 \cdot 60 + 0 \\
60 &= 2 \cdot 30 + 0 \\
30 &= 2 \cdot 15 + 0 \\
15 &= 2 \cdot 7 + 1 \\
7 &= 2 \cdot 3 + 1 \\
3 &= 2 \cdot 1 + 1 \\
1 &= 2 \cdot 0 + 1.
\end{aligned}$$

Therefore, 241 in binary base is $(1111\ 0001)_2$.

Conversion Algorithm from Decimals

Conversion algorithm of an integer $n > 0$ to base b can be written as follows.

Constructing Base b Expansion

procedure `Convert`(n, b) // converting n to base b

  $q := n$

  $k := 0$

  while $q \neq 0$

    $a_k := q \bmod b$

    $q := q \operatorname{div} b$

    $k := k + 1$

  return $(a_{k-1}, \ldots, a_1, a_0)$ // $(a_{k-1}, \ldots, a_1, a_0)_b$ is a representation of
// n in base b)

Conversion Table (0 – 15)

decimal	0	1	2	3	4	5	6	7
binary	0	1	10	11	100	101	110	111
octal	0	1	2	3	4	5	6	7
hexadecimal	0	1	2	3	4	5	6	7

decimal	8	9	10	11	12	13	14	15
binary	1000	1001	1010	1011	1100	1101	1110	1111
octal	10	11	12	13	14	15	16	17
hexadecimal	8	9	A	B	C	D	E	F