Number Theory

Introduction to number theory

- The theory of number is part of discrete mathematics and involving the integers and their properties.
- The concept of division of integers is fundamental to computer arithmetic.
- This chapter involves algorithms – used to solves many problems; searching a list, sorting finding the shortest path, find greatest common divisor, etc.

Divisibility

- Number theory is concerned with the properties of integers.
- One of the most important is *divisibility*.

Definition

ก็คือ $b \div a$ ลงตัวจะเขียนแทนด้วย $a|b$ หรือ $b=ak$

Let a and b be integers with $a \neq 0$. We say that a divides b if there is an integer k such that $b=ak$. This is denoted by $a|b$

Another way to express this is that a is a factor of b and b is a multiple of a

Examples

Determine whether they are divisible or not.

a) $3 \mid 15$ ✓

b) $-15 \mid 60$ ✓

c) $7 \mid 18$ ✗

Activity : Proof them !!

Basic Properties of Divisibility

i. if a|b and a|c then a|(b+c)

ii. if a|b then a|bc , for all integer c

iii. if a|b and b|c , then a|c

iv. n|n for every n.

v. if d|n and n|d, then d = ±n.

vi. if d|n and d|m, then d|(xm + yn) for all integers x and y.

Prime Numbers

เลขที่หารได้แค่ 1 และตัวมันเอง

Definition

A number $p>1$ that is divisible only by 1 and itself is called prime number

An integer $n>1$ that is not prime is call composite , which mean there exist some a such that $1<a<n$ and $a|n$

Examples

Determine each number is prime number or not.

a) 7 prime

b) 9 not prime

The first 1000 primes are listed below.

	2	3	5	7	11	13	17	19	23
29	31	37	41	43	47	53	59	61	67
71	73	79	83	89	97	101	103	107	109
113	127	131	137	139	149	151	157	163	167
173	179	181	191	193	197	199	211	223	227
229	233	239	241	251	257	263	269	271	277
281	283	293	307	311	313	317	331	337	347
349	353	359	367	373	379	383	389	397	401
409	419	421	431	433	439	443	449	457	461
463	467	479	487	491	499	503	509	521	523
541	547	557	563	569	571	577	587	593	599
601	607	613	617	619	631	641	643	647	653
659	661	673	677	683	691	701	709	719	727
733	739	743	751	757	761	769	773	787	797
809	811	821	823	827	829	839	853	857	859
863	877	881	883	887	907	911	919	929	937
941	947	953	967	971	977	983	991	997	

Factorization

Definition

Any integer a>1 is a product of primes uniquely, up to the order of primes. It can be factored in unique way as:

$$a = p_1^{x1} p_2^{x2} \dots p_t^{xt}$$

Where $p_1 < p_2 < \dots < p_t$ are prime numbers and xi > 0

Examples

Find prime factorizations of:

a) 91

b) 11011

c) last 4 digits of your student ID

Greatest Common Divisor (GCD)

ตัวหารร่วมมาก

Definition

The greatest common divisor of a and b is the largest positive integer dividing both a and b and is denote by either GCD(a,b). When GCD(a,b)=1 , we say a and b are relatively primes.

ตัวที่ หรม มีค่าเท่ากับ 1

Steps to find GCD.

- If you can factor a and b into primes, do so. For each prime number, look at the powers that it appears in the factorizations of a and b. Take the smaller of the two. Put these prime powers together to get the gcd. This is easiest understand by examples:

$$576 = 2^6 3^2$$

$$135 = 3^3 5$$

$$GCD(576,135)=3^2=9$$

Steps to find gcd.

- Gcd($2^5 3^4 7^2, 2^5 5^3 7, 2^2 7$)=$2^2 7$=28

  Note that if prime does not appear in factorization, then it cannot appear in the gcd.

- Suppose and are **large numbers**, so it might not be easy to factor them. The gcd can be calculated by a procedure known as the **Euclidean algorithm**. It goes back to what everyone learned in grade school: division with remainder.

The Euclidean Algorithm

- Suppose that a is greater than b . If not, switch

  a and b . The first step is divide the larger of the two integers by the smaller; let a is larger than b , hence represent a in the form

$$a = q_1 b + r_1$$

Where a is called the *dividend*, b is called the *divisor*, q_1 is called the *quotient*, and r_1 is called the *remainder*.

The Euclidean Algorithm

- If $r_1 \neq 0$ then continue by representing b in the form

$$b = q_2 r_1 + r_2$$

- Continue this way until the remainder that is zero.

- Let $r_0 = a$ and $r_1 = b$.
- The following sequence of steps:

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2 && 0 \le r_2 < r_1 \\
r_1 &= r_2 q_2 + r_3 && 0 \le r_3 < r_2 \\
&\vdots && \\
r_{k-2} &= r_{k-1} q_{k-1} + r_k && 0 \le r_k < r_{k-1} \\
r_{k-1} &= r_k q_k &&
\end{aligned}
$$

- Hence, the greatest common divisor is the last nonzero remainder in the sequence of divisions

$$\gcd(a, b) = r_k$$

The Extended Euclidean Algorithm

Example 1: $m = 65, n = 40$

Step 1: The (usual) Euclidean algorithm:

$$
\begin{aligned}
(1) \qquad 65 &= 1 \cdot 40 + \boxed{25} \\
(2) \qquad 40 &= 1 \cdot \boxed{25} + 15 \\
(3) \qquad \boxed{25} &= 1 \cdot 15 + 10 \\
(4) \qquad 15 &= 1 \cdot 10 + 5 \\
10 &= 2 \cdot 5
\end{aligned}
$$

Therefore: $\gcd(65, 40) = 5$.

- There are two important aspects to this algorithm:
  - ❖ It does not require factorization of the numbers.
  - ❖ It is fast.

Activity :

Compute : gcd(482,1180)

$1180 = 2(482) + 216$

$482 = 2(216) + 50$

$216 = 4(50) + 16$

$50 = 3(16) + 2$

$16 = 8 \times 2$

2 คือ ห.ร.ม.ของ 482, 1180

Modular Arithmetic

- Sometimes we care about the remainder of an integer when it is divided by some specified positive integer.

Definition

Let n be a fixes positive integer. For any integer a, a mod n is the remainder upon dividing a by n,

- Eg. 8 mod 3 = 2

Modular Arithmetic

- One of the most basic and useful in number theory is modular arithmetic, or known as **congruence.**

Definition

if a and b are integers and n is a positive integer, then a and b are said to be congruent modulo if (a mod n) = (b mod n). This is written

$$a \equiv b \pmod{n}$$

Activity :

a) Determine whether 32 is congruent to 7 modulo 5.

Property of Modulo Operator

- $a \equiv b \pmod{n}$ if $n|(a-b)$
- $(a \bmod n) = (b \bmod n)$ implies $a \equiv b \pmod{n}$
- $a \equiv b \pmod{n}$ implies $a \equiv b \pmod{n}$
- $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$ implies $a \equiv c \pmod{n}$

- To demonstrate the first point, if $n|(a-b)$ then $(a-b)=kn$ for some k. So we can write $a=b+kn$

Activity :

a) $23 \equiv 8 \pmod 5$

b) $-11 \equiv 5 \pmod 8$

Modular Arithmetic Operation

Proof !!

$$[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$$
$$[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$$
$$[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$$

Proof !!

Theorem :

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$: