Number Theory

Blathnaid Sheridan

September 13, 2023

Integers

The integer (whole) numbers are: $1, 2, 3, 4, \ldots$ (positive integers) and also $-1. -2, -3,$ (negative integers).

When two or more integers are multiplied together you get a **product**. The numbers that multiply to give a product are called it's **factors**.
e.g. $2 \times 7 = 14$. The numbers 2 and 7 are factors and the number 14 is a product.
Every integer has at least two factors (namely 1 and itself). **Prime** numbers are integers whose only factors are 1 and itself.
e.g. The first few prime numbers are

$$2, 3, 5, 7, 11, 13, 17, 19, 23...$$

Factorising Integers

To factorise an integer means to write it as the product of prime factors (that is, factors that cannot be factorised any further). This factorisation is then unique.
Example:

$$231 = 3x7x11$$

$$200 = 2x2x3x5x5$$

Fundamental Theorem of Arithmetic
Every integer can be uniquely written as the product of prime factors.

The Greatest Common Divisor/Highest Common Factor (HCF/GCD)

If two integers have a factor in common then it is called a **common factor/divisor** of the numbers. The greatest/largest of all common divisors is called the **greatest common divisor - GCD** of the two integers.

Example

The number 24 has divisors $1, 2, 3, 4, 6, 8, 12, 24$.
The number 80 has divisors $1, 2, 4, 5, 8, 10, 16, 20, 40, 40$. The common divisors are $1, 2, 4, 8$ and the greatest of these is 8.
$\longrightarrow gcd(24, 80) = 8$

Exercise

The easiest way to find the GCD of two integers is to use *prime factorisation*.
Example: Find the

$$gcd(210, 720)$$

Solution: First find the common prime factors

$$210 = 2^1 \times 3^1 \times 5^1 \times 7^1$$

$$720 = 2^4 \times 3^2 \times 5^1 \times 7^0$$

To find the GCD we take the **smallest** power of each common prime factor:

$$GCD(210, 720) = 2^1 \times 3^1 \times 5^1 \times 7^0 = 30$$

Exercise

Find the $gcd(2100, 17640)$

The Lowest Common Multiple (LCM)

The lowest common multiple (LCM) of two integers is the smallest number which is divisible by both integers.

LCM(2,5)=10

LCM(6,10)=30

Exercise

The easiest way to find the LCM is to use prime factorisation.
Example: Find the

$$LCM(24, 36)$$

Solution: First find the common prime factors

$$24 = 2^3 \times 3^1$$

$$36 = 2^2 \times 3^2$$

To find the LCM we take the **biggest** power of each common prime factor:

$$LCM(24, 36) = 2^3 \times 3^2 = 72$$

Exercise

Find the LCM of 210 and 720.

Check your answers!

The product of any two integers is **equal** to the product of their GCD and their LCM.
Use the answers on the last two slides to verify this fact for 210 and 720.

$$\boxed{210 \times 720 = 151200}$$

$$\boxed{30 \times 5040 = 151200}$$

Algorithm for calculating the GCD

We have (unwittingly!) come up with a handy algorithm for finding the GCD of any two integers, a and b.

1. Find the prime factors of both integers.

$$a = p_1^{l_1} \times p_2^{l_2} \ldots p_n^{l_n}$$

$$b = p_1^{m_1} \times p_2^{m_2} \ldots p_n^{m_n}$$

   Some of the powers of the primes might be zero!

2. Then

$$GCD(a, b) = p_1^{k_1} \times p_2^{k_2} \ldots p^{k_n}$$

   where $k_i = min(l_i, m_i)$.

Euclidean Algorithm

The algorithm above is a nice way of calculating the GCD between two integers. However it is time consuming as it is necessary to find all the prime factors to begin with.
We will now look at a much more efficient method of calculating the GCD between any two integers (which does not involve prime factorisation), called Euclid's Algorithm.
The Euclidean Algorithm is a set of instructions for finding the greatest common divisor of any two positive integers.It's original importance was probably as a tool in construction and measurement.
The Euclidean Algorithm makes repeated use of the integer division idea that a small number (b) can be divided into a bigger number (a) and have a remainder (r).

$$a = q(b) + r$$

where q = quotient, which is how many times b divides into a exactly.

