Number Theory

By : D. Zaynab Anwer Ahmed

Contents

References:

1. Elementary Number theory by David Burton
2. An Introductory Course in Elementary Number Theory by Wissam Raji
3. 104 number theory problem
4. مقدمة في نظرية الاعداد (فالح الدوسري)
5. Cryptography and Network Security, seventh Edition. By William Stallings. Publisher: Prentice Hall. 2017.

1. Introduction

First, what is number theory? At the most basic level, it's the study of the properties of the integers Z = {. . . , −2, −1, 0, 1, 2, . . . } or the natural numbers N = {0, 1, 2, . . . }. A few reasons to study number theory:

In some ways the most basic piece of mathematics, for you can build everything else from natural numbers.

$$N \longrightarrow Z \longrightarrow Q \longrightarrow R \longrightarrow C$$

From there you can get to calculus, topology, etc.

(Mathematics is the queen of sciences and number theory is the queen of mathematics) Carl Friedrich Gauss (1777-1855).

–Number theory uses techniques from algebra, analysis, geometry and topology, logic and computer science, and often drives development in these fields.

2. Mathematical Methods

1. Induction Method
2. Contrary Method
3. Analytic Method

(2.1) Induction Method:

Principle of Induction: Any mathematical statement is true for all n≥ 1 if:

1) It is true for integer n=1 and 2) it is true for n≤k for some k
   then it is true for all n=k +1

In another wards :In order to show that $\forall n$, the statement P(n) is true, it suffices to establish the following two properties:

(1) Base case: Show that P(1) is true.

(2) Induction step: Assume that P(k) is true (the Induction Hypothesis (IH)), and show that P(k+1) also true for all positive integer k.

Example:

Use mathematical induction to prove:

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

Solution:

1) P_1 : since $1 = \frac{1(1+1)}{2}$ then P_1 is true.

2) Assume that P_k is true for some integer k ≥ 1; that is (IH) is:

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2} \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

We need to show that P_{k+1} also true for all positive integer k

We need to prove $P_{k+1}: 1 + 2 + 3 + \cdots + k + k + 1 = \frac{(k+1)(k+1+1)}{2}$

Start with the left side by using eq(1) $1 + 2 + 3 + \cdots + k + k + 1 = \frac{k(k+1)}{2} + k + 1$

$= \frac{k(k+1)+2(k+1)}{2}$

$= \frac{(k+1)(k+2)}{2}$= right side

Example: Use mathematical induction to prove:

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

Solution:

1) P_1 : since $1 = 1^2$ then P_1 is true.

2) Assume that P_k is true for some integer k ≥ 1; that is (IH) is:

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2 \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

We need to show that P_{k+1} also true for all positive integer k

We need to prove $P_{k+1}: 1 + 3 + 5 + \cdots + [2(k+1) - 1] = (k+1)^2$

or since 2(k+1) -1 = 2k+2 -1 = 2k+1, an equvalient statement would be:

$$P_{k+1}: 1 + 3 + \ldots + (2k+1) = (k+1)^2$$

Start with the left side by using eq(1)

$$1 + 3 + 5 + \ldots + (2k-1) + (2k+1) = k^2 + (2k+1)$$

$= (k+1)^2$ = right side

Example: Use mathematical induction to prove:

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^n}=\frac{2^n-1}{2^n}$$

Solution:

1) P_1 : since $\frac{1}{2^1}=\frac{2^1-1}{2^1}$ then P_1 is true.

2) Assume that P_k is true for some integer k ≥ 1; that is (IH) is:

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^k}=\frac{2^k-1}{2^k} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

We need to show that P_{k+1} also true for all positive integer k

We need to prove $P_{k+1}: \frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^k}+\frac{1}{2^{(k+1)}}=\frac{2^{k+1}-1}{2^{k+1}}$

Start with the left side by using eq(1)

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^k}+\frac{1}{2^{(k+1)}}=\frac{2^k-1}{2^k}+\frac{1}{2^{(k+1)}}=\frac{2(2^k-1)+1}{2^{(k+1)}}$$

$$=\frac{(2^{k+1}-2)+1}{2^{(k+1)}}$$

$=\frac{2^{k+1}-1}{2^{(k+1)}}$= right side

Example: Use mathematical induction to prove:

$$n<2^n$$

Solution:

1) P_1 : since $1<2^1$ then P_1 is true.

2) Assume that P_k is true for some integer k ≥ 1; that is (IH) is:

$$k<2^k \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

We need to show that P_{k+1} also true for all positive integer k

We need to prove: $P_{k+1}: k+1<2^{k+1}$

By using eq(1) we get: $k<2^k$ ➔ $2k<2*2^k$ ➔ $k+k<2^{k+1}$

Since k ≥1 then k+1 ≤ $k+k$ then $k+1<2^{k+1}$

Hence the proof was completed

(2.2) Contrary Method

Example:

The number $\sqrt{2}$ is irrational.

Proof:

Suppose, to the contrary, that $\sqrt{2}$ is a rational number, say, $\sqrt{2} = \frac{a}{b}$, where *a*and *b* *are* both integers with gcd(a, *b)*= 1. Squaring, we get $a^2 = 2b^2$, so that $2|a^2$. ➔ 2|a

a=2c➔ $4c^2 = 2b^2$➔ 2|b and hence contradiction

Remark:

Odd integer are of the form 2n-1, 2n+1, 4n+1, 6n+1

Even integer: 2n, 4n,6n,…

H.W: Use Mathematical induction to prove the following statement:

1) $1*2+2*3+\cdots+n(n+1)=\frac{n(n+1)(n+2)}{3}$

2) 3 divides n^3+2n

3) $2+4+6+\cdots+2n = n(n+1)$

4) $1+5+9+\cdots+(4n-3) = n(2n-1)$

5) $2+4+8+\cdots+2^n = 2(2^n-1)$

6) $3+3^2+3^3+\cdots+3^n = \frac{3(3^n-1)}{2}$

7) $\sum_{s=1}^{n} s^3 = \frac{n^2(n+1)^2}{4}$

8) $\sum_{s=1}^{n}(5s-3) = \frac{n(5n-1)}{2}$

9) $\sum_{k=1}^{n} k\,k! = (n+1)!-1$

10) let m, n are positive integer and m>1 then $n < m^n$

3. Divisibility and the Division Algorithm of Integers:

(3.1) Divisibility

An integer **a** is said to be *divisible* by another integer b ≠0, if there is a third integer c such that $a = bc$.

If a and *b* are positive, c is necessarily positive.

We express the fact that **a** is divisible by **b**, or **b** divides **a**, by b |a. and use b ł a express b dose not divide a.

Example:

3|12 since 12=3*4 but 3 ł4 , -3|3

Theorem 2.1

For integers a, *b,* c, the following hold:

(a) $a \mid 0, 1 \mid a, a \mid a.$
(b) $a \mid 1$ if and only if $a = \pm 1.$
(c) If $a \mid b$ and $c \mid d$, then $ac \mid bd.$
(d) If $a \mid b$ and $b \mid c$, then $a \mid c.$
(e) $a \mid b$ and $b \mid a$ if and only if $a = \pm b.$
(f) If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|.$
(g) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for arbitrary integers x and $y.$

Proof*:*

a, b, c. d, e (H.W)

(f) : If $a \mid b$, then there exists an integer c such that $b = ac$; since $b \neq 0$ then $c \neq 0$.

Upon taking absolute values, we get $|b| = |ac| = |a||c|$. Because $c \neq 0$, so that $|c| \geq 1$, and hence $|b| = |a||c| \geq |a|$.

(g): the relations $a \mid b$ and $a \mid c$ gives that there exist two integer r and s such that $b = ar$ and $c = as$. Now for any x and y, *we have:*

$bx + cy = arx + asy = a(rx + sy)$

since $rx + sy$ is an integer, this meen that $a \mid (bx + cy)$.

Remark:

The property (g) of the above theorem can be extending by induction to sums of more than two terms. That is, if $a \mid b_k$ for k = 1, 2, ... , n, then

$$a \mid (b_1x_1 + b_2x_2 + \cdots + b_nx_n)$$

for all integers $x_1, x_2, \ldots, x_n$.

(3.2) THE DIVISION ALGORITHM

Given integers *a* and *b,* with $b > 0$, there exist unique integers q and r satisfying

$$a = qb + r \qquad 0 \le r < b$$

The integers q and r are called the quotient and remainder respectively, in the division *of a by b.* $q = \left\lfloor \frac{a}{b} \right\rfloor$

Examples:

1) Let a=13 and b=6 then there exist a unique integer q and r such that: 13=6q+r ➔ q=2 and r=1 i.e. 13=6*2+1
2) If 3|6 ➔ 6=3*2+0, q=2, r=0
3) If 4|15 ➔ 15=4*3+3 , q=3 , r=1

Example:

Show that the expression $a(a^2 + 2)/3$ is an integer for all a ≥ 1.

Sol: According to the Division Algorithm, of the integers a and 3 we have: there exist a unique integers q and r satisfying

$$a = 3q + r \qquad 0 \le r < 3$$

That is mean a= 3q, 3q + 1, or 3q + 2. Assume the first of these cases. Then

$$a(a^2 + 2)/3 = q(9q2 + 2)$$

which clearly is an integer. Similarly, if $a = 3q + 1$, then

$$\frac{(3q + 1)((3q + 1)^2 + 2)}{3} = (3q + 1)(3q^2 + 2q + 1)$$

and $a(a^2 + 2)/3$ is an integer in this instance also. Finally, for $a = 3q + 2$, we obtain

$$\frac{(3q + 2)((3q + 2)^2 + 2)}{3} = (3q + 2)(3q^2 + 4q + 2)$$

Also an integer. Then it is integer in all cases.

H.W:

1) Prove by using **Division Algorithm** that any integer either even or odd but never both.

2) Use the division algorithm to find the quotient and the remainder when 76 is divided by 13.

3) Show that if m is an integer then 3 divides $m^3 - m$.

4) Use the division algorithm to find the quotient and the remainder when 2220 is divided by 77.

5) If d|a and d|(a+b) then d|b

4. The Greatest Common Divisor

Definition

Let a and b be given integers, with at least one of them different from zero. The *greatest common divisor* of *a* and *b*, denoted by gcd(a, *b),* is the positive integer *d* satisfying the following:

(a) d>0

(b) d | a and d | *b.*

(c) If c|a and c|b, then c|d or c≤d .

Example :

$$\gcd(-5, 5) = 5 \qquad \gcd(8, 17) = 1 \qquad \gcd(-8, -36) = 4$$

Def:

A *linear combination* of *a* and *b,* mean an expression of the form *ax +by,* where *x* and y are integers.

Theorem 4.1

Given integers a and b, not both of which are zero, there exist integers x and y such that gcd(a, *b)= ax+ by.*

Example

gcd(-12, 30) = 6 = (-12)2 + 30 * 1

gcd(-8, -36) = 4 = (-8)4 + (-36)(-1)

Definition

Two integers a and b are relatively prime if gcd(a,b) = 1.

Example
The greatest common divisor of 9 and 16 is 1, thus they are relatively prime.

Theorem 4.2
Let *a* and *b* be integers, not both zero. Then *a* and *b* are relatively prime if and only if there exist integers *x* and *y* such that *ax + by=1*

Proof
If *a* and b are relatively prime so that gcd(a, *b)*= 1, then by Theorem 4.1 there exist integers *x* and *y* satisfying 1 = *ax + by.*

To prove the converse, if there exist integers *x* and *y* such that *ax + by.=1 we need to prove* gcd(a, *b)=1. Suppose* that d = gcd(a, *b).* Because *d*|*a* and *d* |*b, then by (*Theorem 1, part (g)) we have *d* |*(ax+ by,* ➔ *d* |1. Since *d is* a positive integer, ➔ *d* =1 (part (b) of Theorem 1) ➔ gcd(a,b)=1.

Example:
Let us observe that gcd(-12, 30) = 6 and gcd(-12/6, 30/6) = gcd(-2, 5) = 1

Corollary
If gcd(a, b)= d, then gcd(a/d, b/d)= 1.

Corollary
If *a*| *c* and *b* | c, with gcd(a, *b)*= 1, then *ab* | c.

Theorem 4.3 (Euclid's lemma.)
If *a* | bc , with gcd(a, *b)*= 1, then *a* | *c.*

Proof
We start again from Theorem 4.2, writing 1 =*ax+ by,* where *x* and *y* are integers. Multiplication of this equation by *c* produces

c = 1 · c =(ax + by)c = acx +bcy

Because *a* | *ac* and *a* | *bc,* it follows that *a* | *(acx +bcy),* then *a* | *c.*

Remark:
If *a* and *b* are not relatively prime, then Euclid's lemma may fail to hold. Here is a specific example: 12|9 * 8, but 12 ∤ 9 and 12 ∤8.

Theorem 5:
Let *a, b* be integers, not both zero. For a positive integer *d, d* = gcd(a, *b)* if and only if

(a) $d \mid a$ and $d \mid b$.

(b) Whenever c|a and $c \mid b$, then $c \mid d$.

Proof

To begin, suppose that $d = \gcd(a, b)$.

Certainly, $d \mid a$ and $d \mid b$, so that (a) holds.

In light of Theorem 4.1, d can be written as $d = ax + by$ for some integers x, y. Thus, if $c \mid a$ and $c \mid b$, then $c \mid (ax + by)$, ➔ $c \mid d$. *i.e* (b) holds.

Conversely, let d be any positive integer satisfying the stated conditions. Given any common divisor c of a and b, we have $c \mid d$ from hypothesis (b). This mean s that $d \geq c$, and hnce d is the greatest common divisor of a and b.

H.W.

1) Prove or disprove: If $a \mid (b + c)$, then either $a \mid b$ *or* $a \mid c$.

2) For $n \geq 1$, use mathematical induction to establish each of the following divisibility statements:

$8 \mid 5^{2n} + 7$. [Hint: $5^{2(k+l)} + 7 = 5^2(5^{2k} + 7) + (7 - 5^2 * 7)$]

3) Prove that for any integer a, one of the integers a, $a + 2$, $a + 4$ is divisible by 3

4) Establish that the difference of two consecutive cubes is never divisible by 2.

5) For a nonzero integer a, show that gcd(a, 0) =|a| gcd(a, a)= |a|, and gcd(a, 1) =1

6) Prove that, for a positive integer n and any integer a, gcd(a, a+ n) divides n; hence, gcd(a, a+ 1) = 1.

7) Given integers a and b, prove the following:

(a) There exist integers x and y for which c = ax +by if and only if gcd(a , b) | c.

(b) If there exist integers x and y for which ax+ by= gcd(a, b), then gcd(x, y) = 1.

8) If gcd(a, b) = 1, and c|a, then gcd(b, c)= 1.

9) If a | bc, show that a | gcd(a, b) gcd(a, c).

5. THE EUCLIDEAN ALGORITHM

The greatest common divisor of two integers is difficult for large numbers. Therefore the following method has been introduce in (300 BC). This method depends on division algorithm and the following lemma.

Lemma 5.1

If $a = qb + r$, then gcd(a, *b)*= gcd(b, *r)*.

Euclid's algorithm: is an efficient method for computing the greatest common divisor (GCD) of two integers as follows:

Because gcd(|*a* |, | *b* |) = gcd(a , *b), therefor we can a*ssume that $a \geq b > 0$. The first step is to apply the Division Algorithm to *a* and *b* to get

$$a = q_1 b + r_1 \qquad 0 \leq r_1 < b$$

If $r_1 = 0$, then $b \mid a$ and gcd(a, *b)* = *b*. When $r_1 \neq 0$, divide *b* by r_1 to produce integers q_2 and r_2 satisfying

$$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1$$

If $r_2 = 0$, then we stop; otherwise, proceed as before to obtain

$$r_1 = q_3 r_2 + r_3 \qquad 0 \leq r_3 < r_2$$

This division process continues until some zero remainder appears,

We have that r_n, the last nonzero remainder that appears in this manner, is equal to gcd(a , *b)*.

Example:

Find gcd(12378, 3054) and represent it as a linear compensation of them.

Sol:

By using division algorithm on 12378 & 3054

First we find the lower integer of the long division $\left\lfloor \frac{12378}{3054} \right\rfloor$ we have:

12378 = 4* 3054 + 162

Repeat on 3054 & 162 and continue

3054 = 18 *162 + 138

162 = 1 * 138 + 24

138 = 5* 24 + 18

24 = 1* 18 + 6

18 = 3*6+0

Then the integer 6, is the greatest common divisor of 12378 and 3054:

6 = gcd(12378, 3054)

Another way by table:

Find the gcd(1760, 2740)

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

6. Extended Euclidean algorithm

The extended Euclidean algorithm can calculate the gcd (a, b) and at the same time calculate the value of x and y in which gcd(a, b)= ax+ by.

To represent 6 as a linear combination of the integers 12378 and 3054, we start from the last step above toward the first step:

Thus, from the last step we have

6 = 24-18

= 24- (138- 5 . 24)

= 6* 24- 138

= 6(162- 138)- 138

= 6* 162 – 7* 138

= 6* 162- 7(3054- 18* 162)

= 132* 162- 7* 3054

= 132(12378 - 4. 3054)- 7* 3054

= 132 *12378 + (-535)*3054

6 = gcd(12378, 3054) = 12378 x + *3054 y*

where *x* = 132 and y = -535. Note that this is not the only way to express the integer 6 as a linear combination of 12378 and 3054.

Example:

Given *a* = 161 and *b* = 28, find gcd (*a*, *b*) and the values of *s* and *t such that gcd(a,b)=as+bt*

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	−5
1	28	21	7	0	1	−1	1	−5	6
3	21	7	0	1	−1	4	−5	6	−23
	7	0		−1	4		6	−23	

Theorem 5.2
If *k* > 0, then *gcd(ka, kb)* = *k* gcd(a, *b)*.

Corollary.
For any integer *k* ≠0, gcd(ka,*kb)* = | *k*| gcd(a, *b)*.

Definition
The *least common multiple* of two nonzero integers *a* and *b*, denoted by lcm(a, *b)*, is the positive integer *m* satisfying the following:

(a) a|m and b |m.

(b) If *a* | c and *b* | c, with c > 0, then *m* ≤ c.

Example:

The positive common multiples of the integers -12 and 30 are

60, 120, 180, ... ; hence, lcm(-12, 30) = 60.

Remark: Given nonzero integers *a* and *b*, lcm(a, *b)* always exists and lcm(a, *b)*≤ |*ab*|.

Theorem 5.3:
For positive integers *a* and *b*

gcd(a, *b)* lcm(a, *b)*= *ab*

Corollary:
For any choice of positive integers *a* and *b*, lcm(a, *b)* = *ab* if and only if

gcd(a, *b)*= 1.

Example:

From previous example: we found the gcd of the integers 3054 and 12378, by using **Euclid's algorithm** gcd(3054, 12378) = 6;

Then by The. 5.3 :

lcm(3054, 12378) =(3054* 12378)/ 6 = 6300402

H.W.

1. Find

a) gcd(143, 227),

b) gcd(306, 657),

c) gcd(272, 1479).

2. . Find

a) lcm(143, 227),

b) lcm(306, 657),

c)lcm(272, 1479).

3. Use the Extended Euclidean Algorithm to obtain integers *x* and y satisfying the following: gcd(56, 72) = *56x + 72y*.

7. Solving linear Equatios

Theorem 6.1

The linear equation *ax + by = c* has infinite number of solution if and only if *d* | c, where *d* = gcd(a, *b).* If x_0 , y_o is any particular solution (initial sol) of this equation, then all other solutions are given by

$$x = x_0 + \left(\frac{b}{d}\right) t \qquad y = y_0 - \left(\frac{a}{d}\right) t$$

where *t* is an arbitrary integer.

Remark: we can use Extended Euclidean Algorithm to obtain initial solution.

Corollary. If gcd(a , *b)* = 1 and if x_0 , y_o is a particular solution of the linear equation *ax* +*by* = c, then all solutions are given by

$$x = x_0 + bt \qquad y = y_0 - at$$

for integer values of *t.*

Example

The linear equation

5x + *6y* = 1 ……(1)

The gcd(5 , 6) = 1. Then eq. (1) has a solution.

By D. A. on 5 & 6 we have

6=5*1+1

Hence 6*1-5*1=1 (-5+6=1) then $x_0 = -1$ and $y_0 = 1$

Then we have

x *= -1 +6 t*

y *= 1-5t*

for some integer *t.*

Example:

Determine all solutions of the following equation The equation *5x + 22y* = 18

Sol:

gcd(5,22) = 1

by D.A. 22= 4*5+2 ➔ $4 * 5 - 22 = -2$ ➔ 4*5-22+20= -2+20

8*5-22=18

Then $x_0 = 8$ and $y_0 = -1$ as one solution, a complete solution is given by

x = 8 + 22t,

y = -1 - 5t

for arbitrary *t.*

Example:

Determine all solutions in the **positive integers** of the following equation:

2x+6y=8

Sol: we have gcd(2,6)=2 and 2|8 then has a solution

6=3*2+0 ➔ 3*2-6+8=8 ➔ 7*2-6= 8

Then $x_0 = 7$ and $y_0 = -1$ as one solution, a complete solution is given by

$$x = 7 + \frac{6}{2}t = 7 + 3t$$

$$y = -1 - \frac{2}{2}t = -1 - t$$

for some integer *t*.

Now the solutions in the positive int. then $7 + 3t > 0$ ^ $-1 - t > 0$

$$t > -\frac{7}{3} \quad \text{^} \quad t < -1$$

Then t= -2 ➔ x= 1 & y= 1

H.W.

1) Which of the following equations cannot be solved?
   a. *6x* + 51y = 22.
   b. *33x* + 14y = 115.
   c. 14x + *35y* = 93.
2) Determine all solutions in the integers of the following equations:
   a. *56x* + *12y* = 40.
   b. *24x* + 138y = 18.
   c. 221x + *35y* = 11.
3) Determine all solutions in the positive integers of the following equations:
   a. 18x + *5y* = 48.
   b. 158x - 57y = 7.

8. The Fundamental Theorem of Arithmetic

Definition

An integer $p > 1$ is called a *prime number*, if its only positive divisors are 1 and p. An integer greater than 1 that is not a prime is termed *composite.*

In the other words a prime number is an integer p > 1 such that it cannot be written as p = ab with a, b > 1.

Example:

Among the first ten positive integers, 2, 3, 5, 7 are primes and 4, 6, 8, 9, 10 are composite numbers. Note that the integer 2 is the only even prime, and according to our definition the integer 1 plays a special role, being neither prime nor composite.

Theorem 8.1

If p *is* a prime and p| ab, then $p \mid a$ or $p \mid b$.

Proof:

If p|a, then we need go no further, so let us assume that p∤a. Because the only positive divisors of p are 1 and p itself, this implies that gcd(p , a) = 1. (In general, gcd(p, a)= p or gcd(p, a)= 1 according as p | a or $p \nmid a$.) Hence, by Euclid's lemma, we get $p \mid b$.

Corollary 1.

If p is a prime and $p \mid a_1 \ a_2 \ \cdots \ a_n$, then $p \mid a_k$ for some k, where 1≤ k≤ n.

Proof.

It is clear if n = 1, and true by theorem 5.1 for n = 2. By induction, suppose that it holds for n = k. Check for n = k + 1:

$$p \mid \underbrace{a_1 a_2 \ldots a_k}_{A} \underbrace{a_{k+1}}_{B}$$

$$p|AB \Rightarrow \begin{cases} p|A & = p|a_1 a_2 \ldots a_k \\ & \Rightarrow p|a_i \text{for some } i \text{ by the induction hypothesis} \\ p|B & \Rightarrow p|a_{k+1} \end{cases}$$

And so we see that the hypothesis holds for n = k + 1 as well.

Corollary 2.
If $p, q_1, q_2, \cdots, q_n$ are all primes and $p \mid q_1\ q_2\ \cdots\ q_n$ then $p = q_k$ for some k, where $1 \leq k \leq n$.

Proof.
H.W

Theorem 8.2 (Fundamental Theorem of Arithmetic).
Every positive integer *n* > 1 can be written as a product of primes (possibly with repetition) and any such expression is unique up to a permutation of the prime factors.

Example:
$360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$ we can see that several of the primes that appear in the factorization of a given positive integer has been repeated.

Corollary.
Any positive integer *n* > 1 can be written uniquely in the form

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

for *i* = 1, 2, ... , *r*, each k_i is a positive integer and each p_i is a prime, with

$$p_1 < p_2 < \cdots < p_r \cdot$$

Remark:
The above form $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ called ***canonical*** form,

Example:
The canonical form of the integer 360 is $360 = 2^3 \cdot 3^2 \cdot 5$

$4725 = 3^3 \cdot 5^2 \cdot 7$ and $17460 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$

Note:
If the integer $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is even iff one of $p_i = 2$ for some i.

Theorem 8.3:

If n is a composite integer, then n has a prime divisor less than $\sqrt{n}$.

Proof:
If n is composite, then it has a positive integer divisor ***a*** with 1 < a < n by definition. This means that n = ab, where b is an integer greater than 1. Assume a > $\sqrt{n}$ and b > $\sqrt{n}$. Then ab > $\sqrt{n}\ \sqrt{n}$ = n, which is a contradiction.

So either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Thus, n has a divisor less than $\sqrt{n}$. By the fundamental theorem of arithmetic, this divisor is either prime, or is a product of primes. In either case, n has a prime divisor less than $\sqrt{n}$.

Corollary:
If n is a positive integer that does not have a prime divisor less than $\sqrt{n}$, then n prime.

Example:
Is 101 prime?

Sol

Since $10<\sqrt{101}<11$, then the primes less than 10 are 2, 3, 5, and 7

Since 101 is not divisible by 2, 3, 5, or 7, it must be prime

Example:
Is 1147 prime?

Sol
$33 <\sqrt{1147} < 34$, then the primes less than 33 are 2, 3, 5, 7, 11, 13, 17, 23, 29, and 31

1147 = 31 × 37, so 1147 must be composite

Theorem 8.4. Euclid
There is an infinite number of primes.

Theorem 8.5.
Let n≥1 then there exist a prime p satisfying the inequality: n≤p<2n

H.W.

1- Given that p is a prime and $p \mid a^n$, prove that $p^n \mid a^n$.

2- Give an example to show that the following conjecture is not true: Every positive integer can be written in the form $p + a^2$, where p *is* either a prime or 1, and $a \geq 0$.

3- Show that gcd(ab, a + b) = 1 if gcd(a, b) = 1.

4- Determine whether the following integers are prime or not

a) 157
b) 701
c) 97

5- Establish the following facts: $\sqrt{p}$ is irrational for any prime p.

6- If $p \neq 5$ is an odd prime, prove that either $p^2 - 1$ or $p^2 + 1$ is divisible by 10.

9. CONGRUENCES

Definition

Let *n* be a fixed positive integer. Two integers *a* and *b* are said to be *congruent modulo n*, symbolized by

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

if *n* divides the difference *a - b;* that is, provided that *a - b = kn* for some integer *k.* When n∤*(a- b),* we say that *a* is *incongruent to b modulo n,* and in this case we write a≢b (mod *n)*

Example:

1) Let *n* = 7.

Then 24 ≡ 3 (mod7) -31 ≡ 11 (mod7) 11≡ 4(mod7)

- 15 ≡ -64 (mod 7)

because 3-24 = (-3)7, -31- 11 = (-6)7, 11-4 =7 -15- (-64) = 7 · 7.

2) 25 ≢ 12 (mod 7), because 7 fails to divide 25- 12 = 13.

Remarks:

1- It is to be noted that any two integers are congruent modulo 1.

2- Any two integers are congruent modulo 2 when they are both even or both odd.

3- Given an integer *a,* let *q* and *r* be its quotient and remainder upon division algorithm by *n,* so that

$$a = qn + r \qquad 0 \le r < n$$

Then, by definition of congruence, *a* ≡ *r* (mod *n).*

4- The set of *n* integers 0, 1, 2, ... , *n* - 1 is called the set of *least nonnegative residues modulo n.*

5- A *complete set of residues modulo n* is the set of integers satisfying no two of the integers are congruent modulo n.

Theorem 9.1

For arbitrary integers *a* and *b*, *a* ≡ *b* (mod *n)* if and only if *a* and *b* have the same nonnegative remainder when divided by *n.*

Proof.

First take $a \equiv b \pmod{n}$, so that n|a-b then $a - b = kn$ *and hence* $a=kn+b$ for some integer *k.*

Upon division by *n, b* we get $b = qn + r$, where $0 \leq r < n$. Therefore,

a= b + kn = (qn + r) + kn = (q + k)n + r then *a* has the same remainder as *b.*

On the other hand, suppose we can write $a = q_1 n + r$ and $b = q_2 n + r$, with the same remainder r $(0 \leq r < n)$. Then $a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n$, hence $n \mid a- b$. *i.e* we have $a \equiv b \pmod{n}$.

Example:

1) Because the integers -56 and -11 can be expressed in the form

$$-56= (-7)9 + 7 \qquad -11 = (-2)9 + 7$$

with the same remainder 7, Theorem 6.1 tells us that $-56\equiv -11 \pmod 9$.

2) $-31 \equiv 11 \pmod 7$ implies that -31 and 11 have the same remainder when divided by 7; this is clear from the relations

$$-31 = (-5)7 +4 \qquad 11=1\cdot 7+4$$

Theorem 9.2

Let $n > 1$ be fixed and *a, b, c, d* be arbitrary integers. Then the following properties hold:

1. $a\equiv a \pmod n$ for any a;
2. $a\equiv b \pmod n$ implies $b \equiv a \pmod n$;
3. $a\equiv b \pmod n$ and $b \equiv c \pmod n$ implies $a\equiv c \pmod n$;
4. $a\equiv 0 \pmod n$ iff n|a ;
5. $a\equiv b \pmod n$ and $c\equiv d \pmod n$ implies $a+c\equiv b+ d \pmod n$;
6. $a\equiv b \pmod n$ and $c\equiv d \pmod n$ implies $a-c\equiv b-d \pmod n$;
7. $a\equiv b \pmod n$ and $c\equiv d \pmod n$ implies $ac\equiv bd \pmod n$; [the converse is not true show me that](H.W)
8. If $a\equiv b \pmod n$, then $a+c \equiv b + c \pmod n$ and $ac \equiv bc \pmod n$.
9. $a\equiv b \pmod n$ implies $a^j \equiv b^j \pmod n$ for each integer $j\geq 1$.

Proof:

1, 2, 3,4, 5 & 8 (H.W)

6. Since a≡b (mod n) and c≡d (mod n) then n|a−b and n|c−d, so we have n|(a−b)−(c−d). Rearranging the terms, this means n|(a−c)−(b−d), so a−c≡b− d.

7. Since a≡ b (mod n) and c≡ d (mod n) then n|a−b and n|c−d, so we have n|(a−b)(c−d).

(a−b)(c−d)= ac-ad-bc+bd =ac-bd+bd -ad-bc+bd= (ac-bd)-b(c-d)-d(a-b)

∴ n|(ac-bd)-b(c-d)-d(a-b) since n|c-d & n|a-b then n|ac-bd ➔ ac ≡bd (mod n)

9. Proof by induction.

-The statement is true *for j*= 1,

-Assume it is true for some k *i.e.* $a^k \equiv b^k$

Now we have $a \equiv b$ (mod *n)* and $a^k \equiv b^k$ (mod *n) then by (7)* $aa^k \equiv bb^k$ (mod *n),* ➔ $a^{k+1} \equiv b^{k+1}$ (mod n) and so the induction step is complete.

Example
Show that 41 divides $2^{20} - 1$.

Sol
$2^5 \equiv -9\ (mod\ 41)$,

$2^{5^4} \equiv (-9)^4\ (mod\ 41)$ [by Theorem 6.2(9)]

$2^{20} \equiv 81 \cdot 81\ (mod\ 41)$.

$2^{20} - 1 \equiv 81 \cdot 81 - 1\ (mod\ 41)$. [by Theorem 6.2(8)]

81 ≡ -1 (mod 41) ➔ $81 \cdot 81 \equiv 1$ (mod 41). [by Theorem 6.2(7)]

$2^{20} - 1 \equiv 1 - 1 = 0 (mod\ 41)$.

Thus, $41 \mid 2^{20} - 1$

Example

Find the remainder obtained upon dividing the sum

1! + 2! + 3! + 4! + ... + 99! + 100! by 12.

Sol:
4! = 24 ≡ 0 (mod 12); thus, *for* $k \geq 4$,

k! = $4! \cdot 5 \cdot 6 \cdots k = 0 \cdot 5 \cdot 6 \cdots k \equiv 0$ (mod 12)

In this way, we find that

$1! + 2! + 3! + 4! + ... + 100! \equiv 1! + 2! + 3! + 0 + \cdots + 0 \equiv 9 \pmod{12}$

i.e r=9

Theorem 9.3.

If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Corollary 1.

If $ca \equiv cb \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.

Corollary 2.

If $ca \equiv cb \pmod{p}$ and $p \nmid c$, where p is a prime number, then $a \equiv b \pmod{p}$.

Proof: The conditions $p \nmid c$ and p a prime imply that $\gcd(c, p) = 1$.

Example

1) Consider the congruence $33 \equiv 15 \pmod{9}$ or, if one prefers,

$$3 \cdot 11 \equiv 3 \cdot 5 \pmod{9}.$$

Because gcd(3 , 9) = 3, Theorem 6.3 leads to the conclusion that

$$11 \equiv 5 \pmod{3}.$$

2) $-35 \equiv 45 \pmod{8}$, which is the same as $5 \cdot (-7) \equiv 5 \cdot 9 \pmod{8}$. The integers 5 and 8 being relatively prime,

we may cancel the factor 5 to obtain a correct congruence $-7 \equiv 9 \pmod{8}$.

Remark:

If $ab \equiv 0 \pmod{n}$ it is not necessary to have $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$

For example $4 \cdot 3 \equiv 0 \pmod{12}$, but $4 \not\equiv 0 \pmod{12}$ and $3 \not\equiv 0 \pmod{12}$.

While if $ab \equiv 0 \pmod{n}$ and gcd(a , n) = **1,** then $b \equiv 0 \pmod{n}$ [Corollary 1] since $ab \equiv a \cdot 0 \pmod{n}$.

Also $ab \equiv 0 \pmod{p}$, with p a prime, then either $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

10. linear congruent

Def.

let a,b be any non-zero integers then there exist an integer x s.t.

$ax \equiv b(mod\ n)$ for all n≥1 then this form called linear congruent.

Ex.: $2x \equiv 1(mod\ 5)$ $, x = 3, -2, 8, ...$

Ex.: $7x \equiv 3\ (mod\ 11)$ $\quad , x = 2, 13, -9$

Ex.: $5x \equiv -9\ (mod\ 12)$ $\quad , x = 3,15, \ldots$

Example

Find all integers x such that

1) $3x-5$ is divisible by 11.
2) $10x \equiv 8 \pmod 6$

Sol.

1) $3x \equiv 5 \pmod{11}$

$3x \equiv 5 \Rightarrow 4 \cdot 3x \equiv 4 \cdot 5 \pmod{11} \Rightarrow 12x \equiv 20 \pmod{11} \Rightarrow x \equiv 9 \pmod{11}$

So if $3x \equiv 5$ then $x \equiv 9$, or $x \in \{\ldots, -13, -2, 9, 20, \ldots\}$.

2) $10x \equiv 8 \pmod 6$

By The. 6.3 we have $5x \equiv 4 \pmod 3 \Rightarrow 5x - 6x \equiv 4 \pmod 3$

$-x \equiv 4 \pmod 3 \Rightarrow x \equiv -4 \pmod 3 \Rightarrow x \equiv -4+6 \pmod 3 \Rightarrow x \equiv 2$

$x \in \{\ldots, -4, -1, 2, 5, \ldots\}$.

Theorem 10.1: The linear congruence $ax \equiv b \pmod n$ has a solution if and only if $d \mid b$, where $d = \gcd(a, n)$. If $d \mid b$, then it has ***d*** **incongruent solutions** modulo n.

Corollary:

If gcd(a , n) = 1, then the linear congruence $ax \equiv b \pmod n$ has a unique solution modulo n.

Def:

Given relatively prime integers a and n, the congruence $ax \equiv 1 \pmod n$ has a unique solution. This solution is sometimes called the (**multiplicative**) inverse of a modulo n.

Example : First consider the linear congruence $18x \equiv 30 \pmod{42}$. Because gcd(18, 42) = 6 and 6 surely divides 30, Theorem 6.4 guarantees the existence of exactly six solutions, which are incongruent modulo 42. One solution is found as follows:

$18x \equiv 30 \pmod{42}$.

$6.3x \equiv 6.5 \pmod{42}$.

3x≡5 (mod 42/gcd(6,42)).

3x≡5 (mod 7).

6x≡10 (mod 7).

-x≡ 3 (mod 7)

x≡-3 (mod 7)

x≡ 4 mod 7

The six solutions are as follows:

$x = 4 + (42/6)t = 4 + 7t \pmod{42}$ $t = 0, 1, \ldots, 5$

$x = 4, 11, 18, 25, 32, 39 \pmod{42}$

Example: Let us solve the linear congruence $9x \equiv 21 \pmod{30}$. At the outset, because gcd(9, 30) = 3 and 3 | 21, we know that there must be three incongruent solutions can be find as follows:

$9x \equiv 21 \pmod{30}$

$3.3x \equiv 3.7 \pmod{30}$

$3x \equiv 7 \pmod{10}$.

9x ≡ 21 mod 10

-x≡ 1 mod 10

x≡ -1 mod 10

x≡9 mod 10

Now $x = 9 + \frac{30}{3}t \ , t = 0,1,2$

we obtain 9, 19, 29, whence $x \equiv 9 \pmod{30}$, $x \equiv 19 \pmod{30}$, $x \equiv 29 \pmod{30}$ are the required three solutions of $9x \equiv 21 \pmod{30}$.

H. W.

1) Find the remainder obtained by

a) $3|41^{75}$

b) 2^{50} are divided by 7.

c) 41^{65} are divided by 7.

2) Prove each of the following:

(a) If $a \equiv b \pmod{n}$ and $m|n$, then $a \equiv b \pmod{m}$.

(b) If $a \equiv b \pmod{n}$ and $c > 0$, then $ca \equiv cb \pmod{cn}$.

3) Give an example to show that $a^2 \equiv b^2 \pmod{n}$ need not imply that $a = b \pmod{n}$.

4) If $a \equiv b \pmod{n}$, prove that gcd(a, n) = gcd(b, n).

5) What is the remainder when the following sum is divided by 4?

$$1^5 + 2^5 + 3^5 + \ldots + 99^5 + 100^5$$

6) Prove that the integer $53^{103} + 103^{53}$ is divisible by 39.

7) Find all the solution if exist to the following equation.

a) $7x = 3 \pmod{11}$

b) $5x \equiv -9 \pmod{12}$

c) $12x \equiv 16 \pmod{32}$

11. Important Theorems

Def.:

The form

$$a_1 x \equiv b_1 (mod\ m_1)$$
$$a_2 x \equiv b_2 (mod\ m_2)$$
$$\vdots$$
$$a_n x \equiv b_n (mod\ m_n)$$

is called n-linear congruence system

(11.1) (Chinese Remainder Theorem.)

Let $n_1, n_2, \ldots, n_r$ be positive integers such that $gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$x = a_1\ (mod\ n_1)$$
$$x = a_2\ (mod\ n_2)$$
$$\vdots$$
$$x = a_r\ (mod\ n_r)$$

has a simultaneous solution, which is unique modulo the integer $n = n_1 n_2, \cdots n_r$ and these solution is

$$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$$

Where $N_k = \frac{n}{n_k} = n_1 \cdots n_{k-1} n_{k+1} \cdots n_r$

$N_k x_k \equiv 1\ (mod\ n_k)$. , x_k was chosen to satisfy the congruence

Example:

Find the simultaneous solution

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

By Theorem 11.1 we have n= 3.5.7=105 and

$$N_1 = \frac{n}{3} = 35 \qquad N_2 = \frac{n}{5} = 21 \qquad N_3 = \frac{n}{7} = 15$$

Now the linear congruences

$$35x \equiv 1 \pmod 3 \qquad 21x \equiv 1 \pmod 5 \qquad 15x \equiv 1 \pmod 7$$

are satisfied by $x_1 = 2, x_2 = 1, x_3 = 1$, respectively. Thus, a solution of the system is given by

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$$

Then the unique solution is $x = 233 \equiv 23 \pmod{105}$.

Example: Use the Chinese Remainder Theorem to find an x such that

$$x \equiv 2 \pmod 5$$

$$x \equiv 3 \pmod 7$$

$$x \equiv 10 \pmod{11}$$

Solution:

n = 5 × 7 × 11 = 385.

$$N_1 = \frac{n}{5} = 77, \qquad N_2 = \frac{n}{7} = 55, \qquad N_3 = \frac{n}{11} = 35.$$

$77x \equiv 1 \pmod 5$, $55x \equiv 1 \pmod 7$, $35x \equiv 1 \pmod{11}$

and hence an inverse to N1 mod n1 is x1 = 3.

an inverse to N2 mod n2 is x2 = 6.

an inverse to N3 mod n3 is x3 = 6.

By Theorem 11.1 we have

$$x = x_1 a_1 N_1 + x_2 a_2 N_2 + x_3 a_3 N_3$$

$$x = 3 \times 2 \times 77 + 6 \times 3 \times 55 + 6 \times 10 \times 35 = 3552.$$

Since we may take the solution modulo N = 385, we can reduce this to 87, since $2852 \equiv 87 \pmod{385}$

(11.2) Fermat's theorem.

Let p be a prime and suppose that $p \nmid a$. Then $a^{p-1} \equiv 1 \ (mod\ p)$.

Example:

Take p=5 and a=2 , gcd(a,p) =1 then by Fermat the. $2^{5-1} \equiv 1 \ (mod\ 5)$

H.W

p=7 , a= 3

Corollary

If p is a prime, then $a^p \equiv a \ (mod\ p)$ for any integer a.

Example:

verify that $5^{38} \equiv 4 \ (mod\ 11\ )$, by Fermat the., we have the congruence

$$5^{10} \equiv 1 \pmod{11}$$

$5^{38} \equiv 5^{10.3+8} \ (mod\ 11\ ) \equiv (5^{10})^3 . (5^2)^4 \equiv 1^3 . 3^4 \equiv 81 \equiv 4 \pmod{11}$

Test Prime

Another use of Fermat's theorem is as a tool in testing the primality of a given integer n. If it could be shown that the congruence $a^n \equiv a \ (mod\ n)$ fails to hold for some choice of a, then n is necessarily composite. As an example of this approach, let us look at n = 117. The computation is kept under control by selecting a small integer for a, say, a = 2. Because 2^{117} may be written as:

$$2^{117} = 2^{7 \cdot 16+5} = (2^7)^{16} 2^5$$

and $2^7 = 128 \equiv 11 \pmod{117}$, we have

$$2^{117} \equiv 11^{16} \cdot 2^5 \equiv (121)^8 2^5 \equiv 4^8 \cdot 2^5 \equiv 2^{21} \pmod{117}$$

But $2^{21} = (2^7)^3$, which leads to

$$2^{21} \equiv 11^3 \equiv 121 \cdot 11 \equiv 4 \cdot 11 \equiv 44 \pmod{117}$$

Combining these congruences, we finally obtain

$$2^{117} \equiv 44 \not\equiv 2 \pmod{117}$$

so that 117 must be composite; actually, $117 = 13 \cdot 9$.

The converse of Fermat's theorem is not true:

Example:

$5^3 \equiv 1 \pmod{4}$ but 4 is not prime

Definition :

A composite integer *m* is called *pseudoprime* whenever $a^{m-1} \equiv 1\ (mod\ m)$. Or $a^m \equiv$ a (mod m).

It can be shown that there are infinitely many pseudoprimes, the smallest four being 341, 561, 645, and 1105.

H.W.

561 is *pseudoprime*

Proposition:

Any absolute pseudoprime is square-free.

Proof:

Suppose that n is pseudoprime, then $a^n \equiv$ a $(mod\ n)$ for every integer a, suppose $k^2 | n$ for some k > l. put a = k, then $k^n \equiv$ k $(mod\ n)$. Because $k^2 | n$, this last congruence holds modulo k2; that is, $k^n \equiv$ k $\equiv 0 (mod\ k^2)$. whence $k^2 | k$ which is impossible. Thus, n must be square-free.

(11.3) WILSON'S THEOREM :

If p is a prime, then $(p - 1)! \equiv -1\ (mod\ p)$.

Example

Take p = 13. It is possible to divide the integers 2, 3, ... , 11 into pairs, each product of which is congruent to 1 modulo 13.

$$2 \cdot 7 \equiv 1 \pmod{13}$$
$$3 \cdot 9 \equiv 1 \pmod{13}$$
$$4 \cdot 10 \equiv 1 \pmod{13}$$
$$5 \cdot 8 \equiv 1 \pmod{13}$$
$$6 \cdot 11 \equiv 1 \pmod{13}$$

Multiplying these congruences gives the result

$$11! = (2 \cdot 7)(3 \cdot 9)(4 \cdot 10)(5 \cdot 8)(6 \cdot 11) \equiv 1 \pmod{13}$$

and so

$$12! \equiv 12 \equiv -1 \pmod{13}$$

Thus, $(p - 1)! \equiv -1 \pmod{p}$, with $p = 13$.

Theorem (The converse of Wilson's theorem)

If (n- 1)! = -1 (mod n), then *n* must be prime.

Proof

If *n* is not a prime, then *n* has a divisor *d* with $1 < d < n$.

Furthermore, because $d \leq n$- 1, *d* occurs as one of the factors in (n- 1)!, whence *d* |(n - 1)!.

Now we have *n*|(n- 1)! + 1, and so d |(n - 1)! + 1, too. The conclusion is that *d* | 1, which is a contradiction.

H.W.

1. Use Fermat's theorem to verify that 17 divides $11^{104} + 1$.
2. Using Wilson's theorem, prove that for any odd prime p,

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$$

[*Hint:* Because $k \equiv -(p-k) \pmod{p}$, it follows that

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv (-1)^{(p-1)/2} 1 \cdot 3 \cdot 5 \cdots (p-2) \pmod{p}.]$$

3. Show that $18! \equiv -1 \pmod{437}$.

12. Number-theoretic functions

Definition :

Any function whose domain of definition is the set of positive integers is said to be a *number-theoretic* (or *arithmetic) function.*

Definition :

A number-theoretic function *f* is said to be *multiplicative* if *f(mn) = f(m)f(n)* whenever *gcd(m, n)* = 1

Theorem 12.1

If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then the positive divisors of *n* are precisely those integers *d* of the form

$$d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where $0 \leq a_i \leq k_i$ $(i = 1, 2, \ldots, r)$.

Lemma

If *gcd(m, n)* = 1, then the set of positive divisors of *mn* consists of all products $d_1 d_2$, where $d_1 | m$, $d_2 | n$ and gcd(d_1, d_2) = 1; furthermore, these products are all distinct.

(12.1) τ and σ multiplicative functions:

Given a positive integer *n*, let $\tau(n)$ denote the number of positive divisors of *n* and $\sigma(n)$ denote the sum of these divisors.

i.e.

$$\tau(n) = \sum_{d \mid n} 1 \qquad \sigma(n) = \sum_{d \mid n} d$$

For an example of these notions, consider $n = 12$. Because 12 has the positive divisors 1, 2, 3, 4, 6, 12, we find that

$$\tau(12) = 6 \qquad \text{and} \qquad \sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$$

For the first few integers,

$$\tau(1) = 1 \quad \tau(2) = 2 \quad \tau(3) = 2 \quad \tau(4) = 3 \quad \tau(5) = 2 \quad \tau(6) = 4, \ldots$$

and

$$\sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 7, \sigma(5) = 6, \sigma(6) = 12, \ldots$$

It is not difficult to see that $\tau(n) = 2$ if and only if n is a prime number; also, $\sigma(n) = n + 1$ if and only if n is a prime.

Remark:

If $n = p^a$, $a \geq 0$, p is any prime, the all positive of n are $1, p, p^2, p^3, \ldots, p^{a-1}, p^a$. This mean that the number of all positive divisor of n is equal a+1 i.e.

$$\tau(p^a) = a + 1$$

And

$$\sigma(p^a) = 1 + p + p^2 + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1}$$

Theorem 12.3:

If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then

(a) $\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$, and

(b) $\sigma(n) = \dfrac{p_1^{k_1+1} - 1}{p_1 - 1} \dfrac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \dfrac{p_r^{k_r+1} - 1}{p_r - 1}$.

Example:

The number $180 = 2^2 \cdot 3^2 \cdot 5$ has

$$\tau(180) = (2 + 1)(2 + 1)(1 + 1) = 18$$

The sum of these integers is

$$\sigma(180) = \frac{2^3 - 1}{2 - 1} \frac{3^3 - 1}{3 - 1} \frac{5^2 - 1}{5 - 1} = \frac{7}{1} \frac{26}{2} \frac{24}{4} = 7 \cdot 13 \cdot 6 = 546$$

H.W.

1. $\tau(1000000)$ *and* $\sigma(1000000)$

2. $\tau(120)$ *and* $\sigma(120)$

Theorem 12.4

The functions τ and σ are both multiplicative functions.

Proof.

Let *m* and *n* be relatively prime integers. Because the result is trivially true if either *m or n* is equal to 1, we may assume that $m > 1$ and $n > 1$. If

$$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \qquad \text{and} \qquad n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$$

are the prime factorizations of *m* and *n,* then because *gcd(m, n)* = 1, it follows that the prime factorization of the product *mn* is given by

$$mn = p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}$$

Appealing to Theorem 12.3, we obtain

$$\begin{aligned} \tau(mn) &= [(k_1 + 1) \cdots (k_r + 1)][(j_1 + 1) \cdots (j_s + 1)] \\ &= \tau(m)\tau(n) \end{aligned}$$

In a similar Theorem 7.3 gives

$$\begin{aligned} \sigma(mn) &= \left[\frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}\right]\left[\frac{q_1^{j_1+1} - 1}{q_1 - 1} \cdots \frac{q_s^{j_s+1} - 1}{q_s - 1}\right] \\ &= \sigma(m)\sigma(n) \end{aligned}$$

Thus, τ and σ are multiplicative functions.

H.W.

Does σ is multiplication function when m=2 and n=10?? Why?

(12.2) EULER'S PHI-FUNCTION

Definition

For $n \geq 1$, let $\phi(n)$ denote the number of positive integers not exceeding *n* that are relatively prime *to n.* The function ϕ is usually called the *Euler ϕ-function.*

Example:

$\phi(30) = 8$; for, among the positive integers that do not exceed 30, there are eight that are relatively prime to 30; specifically, 1, 7, 11, 13, 17,19,23,29

Similarly, for the first few positive integers, the reader may check that

ϕ (l) = 1, ϕ(2) = 1, ϕ (3) = 2, ϕ (4) = 2, ϕ (5) = 4, ϕ (6) = 2, ϕ (7) = 6, ...

Remark:

ϕ(p)=p-1 {p is prime}

Theorem 13.1

If *p* is a prime and *k* > 0, then

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

Example:

$$\phi(9) = \phi(3^2) = 3^2 - 3 = 6$$

$$\phi(16) = \phi(2^4) = 2^4 - 2^3 = 16 - 8 = 8$$

Lemma.

Given integers *a, b,* c, gcd(a, *bc)*= 1 if and only if gcd(a, *b)*= 1 and gcd(a, c) = 1.

Theorem 8.2

The function ϕ is a multiplicative function.

Corollary 8.3

If the integer *n* > 1 has the prime factorization, $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ then

$$\begin{aligned}\phi(n) &= \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\cdots\left(p_r^{k_r} - p_r^{k_r-1}\right)\\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)\end{aligned}$$

Example:

$$\phi\,(100) = \phi(2^2 5^2) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 100 * \frac{1}{2} * \frac{4}{5} = 40$$

Theorem 8.4

For n > 2, ϕ(n) is an even integer.

EULER'S THEOREM

We have seen while discussing Fermat's Theorem that $a^{p-1} \equiv 1 \pmod{p}$ for any integer a if p†a. Note that the exponent p− 1 equals φ(p). Let us now take a

composite number, say n = 12 and another integer a = 5 relatively prime to 12. If we look at $a^{\varphi(n)}\ mod\ n$, we find that $5^{\varphi(12)} = 5^4 = 5^2 \cdot 5^2 \equiv 1 \bmod 12$. The following theorem explains the above observation. The theorem is known as Euler's theorem .

Theorem (Euler) 8.5

If $n \geq 1$ and gcd(a, *n)* = 1. Then $a^{\varphi(n)} \equiv 1\ mod\ n$.

Example:

n = 18. Then $\varphi(18) = \varphi(2)\varphi(9) = (2-1)(3^2-3) = 6$. Euler's theorem says that $a^6 - 1$ is divisible by 18 for any integer a relatively prime to 18.

Take a = 5. We can directly verify that $5^6 \equiv 25^3 \equiv 7^3 \equiv 1\ (mod\ 18)$.