CHAPTER THREE

NUMBER THEORY

INTRODUCTION

Number theory is principally the study of the natural numbers. However, the term is often extended to include the study of all the integers or all the rational numbers .

We will be covering the following topics

- divisibility and modular arithmetic
- Prime numbers, greatest common divisors (GCD) and Euclidean algorithm
- the Euler function
- Chinese remainder theorem

Divisibility

Definition :- If a and b are integers such that $a \neq 0$, then we say "a divides b" if there exists an integer k such that $b = ka$.

If a divides b, we also say "a is a factor of b" or "b is a multiple of a" and we write $a \mid b$. If a doesn't divide b, we write $a \nmid b$.

Example :- $3 \mid 12$ but $5 \nmid 12$

Exercise :- Let a and b be positive integers and $a > b$. How many positive integers not exceeding a are divisible by b?

cont.

* **Theorem 1:-** For all integer $a, b, c \in Z$
* a) If $a \mid b$ and $b \mid c$, then $a \mid c$

  b) If $a \mid b$ and $a \mid c$, then $a \mid sb + tc$ for all s and t

  c) For all $c \neq 0, a \mid b$ if and only if $ca \mid cb$

Application :

- Do there exist integers x, y, and z such that

$$6x + 9y + 15z = 107?$$

The answer is no

$$3 \mid 6x + 9y + 15z = 3 \mid 107$$ which is wrong.

division algorithm

* **The Division Algorithm** If a and b are integers such that $b > 0$, then there exist unique integers q and r such that $a = bq + r$ where $0 \leq r < b$.
- b is called the divisor
- a is called the dividend
- q is called the quotient; can be expressed $q = a \ \boldsymbol{div}\ b$
- r is called the remainder; can be expressed r $= a \ \boldsymbol{mod}\ b$

Example:-

If $a = 71$ and $b = 6$, then $71 = 6 \cdot 11 + 5$. Here $q = 11$ and $r = 5$.

If $a = -7$ and $b = 3$, then -7 $= -3 \cdot 3 + 2$. Here $q = -3$ and $r = 2$.

modular arithmetic

Definition :- if a and b are integers and m is a positive integer , then a is congruent to b modulo m if m divides $a - b$.

We use the notation

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

to indicate that a is congruent to b modulo m.

If a and b are not congruent modulo m, we write

$$a \not\equiv b(mod\ m)$$

Example :-

Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Solution :- $17 \equiv 5(mod\ 6)$

$24 \not\equiv 14(mod\ 6)$

cont.

Theorem :- let a and b be integers and let m be a positive integer. Then $a \equiv b (mod\ m)$ if and only if $a\ mod\ m = b\ mod\ m$

Theorem :- let m be a positive integer. The integer a and b are congruent modulo m if and only if there is an integer $a = b + km$

Proof:- $(\Rightarrow)$

if $a \equiv b (mod\ m)$

by definition

$$m|a - b$$

$a - b = km$ for some integer k

$(\Leftarrow)$ **Exercise**

Cont.

Theorem :- let m be a positive integer. If $a \equiv b (mod\ m)$ and c$\equiv d (mod\ m)$, then $a + c \equiv b + d (mod\ m)$ and $ac \equiv bd (mod\ m)$

proof :-

$a \equiv b (mod\ m)$ implies b $= a + sm$

c$\equiv d (mod\ m)$ implies d $= c + tm$

Hence

$$b + d = (a + sm) + (c + tm)$$
$$= a + c + m(s + t)$$
$$\therefore a + c \equiv b + d (mod\ m)$$

And

$$bd = (a + sm)(c + tm)$$
$$= ac + m(at + cs + stm)$$
$$\therefore ac \equiv bd (mod\ m)$$

cont.

Example:-

$7 \equiv 2(mod5)$ and $11 \equiv 1(mod5)$, it follows from the above

$$18 = 7 + 11 \equiv 2 + 1 = 3(mod\ 5)$$

and

$$77 = 7.11 \equiv 2.1 = 2(mod\ 5)$$

Corollary :- let m be a positive integer and let a and b be integers. Then,

$$(a + b)\ mod\ m = \big((a\ mod\ m) + (b\ mod\ m)\big) mod\ m$$

$$(ab)\ mod\ m = \big((a\ mod\ m)(b\ mod\ m)\big) mod\ m$$

Prime numbers

Definition:- suppose that $a \in N$ and $a > 1$. then we say that a is prime if it has exactly two positive divisors, namely 1 and a.

We say that a is composite if it is not prime

Remark :- the integer n is composite if and only if there exist an integer a such that $a|n$ and $1 < a < n$

Example :- 7 is prime

9 is composite

Theorem :- (the fundamental theorem of arithmetic)

Every integer greater than 1 can be written uniquely as a prime or as a product of two or more primes where the prime factors are written in order of non decreasing size.

Cont.

