MODULE I

<u>Elements</u> of <u>Number</u> <u>Theory</u> We begin with a basic study of the multiplicative structure of Z and we introduce the Euler phi function, which plays an important role in the study of "residue systems".

<u>Definition 1</u> If $a, b \in Z$ we say a <u>divides</u> b, denoted by $a \mid b$, provided $\exists\, c \in Z$ such that $b = ac$.

<u>Examples</u> 1. $a \mid 0 \; \forall a \in Z$ since $0 = a \cdot 0$

2. $5 \mid -5$ because $-5 = 5(-1)$

3. $7 \mid 49$ because $49 = 7(7)$

<u>Proposition 1</u> $\forall\, a, b, c \in Z$

1. $a \mid b$ and $b \mid c \Rightarrow a \mid c$
2. $a \mid b$ and $a \mid c \Rightarrow a \mid bx+cy \quad \forall\, x, y \in Z$
3. $a \mid a \;\; \forall a$ (EVEN $a = 0$)
4. $a \mid b$ and $b \mid a \Rightarrow a = \pm\, b$

Some proofs: 1. $b = ad$, $c = be \Rightarrow c=(ed)a$

4. $b = af$, $a = gb \Rightarrow a = gfa$

$a \neq 0 \Rightarrow gf = 1 \Rightarrow g = f=1$ or $g = f = -1$

Exercise 1 (Submit b and d) Prove

a) $\forall n\, (4 \chi\, n^2 + 1)$

b) $\forall\, x,y \in Z$ (x,y odd $\Rightarrow x^2 + y^2$ is even but $4 \chi\, x^2 + y^2$)

c) $\forall\, a,b,c,d \in Z\, (a \mid b$ and $c \mid d \Rightarrow ac \mid bd)$

d) $\forall\, n \in Z$ (n odd $\Rightarrow 8 \mid n^2 - 1)$

e) $\forall n\, (6 \mid (n)\,(n+1)\,(n+2))$

f) $\forall n\, (24 \mid (n)\,(n+1)\,(n+2)\,(n+3))$

<u>Division</u> <u>Algorithm</u>. <u>Theorem 1</u>

Let $a \in Z$, $d \in Z^+$; then $\exists$ a unique pair q, r such that $a = q\,d+r$ were $0 \leq r \leq d-1$.

<u>Notation</u>: r is denoted by <u>a modd</u> and q by <u>a divd</u>.

<u>Proof</u> Let $T = \{a\text{-}cd \mid c \in Z \text{ and } a - cd \geq 0\}$

First we show that $T \neq \emptyset$. Indeed, if $a \geq 0$ then $a = a - 0d \in T$

If $a < 0$ then $(d-1)(-a) = a-(a)d \in T$

Thus T has a smallest element, say r; i.e. $\exists\, q \in Z$ such that $a - qd = r$

<u>Claim</u> $0 \leq r < d$. <u>Proof</u> Of course $r \geq 0$ because $r \in T$.

Suppose $r \geq d$; then $r - d \geq 0$, $r - d < r$ and $a - (q+1)d = r\text{-}d \in T$

which contradicts the fact that r = minimum of T.

<u>Claim</u> q and r are unique; Suppose $a = qd + r = q'd + r'$ where $0 \leq r, r' < d$.

Assuming $r \geq r'$ we get $r - r' = (q' - q)d$

so $q'\text{-}q \geq 0$. But $q'\text{-}q > 0$ implies $(q'\text{-}q)d > d$. However $0 \leq r - r' < d$ - a contradiction.

Thus $q' = q$ and consequently $r = r'$.

<u>Definition</u> 2. If $a \in Z$ and $b \in Z - \{0\}$ then

$\left\lfloor \frac{a}{b} \right\rfloor$ and $\left\lceil \frac{a}{b} \right\rceil$ denotes that <u>largest integer less than or equal to</u> $\frac{a}{b}$

and the smallest <u>integer greater than or equal to</u> $\frac{a}{b}$ respectively.

<u>Remark</u> 1. The question of existence is easily settled with aid of the Division Algorithm.

Indeed, when $b > 0$, $a \text{ div } b = \left\lfloor \frac{a}{b} \right\rfloor$ and $r = a - \left\lfloor \frac{a}{b} \right\rfloor b$

<u>Example 5</u>. Let $d = 5$ and $a = -73$. Then $-73 = (-15)(5) + 2$.

<u>Definition 3.</u> The non - $\emptyset$ set $I \subseteq Z$ is an <u>ideal</u> if and only if

1. $\forall\, a, b\ (a, b \in I \Rightarrow a - b \in I)$,

and 2. $\forall\, a, b\ (a \in Z, b \in I \Rightarrow a\,b \in I)$.

<u>Theorem 2</u> If I is an ideal then $\exists$ a unique $d \geq 0$ such that $I = \{a\,d \mid a \in Z\}$

<u>Notation</u> We write (d) and say that I is generated by d. Such an ideal of Z is <u>principal</u>,

$(Z, +, \bullet)$ is called a <u>principal</u> <u>ideal</u> <u>domain</u> (p.i.d).

Proof Since $I \neq \emptyset \; \exists \; b \in I$. Since $b \in I$ so does $-b = (-1)\, b$ by 2) and we may conclude that $\exists \; b \in I$ such that $b \geq 0$. If only $b = 0$ lies in I then $I = (0)$. Otherwise let

$$d = \min \{ b \in I \,|\, b > 0 \}.$$

Then, by 2) $\quad (d) \subseteq I$.

Next, if $a \in I$ we may invoke the Division Algorithm to get

$$a = q\, d + r$$

where $0 \leq r \leq d-1$. But $r = a - q\, d \in I$ by 1) and 2) so $r = 0$. Hence $a = q\, d \in (d)$.

Finally, uniqueness of d follows from (4) of our first proposition; i.e. Proposition 1.(4).

Application Consider an arbitrary pair $a, b \in Z$, not both 0, and realize that $I = \{ a\,x + b\,y \,|\, x, y \in Z \}$ is an ideal. Furthermore, since $I \neq (0)$, $\exists$ a unique $d > 0$ such that $I = (d)$.

Now, as $a, b \in I$ it follows that $d \,|\, a$ and $d \,|\, b$, i.e. d is a common divisor of a and b.

Next suppose $d' > 0$ is another common divisor of a and b, i.e. $d' \,|\, a$ and $d' \,|\, b$. Then, by 2 of our first proposition, $d' \,|\, a\,x + b\,y \;\; \forall \; x, y \in Z$. Now $\exists \; x_1, y_1$ such that $d = ax_1 + b_1$.

But then $d' \,|\, d$ so d is a greatest common divisor of a and b.

Definition 4 and Remark 2 Given $a, b \in Z$, not both zero, the greatest common divisor of a and b (g c d (a, b)) is the largest positive d such that $d \,|\, a$ and $d \,|\, b$. As per our previous discussion MORE is true: if $d' \,|\, a$ and $d' \,|\, b$ then not only is $d' \leq d$ but ALSO $d' \,|\, d$. If $a = 0$, $b > 0$, g c d (a, b) = b.

Exercise 2 a) (Submit this one) Given $a_1, a_2, \ldots a_n$ $(n \geq 2)$ at most one being 0 prove that the process

$d_2 = \text{g c d}\,(a_1, a_2)$,

$d_3 = \gcd(d_2, a_3), \ldots, d_n = \gcd(d_{n-1}, a_n)$ yields a gcd of $a_1, \ldots a_n$ and

$$(d_n) = \left\{ \sum_{i=1}^{n} a_i \, x_i \,\middle|\, x_i \in Z \; i = 1, \ldots, n \right\}.$$

Exercise 2 b) Prove: $\forall \; a, b \; \big(\text{g c d}\,(a, 4)\big) = \text{g c d}\,(b, 4) = 2 \Rightarrow \text{g c d}\,(a+b, 4) = 4$.

Example 6. The set of divisors of 24 and 36 is $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$ so g c d (24, 36) = 12.

Another related notion is that of the <u>least common</u> multiple of a and b, denoted by <u>lcm(a, b).</u>
We prove it existence and determine its nature in the following theorem:

<u>Theorem 3</u> Given $a, b \in Z^+$ the set $I = \{m \in Z \mid a|m \text{ and } b|m\}$
- the set of ALL common mutiples of a and b, is an ideal and $I \neq (0)$. Its generator, i.e. the smallest positve number in I, say $\overline{m}$, yields $I = (\overline{m})$ and is a common multiple of a and b which <u>divides</u> every common multiple of a and b, we write $\overline{m} = \text{lcm}(a, b)$.

<u>Proof</u> If $a|m_1$, $a|m_2$, $b|m_1$ and $b|m_2$ then a and b divide $m_1 - m_2$. Also if a, b both divide m and $c \in Z$ then $a, b|cm$ so $cm \in I$. Also $I \neq \emptyset$. Hence I is an ideal and has a unique positive generator $\overline{m}$. Since $\overline{m} \in I$ we have $a, b|\overline{m}$. Also $\overline{m}|m$ $\forall$ $m \in I$ so $\overline{m}$ divides every common multiple of a and b.

<u>Question</u> How are gcd(a, b) and lcm(a, b) related?

<u>Theorem 4.</u> $\gcd(a, b)\,\text{lcm}(a, b) = ab$, $\forall$ $a, b \in Z^+$.

<u>Proof</u> Realize that, because $\dfrac{a}{\gcd(a, b)}$ and $\dfrac{b}{\gcd(a, b)}$ are both integers,

$\dfrac{ab}{\gcd(a, b)}$ is a common multiple of a and b. Thus $\text{lcm}(a, b) \mid \dfrac{ab}{\gcd(a, b)}$ and so

$$\text{lcm}(a, b)\gcd(a, b)|ab.$$

Now $\exists$ $\alpha, \beta \in Z$ such that $\text{lcm}(a,b) = \alpha a$, $\text{lcm}(a, b) = \beta b$.
Thus, with $\gcd(a, b) = a x + b y$

$$\text{lcm}(a, b)\gcd(a, b) = (\beta x + \alpha y)\ (ab)$$

i.e. $ab \mid \text{lcm}(a,b)\gcd(a,b)$
As both numbers are positive 4) of Proposition 1 yields the result.

<u>Exercise 3</u> (Submit b; d and e are for extra credit)

a) Given $a_1, a_2, \ldots, a_n \in Z^+$ where $n \geq 2$ prove

$$\text{lcm}(a_1, a_2, \ldots, a_n) \text{exists}$$

and the procedure

$$l_2 = \text{lcm}(a_1, a_2),\ l_3 = \text{lcm}(l_2, a_3), \ldots, l_n = \text{lcm}(l_{n-1}, a_n)$$

terminates in $\text{lcm}(a_1, a_2, \ldots, a_n)$
Is the following true:

$$\text{lcm}(a_1, \ldots, a_n) \bullet \gcd(a_1, \ldots, a_n) = \prod_{i=1}^{n} a_1 \,?$$

b) Prove: $\forall$ a, b, m (gcd(a m) = gcd(b, m) = 1 $\Rightarrow$ gcd(ab, m)=1)

c) Prove: Given $g \in Z^{+}$ and $s \in Z$, $\exists$ $x, y \in Z$ such that

$$x+y = s \text{ and } \gcd(x, y) = g \text{ if and only if } g \mid s$$

d) Prove: $\nexists$ a, b, n > 1 such that $a^n - b^n \mid a^n + b^n$

e) Prove: $\forall$ a, b > 2 $(2^b - 1 \chi\ 2^a + 1)$

f) Prove: $\forall$ a, b, c $\left(a \mid bc \text{ if and only if } \dfrac{a}{\gcd(a, b)} \mid c \right)$

Example 7. Recall gcd(24, 36) = 12. So $\text{lcm}(24, 36) = \dfrac{(24)(36)}{12} = 72$

Corollary 4.1 and Definition 4. Integers a, b are relatively prime (or coprime) if gcd (a, b) = 1. In this event lcm (a, b) = ab.

Theorem 5. If $a \mid bc$ and a and b are relatively prime then $a \mid c$.

Proof Since gcd (a, b) = 1 the ideal

$$I = \{a x + by \mid x, y \in Z\} = (1)$$

Thus $\exists$ x, y such that 1 = a x + b y

Hence

$$c = acx + bcy$$

Now $a \mid acx$ and $a \mid bcy$ implies by 2 of Proposition1. that $a \mid c$

Exercise 4. (Submit this one) Suppose $\gcd(a_i, b) = 1$ $\quad i = 1,\ldots,k$.

Prove $\gcd\left(\prod_{i=1}^{k} a_i, b \right) = 1$.

Corollary 5.1 and Definition 5. The integer $p \geq 2$ is prime if and only if the only positive divisors of p are 1 and p. Otherwise it is composite.

If p is prime and $p|ab$ then $p|a$ or $p|b$.

Proof Suppose $p \not| a$. Then gcd(p, a) = 1 and so $p|b$ by the previous proposition.

Exercise 5 (Submit a)) a) Suppose gcd $(a_i, a_j) = 1$, $1 \leq i, j \leq k$ and $i \neq j$ and

$$a_i \Big| b\ \forall i. \text{ Prove } \prod_{i=1}^{k} a_i \Big| b.$$

b) Suppose a, b > 0 and d = gcd(a, b). Prove: if k|d then $\gcd(\frac{a}{k}, \frac{b}{k}) = \frac{d}{k}$.

Question How is gcd(a, b) calculated algorithmically? We develop two algorithms for this purpose. The essence of the first one, the Euclidean algorithm, is given in the following result:

Proposition 2 Let $a \geq b \geq 0$ not both 0 and write $a = q\,b + r$, where $a > 0$ and $r = a$ if $b = 0$, and $0 \leq r \leq b-1$ if $b > 0$. Then gcd(a, b) = gcd(b, r). If r = 0 then gcd(a, b) = b.

Remark 3. Since the remainder strictly decreases, repeated application of the division algorithm, i.e. divide b by r etc., produces the gcd after at most b. divisions.

Proof Suppose b > 0; then the Division algorithm yields

$$a = bq + r$$

where $0 \leq r < b$. Since $r = a - bq$

any common divisor of a and b divides r and so is a common divisor of b and r.

Of course any common divisor of b and r also divides a and therefore is a common divisor of a and b.

Of course, if r = 0 then a = bq so b = gcd(a, b).

Euclidean Algorithm

Input: given integers $a \geq b \geq 0$, where if $b = 0$ then $a > 0$.

Output: gcd(a, b)

1. While $b \neq 0$ do
   1.1 Set $a \leftarrow b$, $b \leftarrow a \bmod b$
2. Return a

<u>Example 8.</u> Compute gcd (4864, 3458)

Step 1: $4864 = (1)(3458) + 1406$

Set $a = 3458$, $b = 1406$

Step 2: $3458 = (2)(1406) + 646$

Set $a = 1406$, $b = 646$

Step 3: $1406 = (2)(646) + 114$

Set $a = 646$, $b = 114$

Step 4: $646 = (5)(114) + 76$

Set $a = 114$, $b = 76$

Step 5: $114 = (1)(76) + 38$

Set $a = 76$, $b = 38$

Step 6: $76 = (2)(38) + 0$

Set $a = 38$, $b = 0$

Step 7: Since $b = 0$ return $\gcd(a, b) = 38$

Our second algorithm, the so-called Extended Euclidean algorithm, not only provides gcd(a, b) but also an expression

$$\gcd(a, b) = ax + by,$$

the existence of which is guaranteed by the previously obtained result

$$I = \{aw+bz \mid w, z \in Z\} = (\gcd(a, b)).$$

Since the Euclidean algorithm computes gcd(a, b) by repeated use of the Division Algorithm and culminates by declaring the LAST divisor to be the gcd, it is simply a matter of updating the expression for the remainder in terms of a and b at each application of the Division Algorithm.

More specifically, suppose r_1 , r_2 and r_3 are three successive remainders so that

$$r_1 = q_3\ r_2 + r_3$$

and suppose $r_1 = x_1\ a + y_1\ b$ and $r_2 = x_2\ a + y_2\ b$. Then

$$r_3 = r_1 - q_3\ r_2 = (x_1 - q_3\ x_2)\ a + (y_1 - q_3\ y_2)\ b$$

Hence the updating equations are given by

$$x_3 = x_1 - q_3\ x_2 \text{ and } y_3 = y_1 = q_3\ y_2$$

BUT HOW DO WE START? We require initial conditions such that

the FIRST $q_3 = \left\lfloor \frac{a}{b} \right\rfloor$, $r_3 = a - \left\lfloor \frac{a}{b} \right\rfloor b$, $x_3 = 1$ and $y_3 = -\left\lfloor \frac{a}{b} \right\rfloor$.

Thus we want

$$1 = x_1 - \left\lfloor \frac{a}{b} \right\rfloor x_2, \quad - \left\lfloor \frac{a}{b} \right\rfloor = y_1 - \left\lfloor \frac{a}{b} \right\rfloor y_2$$

Hence we <u>begin</u> with $x_1 = 1, x_2 = 0, y_1 = 0, y_2 = 1$.

<u>Extended Euclidean Algorithm</u>

Input: Given integers $a \geq b \geq 0$ or $a > b = 0$

Output: $d = \gcd(a, b)$ and $x, y \in Z$ such that $ax + by = d$.

1. If $b = 0$ then set $d \leftarrow a$, $x \leftarrow 1$, $y \leftarrow 0$ and return (d, x, y)
2. Set $x_1 \leftarrow 1$, $x_2 \leftarrow 0$, $y_1 \leftarrow 0$ and $y_2 \leftarrow 1$.
3. While $b > 0$ do the following:

   3.1 $q_3 \leftarrow \left\lfloor \frac{a}{b} \right\rfloor$, $r \leftarrow a\text{-}q_3 b$, $x_3 \leftarrow x_1 - q_3 x_2$ and $y_3 \leftarrow y_1 - q_3 y_2$

   3.2 $a \leftarrow b$, $b \leftarrow r$, $x_1 \leftarrow x_2$, $y_1 \leftarrow y_2$, $x_2 \leftarrow x_3$, $y_2 \leftarrow y_3$
4. Set $d \leftarrow a$, $x \leftarrow x_1$, $y \leftarrow y_1$ and return (d, x, y)

<u>Example 9.</u> Let a = 362 and b = 102. Then applying the algorithm we get

STEPS	q_3	r	x_3	y_3	a	b	x_2	x_1	y_2	y_1
2					362	102	0	1	1	0
	3.1				3.2					
1^{st} - 3	3	56	1	-3	102	56	1	0	-3	1
2^{nd} - 3	1	46	-1	4	56	46	-1	1	4	-3
3^{rd} - 3	1	10	2	-7	46	10	2	-1	-7	4
4^{th} - 3	4	6	-9	32	10	6	-9	2	32	-7
5^{th} – 3	1	4	11	-39	6	4	11	-9	-39	32
6^{th} - 3	1	2	-20	71	4	2	-20	11	71	-39
7^{th} - 3	2	0	51	-181	2	0	51	-20	-181	71

4. d = 2, x = -20, y = 71

<u>Exercise 6.</u> (Submit b; a is for extra credit) a) Given the following bit complexities $(a, b \geq 0)$

Operation	Bit complexity
Addition a + b	0 (lga +lgb) = 0 (lgn)
Subtraction a – b	0 (lga + lgb) = 0 (lgn)
Multiplication a, b	$0 ((lga)(lgb)) = 0 ((lgn)^2)$
Division a = qb + r	$0 ((lga)(lgb)) = 0 ((lgn)^2)$

where n = max (a, b)

Show that both algorithms have running time $0((lgn)^2)$ bit operations.

b) Find gcd (1819, 3587) and $x, y \in Z$ such that

$$1819\,x + 3587\,y = \gcd(1819, 3587)$$

c) Find values of x, y, and z such that

$$6x + 10y + 15z = 1$$

d) i) Find lcm (482, 1687)

ii) Find lcm (60, 61)

In the following discussion, it is revealed that the prime numbers constitute the "multiplicative" building blocks of $Z^+ - \{1\}$.