Theorem 1 - The Euclidean Algorithm

Given two integers $0 < b < a$, we make a repeated application of the division algorithm to obtain a series of division equations, which eventually terminate with a zero remainder.

$$a = bq_1 + r_1, 0 < r_1 < b,$$

$$b = r_1q_2 + r_2, 0 < r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3, 0 < r_3 < r_2,$$

$$\dots$$

$$r_{j-2} = r_{j-1}q_j + r_j, 0 < r_j < r_{j-1}$$

$$r_{j-1} = r_jq_{j+1}.$$

The greatest common divisor $gcd(a, b)$ of a and b is r_j, the last non-zero remainder in the division process.

Example

Find the $gcd(42823, 6409)$.

Solution

$$42823 = 6(6409) + 4369$$

$$6409 = 1(4369) + 2040$$

$$4369 = 2(2040) + 289$$

$$2040 = 7(289) + 17$$

$$289 = 17(17) + 0$$

Therefore $gcd(42823, 6409) = 17$

Exercise

Use the Euclidean Algorithm to find the GCD of

$$7469, 2464$$

Exercise

Use the Euclidean Algorithm to find the GCD of

$$2689, 4001$$

Exercise

Use the Euclidean Algorithm to find the GCD of

$$2947, 3997$$

Exercise

Use the Euclidean Algorithm to find the GCD of

$$1109, 4999$$

Theorem 2 - Multiplicative Inverse Algorithm/Extended Euclidean Algorithm

Given two integers $0 < b < a$, consider the Euclidean Algorithm equations which yield

$$r_1 = a - bq_1,$$

$$r_2 = b - r_1 q_2,$$

$$r_3 = r_1 - r_2 q_3,$$

$$\dots$$

$$r_{j-1} = r_{j-3} - r_{j-2} q_{j-1}$$

$$r_j = r_{j-2} - r_{j-1} q_j.$$

Then in the last of these equations $r_j = r_{j-2} - r_{j-1}q_j$ replace r_{j-1} with its expression in terms of r_{j-3} and r_{j-2} from the equation immediately above it. Continue this process successively, replacing r_{j-2}, r_{j-3} ... until you obtain the final equation

$$r_j = ax + by$$

with x and y integers.

Example

Find integers x and y to satisfy

$$42823x + 6409y = 17$$

Solution. We begin by solving our previous equations for the remainders. We have:
$4369 = 42823 - 6409(6)$
$2040 = 6409 - 4369$
$289 = 4369 - 2040(2)$
$17 = 2040 - 289(7)$
Now we do the substitutions starting with that last equation and working backwards and combining like terms along the way:
$17 = 2040 - 289(7) = 2040 - (4369 - 2040(2))(7) = 2040(15) - 4369(7)$
$17 = (6409 - 4369)(15) - 4369(7) = 6409(15) - 4369(22)$
$17 = 6409(15) - (42823 - 6409(6))(22) = 6409(147) - 42823(22)$

Exercise

Find integers x and y to satisfy

$$1819x + 3587y = d$$

where $d = gcd(1819, 3587)$.

Exercise

Find integers x and y to satisfy

$$50x + 71y = d$$

where $d = gcd(50, 71)$.

Exercise

Find integers x and y to satisfy

$$12345x + 543321y = d$$

where $d = gcd(12345, 54321)$.

We will return to this theorem at a later date as it will help us to find multiplicative inverses.

Modular Number Systems

In studying the integers we have seen that it is useful to write $a = bq + r$. Often we can solve problems by only considering the remainder. This throws away some of the information because there are only a finitely many remainders to consider. The study of the properties of the system of remainders is called *modular arithmetic*. It is an essential tool of Number Theory.

Definition of $\mathbb{Z}/\mathbb{Z}_n$

We will now give careful treatment of the system called the integers modulo or (mod n).
Let a and $b \in \mathbb{Z}$. We say that a *is congruent to* b *modulo* n written

$$a \equiv b(mod\ n)$$

if n divides into $(a - b)$.
So $\mathbb{Z}_n$ is the set of integers $= \{0, 1, 2, 3, 4, 5 \ldots (n-1)\}$.

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$

$$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

$$\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

Examples

1. $23 \equiv 3 (mod 10)$ because 10 divides into $23 - 3 = 20$.
2. $23 \equiv 7 (mod 8)$ because 8 divides into $23 - 7 = 16$.
3. $10000 \equiv 4 (mod 7)$ because 7 divides into $10000 - 4 = 9996$.

Since any two integers are congruent $mod 1$, we usually require $n \geq 2$ from now on.
In general, if $a = bq + r$ then $a \equiv r (mod\ b)$ since b divides $(a - r)$.
Furthermore, any multiple of a mod in that mod is 0. For example,

$$4(10)\ (mod\ 10) = 0$$

$$7(80)\ (mod\ 80) = 0$$

Addition mod n

We will now look at how to add mod n.
We will use arithmetic tables to help us visualise the process to begin with.
To add two integers mod n, you simply add the two integers as usual and *reduce* the answer down *mod n*.
Evaluate:

$$4 + 3(mod\ 5)$$

$$7(mod\ 5)$$

$$\equiv 2(mod\ 5)$$

$$\longrightarrow 4 + 3(mod\ 5) \equiv 2$$

Addition Tables mod n

1. Write out the addition tables for $\mathbb{Z}_5$.
2. Write out the addition tables for $\mathbb{Z}_7$.

Multiplication mod n

We will now look at how to multiply mod n.
We will use arithmetic tables to help us visualise the process to begin with.
To multiply two integers mod n, you simply multiply the two integers as usual and *reduce* the answer down *mod n*.
Evaluate:

$$4 \times 3 (mod\ 5)$$

$$12 (mod\ 5)$$

$$\equiv 2 (mod\ 5)$$

$$\longrightarrow 4 \times 3 (mod\ 5) \equiv 2$$

Multiplication Tables mod n

1. Write out the multiplication tables for $\mathbb{Z}_5$.
2. Write out the multiplication tables for $\mathbb{Z}_7$.

Examples

1. $5 + 8 \equiv 1 \ (mod 12)$
2. $5 \times 8 = 40 \equiv 4 \ (mod 12)$
3. $5+^3 = 255 \equiv 1 \times 5 = 5 \ (mod 12)$

Modular arithmetic is sometimes introduced using clocks. If we depart at 5 o'clock and our journey takes 8 hours, we arrive at 1 o'clock. Only the remainder mod 12 is used for time in hours.

Negative Numbers in mod n

To change a **negative** number into a positive number in mod n, you **add** the mod n to the negative number until you get a positive number.

Examples:

$$-29 \ (mod\ 32) \equiv 3 \ (mod\ 32)$$

$$-19 \ (mod\ 10) \equiv 1 \ (mod\ 10)$$

$$-102 \ (mod\ 12) \equiv 6 \ (mod\ 12)$$

Inverses in $\mathbb{Z}_n$

We have seen how to add and multiply mod n. We will now look investigate the existence of **inverses** mod n.

- The inverse of an integer is *another* integer that you can multiply it by to get 1 mod n. i.e.
  The inverse of a is x because

$$ax \equiv 1 \ (mod n)$$

  In this case, we call x the **inverse** of a and denote it by a^{-1}.

Examples

1. $3 \cdot 4 \equiv 1 \ (mod 11)$ so 4 is the inverse of 3 (mod 11) i.e. $3^{-1} = 4 \ (mod 11)$.
2. $5 \cdot 5 \equiv 1 \ (mod 12)$ so 5 is the inverse of 5 (mod 12) i.e. $5^{-1} = 5 \ (mod 12)$.
   Look back up at the multiplication table for $\mathbb{Z}_5$ to check this answer!
3. $5 \cdot 3 \equiv 1 \ (mod 7)$ so 3 is the inverse of 5 (mod 7) i.e. $5^{-1} = 3 \ (mod 7)$.
   Look back up at the multiplication table for $\mathbb{Z}_7$ to check this answer!

Fermat's Little Theorem (FLT)

This theorem is a method of finding the inverse of number in a **prime** mod p.
Let p be a prime. Suppose $a \in \mathbb{Z}$ is not divisible by p. Then

$$\boxed{a^{-1} \equiv a^{p-2} \ (mod \ p)}$$

This only works for **prime** mods.

Example - FLT

1. Use FLT to evaluate $5^{-1}\ (mod\ 7)$.
   Solution:
   In this example $a = 5$ and $p = 7$.

$$5^{-1} \equiv 5^{7-2}\ (mod\ 7)$$

$$5^{-1} \equiv 5^{5}\ (mod\ 7)$$

$$5^{-1} = 3125\ (mod\ 7)$$

$$5^{-1} \equiv 3\ (mod\ 7)$$

Check! $5 \cdot 3 = 15 \equiv 1\ (mod\ 7)$ ✓

Example - FLT

1. Use FLT to evaluate $6^{-1}\ (mod\ 11)$.
   Solution:
   In this example $a = 6$ and $p = 11$.

$$6^{-1} \equiv 6^{11-2}\ (mod\ 11)$$

$$6^{-1} \equiv 6^{9}\ (mod\ 11)$$

$$6^{-1} = 10077696\ (mod\ 11)$$

$$6^{-1} \equiv 2\ (mod\ 11)$$

Check! $6 \cdot 2 = 12 \equiv 1\ (mod\ 11)$ ✓

Which numbers have an inverse mod n?

A number a is invertible mod n if and only if $gcd(a, n) = 1$. In other words, if the number you want to find the inverse of has a gcd of 1 with the mod, then that number has an inverse in that mod.

Examples:

1. Which numbers have an inverse mod 3?
   Since $\mathbb{Z}_3$ or mod 3 contains $\{0,1,2\}$ and since $gcd(1, 3) = 1$ and $gcd(2, 3) = 1$, then both 1 and 2 have inverses mod 3.
2. Which numbers have an inverse mod 5?
   Since $\mathbb{Z}_5$ or mod 5 contains $\{0,1,2,3,4\}$ and since $gcd(1, 5) = 1$, $gcd(2, 5) = 1$, $gcd(3, 5) = 1$ and $gcd(4, 5) = 1$, then 1, 2, 3 and 4 have inverses mod 5.
   Note: All (non zero) integers in a **prime** mod will have an inverse.
   Use the multiplication tables above for $\mathbb{Z}_5$ and $\mathbb{Z}_7$ to verify this!

Con't

1. Which numbers have an inverse mod 12?

   Since $\mathbb{Z}_{12}$ or mod 12 contains $\{0,1,2,3,4,5,6,7,8,9,10,11\}$ and since

   $$gcd(1, 12) = 1,$$

   $$gcd(5, 12) = 1,$$

   $$gcd(7, 12) = 1,$$

   and

   $$gcd(11, 12) = 1$$

   then 1, 5, 7 and 11 have inverses mod 12. All the other integers in mod 12 have a factor in common with 12.

Finding the inverse of an integer mod n

To calculate a^{-1} mod n, we simply use the Euclidean algorithm and the inverse algorithm (Extended Euclidean algorithm) to get

$$ax + ny = 1$$

i.e.

$$x \equiv a^{-1} mod\ n$$

The value of y is irrelevant.

Example

Calculate

$$11^{-1} (mod\ 80).$$

I $\gcd(11, 80)$

$80 = 7(11) + 3$

$11 = 3(3) + 2$

$3 = 1(2) + 1$

$\hookrightarrow \gcd = 1$

$80 - 7(11) = 3$

$11 - 3(3) = 2$

$3 - 1(2) = 1$

II $11x + 80y = 1$

$1(3) - 1(2) = 1$

$1(3) - 1[11 - 3(3)] = 1$

$1(3) - 1(11) + 3(3) = 1$ $\rightarrow$ $4(3) - 1(11) = 1$

$4[80 - 7(11)] - 1(11) = 1$

$4(80) - 28(11) - 1(11) = 1$

~~$4(80)$~~ $- 29(11) = 1$

Con't

$4(80) - 29(11) = 1$

Mod 80 :

Any multiple of 80 $\pmod{80} = 0$

$0 - 29(11) = 1 \pmod{80}$

$\Rightarrow (-29)(11) = 1 \pmod{80}$

This means that -29 is the inverse of $11 \pmod{80}$

Remember that mod 80 $= \{0, 1, 2, \ldots 79\}$ so we need to change -29 to mod 80 $\Rightarrow -29 + 80 = 51$

$\Rightarrow$ The inverse of $11 = 51 \pmod{80}$

ie $11^{-1} = 51 \pmod{80}$

Exercises

Evaluate the following (using the Eulcidean algorithm and the Extended Euclidean algorithm)

1. 17^{-1} $(mod\ 64)$.
2. 23^{-1} $(mod\ 79)$.

Check your answers!