Example :-

$$100 = 2.2.5.5 = 2^2 5^2$$

$$641 = 641$$

$$1024 = 2.2.2.2.2.2.2.2.2.2 = 2^{10}$$

Theorem :- if n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$

Example :- show that 101 is prime

Solution :-

the only primes not exceeding $\sqrt{101}$ are $2,3,5$ and 7

Here because 101 is not divisible by $2,3,5$ or 7

It follows that 101 is prime.

Infinitude of primes

Euclid of Alexandria was a Greek mathematician who lived several centuries before the common era.

Euclid proved that if we take any finite set of prime numbers, we can always find another prime number that is not in that set.

Theorem :- there are infinitely many prime numbers

Proof :- Assume that there are finite number of primes

That is $p_1, p_2, \ldots\ p_n$

Consider the number

$$q = p_1 p_2 \ldots\ p_n + 1$$

This number is not divisible by any of the listed primes

If we divided p_i into q there would result a remainder of 1

We must conclude that q is a prime number, not among the primes listed above

This contradict our assumption that all primes are in the list $p_1, p_2, \ldots\ p_n$

GCD and the Euclidean algorithm

Definition :- Let a and b be non-negative integers, not both zero. The greatest common divisor of a and b denoted by $\gcd(a, b)$ is the largest natural number m such that m | a and m | b.

If a and b are both non-zero, the least common multiple of a and b denoted by $\mathrm{lcm}(a, b)$ is the smallest natural number m such that a | m and b | m.

Two natural numbers a and b are coprime (or relatively prime) if their greatest common divisor is 1.

Example :- the integers 17 and 22 are relatively prime

$$\gcd(17,22) = 1$$

Definition :- the integers $a_1, a_2, \ldots . a_n$ are pairwise relatively prime if $\gcd(a_1, a_j) = 1$ whenever $1 \leq i < j \leq n$.

cont.

Suppose that the prime factorization of the positive integer a and b are

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

Where each exponent is a nonnegative integer and all primes occurring in the prime factorization of either a or b are included in both factorization.

Then $\gcd(a, b)$ is given by

$$\gcd(a, b) = p_1^{\min(a_1 b_1)} p_2^{\min(a_2 b_2)} \dots p_n^{\min(a_n b_n)}$$

Example :- $\gcd(120,500) = 2^2 3^0 5^1$

$$= 20$$

cont.

And the least common multiple of a and b is given by

$$\text{lcm}(a,b) = p_1^{max(a_1 b_1)} p_2^{max(a_2 b_2)} \dots p_n^{max(a_n b_n)}$$

Example :- $lcm(95256,432) = 2^4 3^5 7^2$

$= 190512$

Theorem :- let a and b be positive integers. Then

$$ab = \text{gcd}(a,b) * lcm(a,b)$$

The Euclidean algorithm

Theorem :- let $a = bq + r$, where $a, b, q,$ and r are integers. Then $\gcd(a, b) = \gcd(b, r)$

Example :- find the greatest common divisor of 414 and 662 using the Euclidean algorithm

Solution :- successive uses of the division algorithm give

$$662 = 414.1 + 248$$
$$414 = 248.1 + 166$$
$$248 = 166.1 + 82$$
$$166 = 82.2 + 2$$
$$82 = 2.41$$

Hence, $gcd(414,662) = 2$, because 2 is the last nonzero remainder

Linear congruence

A congruence of the form

$$ax \equiv b(mod\ m)$$

Where m is positive integer , a and b are integers and x is variable is called a linear congruence

Theorem :- let m be a positive integer and let a be a non zero integer, the congruence $ax \equiv b(mod\ m)$ has a solution if and only if $d = (a, m)$ is a divisor of b.

If $d|b$ then there are exactly d solution $mod\ m$

Remark:- Notice that if $d = (a, m) = 1$, then there is a unique solution modulo m for the equation $ax \equiv b(mod\ m)$.

This will allow us to talk about modular inverses

Modular inverses

Definition :- we say that integers a and b are multiplicative inverses modulo m if

$$ab \equiv 1(mod\ m)$$

Theorem :- the integer a has an inverse modulo m if and only if

$$(a, m) = 1$$

Example :- find the inverse of $5\ mod\ 7$

Solution :- $1 \equiv 8 \equiv 15(mod\ 7)$

Here $15 = 5 * 3$

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

Example :- find the inverse of $5\ mod\ 11$

Solution :- $1 \equiv 12 \equiv 23 \equiv 34 \equiv 45(mod\ 11)$

Here $45 = 5 * 9$

Therefore $5^{-1} \equiv 9(mod\ 11)$

cont.

Example :- solve $6x \equiv 9(mod\ 27)$

$$\Rightarrow 2x \equiv 3(mod\ 9)$$
$$\Rightarrow 10x \equiv 15(mod\ 9)$$
$$\Rightarrow x \equiv 6(mod\ 9)$$
$$\Rightarrow x \equiv 6,15,24\ (mod\ 27)$$

Example :- solve $15x \equiv 25(mod\ 80)$

$$\Rightarrow 3x \equiv 5(mod\ 16)$$
$$\Rightarrow 33x \equiv 55(mod\ 16)$$
$$\Rightarrow x \equiv 7(mod\ 16)$$
$$\Rightarrow x \equiv 7,23,39,55,77\ (mod\ 80)$$

Example 3:- solve $2x \equiv 7\ (mod\ 8)$

no solution

The Euler function

Definition :- totative of a positive integer n is an integer k $(0 < k \leq n)$ such that n and k are primes

Example :- $n = 8$, then $k = 3$ can be a totative

$n = 12$, then $k = 5$ can be a totative

Definition :- Euler totient function (φ) is a function that count the number of positive integers up to a given integer that are coprimes.

Example :- $1, \varphi(8) = 4$

$2, \varphi(13) = 12$

Note :- for a prime number p, $\varphi(p) = p - 1$

That is , $\varphi(11) = 10$

$\varphi(17) = 16$

Cont.

But for composite numbers

$$c = p_1 * p_2 * \cdots$$

$$\varphi(c) = c\left(1 - {}^{1}/_{p_1}\right) * \left(1 - {}^{1}/_{p_2}\right) * \cdots$$

Example :-

$$\varphi(12) = 12\left(1 - {}^{1}/_{2}\right) * \left(1 - {}^{1}/_{3}\right) = 4$$

$$\varphi(14) = 14\left(1 - {}^{1}/_{2}\right) * \left(1 - {}^{1}/_{7}\right) = 6$$

- for two prime numbers p and q

$$\varphi(pq) = \varphi(p) * \varphi(q)$$

Example :- $\varphi(11 * 13) = \varphi(11) * \varphi(13)$

- if p is prime and $k > 0$

$$\varphi\left(p^k\right) = p^k - p^{k-1}$$

cont.

Theorem:- Euler's Theorem If m is a positive integer and a is an integer such that $(a, m) = 1$, then $a^{\varphi(m)} \equiv 1(mod\ m)$

Example:-

$$3^4 = 81 \equiv 1(mod\ 5)$$
$$2^{\varphi(9)} = 2^6 = 64 \equiv 1(mod\ 9)$$

Theorem:- (Fermat's little theorem)

If p is prime and a is an integer not divisible by p then

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

Furthermore, for every integer a we have

$$a^p \equiv a(mod\ p)$$

Example :- find $7^{222}\ mod\ 11$

Solution:-

By Fermat's theorem we know that $7^{10} \equiv 1(mod\ 11)$

Cont.

So

$$(7^{10})^k \equiv 1(mod\ 11)$$

for every positive integer k

$$7^{222} = 7^{22.10+2} = (7^{10})^{22}7^2 \equiv 1^{22}.49 \equiv 5(mod\ 11)$$

It follows that

$$7^{222}\ mod\ 11 = 5$$

The Chinese remainder theorem

Theorem : (The Chinese remainder theorem)

Let $m_1, m_2, \dots m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \dots a_n$ arbitrary integers then the system

$$x \equiv a_1 (mod\ m_1)$$
$$x \equiv a_2 (mod\ m_2)$$
$$\vdots$$
$$x \equiv a_n (mod\ m_n)$$

Has a unique solution modulo $m = m_1 m_2 \dots m_n$.

Moreover

$$x \equiv a_1 M_1 Y_1 + a_2 M_2 Y_2 + \cdots + a_K M_K Y_K (mod\ m)$$

Where

$$M_i = \frac{m}{m_i} \text{ and } M_i Y_i \equiv 1 (mod\ m_i) for\ i = 1,2, \dots n$$

Cont.

Example :- solve

$$x \equiv 2\ (mod\ 3)$$
$$x \equiv 3\ (mod\ 5)$$
$$x \equiv 2\ (mod\ 7)$$

Solution :-

$$m = 3.5.7 = 105$$

$$M_1 = \frac{105}{3} = 35$$
$$M_2 = \frac{105}{5} = 21$$
$$M_3 = \frac{105}{7} = 15$$

And

$$Y_1 = 2$$
$$Y_2 = 1$$
$$Y_3 = 1$$

cont.

Then

$$x \equiv a_1 M_1 Y_1 + a_2 M_2 Y_2 + \cdots + a_3 M_3 Y_3 (mod\ 105)$$
$$\equiv 2.35.1 + 3.21.1 + 2.15.1 (mod\ 105)$$
$$\equiv 104 + 63 + 30\ (mod\ 105)$$
$$\equiv 233 (mod\ 105)$$
$$= 23$$

Example 2:- solve

$$x \equiv 1\ (mod\ 5)$$
$$x \equiv 2\ (mod\ 6)$$
$$x \equiv 3\ (mod\ 7)$$

THE END