Relevance of Number Theory to Computing

One of the main areas of theoretical computer science where number theory is heavily used is in cyber security. The RSA algorithm, for example, is now the basis for security on the internet and involves many of the techniques we discussed above (Euclidean algorithm and modular arithmetic).

We will now look at two algorithms which develop a method for encoding and decoding messages. They are called:

1. Caeser's Cipher
2. Diffie-Hellman Key Exchange

Caeser's Cipher

This is earliest known example of a **substitution** cipher. It involves replacing every letter of a message with a different letter using a key and mod arithmetic.
Plaintext (P) is the text of the message before it is encoded.
Ciphertext (C) is the text of the message after it has been encoded.
To **encode** a message we use the following:

$$C = E(k, p) = (p + k)(mod\ 26)$$

where k is the key and p is a prime (both will be given).
To **decode** a message we use the following:

$$P = D(k, C) = (C - k)(mod\ 26)$$

where k is the key and C is the ciphertext position..

Example - Caeser's Cipher Encode

Use Caeser's Cipher with a key of $k = 3$ to encode the following message:
Plaintext: ARE YOU READY

Draw out the alphabet positions with plaintent (top) and ciphertext (bottom) and use **k=3** for the substitution.

Ciphertext: DUH BRX UHDGB

Example - Caeser's Cipher Decode

Use Caeser's Cipher with a key of $k = 5$ to decode the following message:
Ciphertext: YMNX NX KZS

Draw out the alphabet positions for ciphertext (top) and plaintext (bottom) and use **k=5** for the substitution.

Plaintext: THIS IS FUN

Exercises

1. Use Caeser's cipher with a key $k = 7$ to encode the message

   PLEASE SEND HELP.

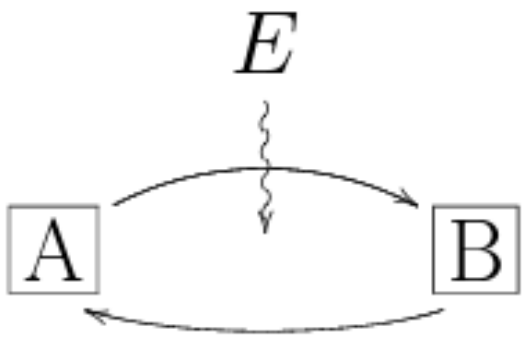
2. Use Caeser's cipher with a key $k = 10$ to decode the message

   GO KBO KGOCYWO.

Diffie-Hellman Key Exchange

Many encryption schemes assume that the users know a secret key (usually a number). Anyone possessing the key can decrypt messages.

How can Alice and Bob establish a secret key in the first place? Suppose they cannot meet in person. Phones can be tapped, emails read enroute etc.



Suppose an eavesdropper Eve can read every message that passes between A and B. It is still possible for A and B to set up a secret key, right under E's nose. The algorithm is based on the following observation:

- Given a and N, it is easy to calculate $a^N \ (mod \ n)$.
- Give $a^N \ (mod \ n)$ and a it is very hard to find N.

Diffie-Hellman Key Exchange Algorithm

1. A and B publically chose a large prime number p and base a.
2. A secretly chooses a number s, and sends $a^s \ (mod \ p)$ to B.
3. B secretly chooses a number t, and sends $a^t \ (mod \ p)$ to A.
4. A secretly calculates $k = (a^t)^s \ (modp)$. B secretly calculates $k = (a^s)^t \ (modp)$. Let k be the secret key.

A and B never reveal s, t or k to anyone else.
E can see a^s and $a^t \ (mod \ p)$ but cannot efficiently find s and t to she cannot find $k = a^{st}$.
(E can always find k given enough time. But if p is chosen large enough, say $p > 10^{100}$, then the running time is expected to be trillions of trillions of years, so they key is effectively safe).

Example - Diffie-Hellman Key Exchange

Suppose $a = 2$ and $p = 11$.
Suppose A choose $s = 4$.
Suppose B choose $t = 8$.
Calculate the secret key.

Solution

- A sends $2^4 \equiv 5 \ (mod\ 11)$ to B.
- B sends $2^8 \equiv 3 \ (mod\ 11)$ to A.
- A receives 3 from B and calculates $k = 3^s = 3^4 \equiv 4 \ (mod\ 11)$.
- B receives 5 from A and calculates $k = 5^t = 5^8 \equiv 4 \ (mod\ 11)$.
- The secret key for A and B is $k = 4$.