Theorem 6. $\forall\ n \in Z^* \big($if $n \geq 2$ then n is a prime number or a product of prime numbers$\big)$
Proof (by induction on n.)
base case: $n = 2$. But 2 is prime.
Induction hypothesis: Given $2 \leq k \leq n$, k is prime or a product of primes.
Induction step: Consider $n + 1$ and suppose it is NOT prime. Then
$\exists\ a \in Z^+$ such that $a \neq 1$ and $a \neq n + 1$ and $a \mid n + 1$. Hence $\exists\ b \in Z^+$ such that
$n + 1 = a\,b$. Of course $b \neq 1$ and $b \neq n+1$ (or else $a = n + 1$ or $a = 1$ respectively).
Thus $2 \leq a, b \leq n$, so by the induction hypothesis, both a and b are either prime numbers or a product of prime numbers. Hence $n + 1 = a\,b$ is product of primes numbers.

Corollary 6.1 $\forall\ n \geq 2\ \exists$ primes numbers $p_1, p_2, \ldots, p_k$ and $m_1, \ldots, m_k \in Z^+$
such that $n = p_1^{m_1}\ p_2^{m_2} \cdots p_k^{m_k}$

Proof Since n is prime or a product of primes let $\{p_1, p_2, \ldots, p_k\}$ be the set of prime numbers in the "product" ($k = 1$ when n is prime). Next let m_1 = the number of times p_i appears in the product. Then, by commutativity and associativity, the result follows.

Next we establish "uniqueness" of this representation.

Theorem 7. The set $\{p_1, \ldots, p_k\}$ and the corresponding m_i's are unique.

Proof Suppose not; i.e. $\exists\{q_1, \ldots, q_\ell\}$ - prime numbers and corresponding non-negative integers $n_1, \ldots, n_\ell$ such that either $\{q_1, \ldots, q_\ell\} \neq \{p_1, \ldots, p_k\}$ or $\{q_1, \ldots, q_\ell\} = \{p_1, \ldots, p_k\}$, say $\ell = k$ and $q_i = p_i$ $i = 1, \ldots, k$), and $\exists$ i such that $m_i \neq n_i$.

Claim If $q \notin \{p_1, \ldots, p_k\}$ then $q \chi\ p_1^{m_1} \ldots p_k^{m_k}$ (where q is prime).
Proof (induction on $m_1 + \cdot + m_k$)

Suppose $m_1 + \cdot + m_k = 1$ so that $m_1 = 1,\ k = 1$

Now $q \neq p_1$ implies $q \chi p_1$.

Induction hypothesis If $m_1 + \cdot\cdot + m_k = t > 1$ then $q \chi p_1^{m_1} \cdots p_k^{m_k}$

Induction step Suppose $m_1 + \cdot\cdot + m_k = t + 1 \geq 2$. Then assume

$q \left| p_1^{m_1} \cdots p_k^{m_k} \right.$. But then $q \left| (p_1)(p_1^{m_1 - 1} \cdots p_k^{m_k}) \right.$

Since gcd $(q, p_1) = 1$ it follows that $q \left| p_1^{m_1 - 1} \cdots p_k^{m_k} \right.$

But

$m_1 - 1 + m_2 + \cdot\cdot + m_k = t$

so this is a contradiction.

Hence $\ell = k$ and we may assume $q_i = p_i \quad i = 1, \ldots, k$. Now

$$p_1^{m_1}\, p_2^{m_2} \cdots p_k^{m_k} = p_1^{n_1}\, p_2^{n_2} \cdots p_k^{n_k}.$$

Suppose i is the smallest index such that $m_i \neq n_i$ and assume without loss of generality that $m_i > n_i$. If $i > 1$ then it follows by cancellation $p_i^{m_i} \cdot\cdot p_k^{m_k} = p_i^{n_i} \cdots p_k^{n_k}$.

If $i = 1$ this is still true. Again by cancellation we get

$$p_i^{m_i - n_i} p_{i+1}^{m_{i+1}} \cdots p^{m_k} = p_{i+1}^{n_{i+1}} \cdots p_k^{n_k} \quad \text{if } i < k$$

or

$$p^{m_i - n_i} = 1 \quad \text{if} \quad i = k$$

In the first case $p_i \left| p_{i+1}^{n_{i+1}} \cdots p_k^{n_k} \right.$ - a contradiction. The seconds yields a more absurd contradiction

Example 10. $180 = 2^2\ 3^2\ 5^1$

Remark 4. This factorization result is called the fundamental theorem of arithmetic.

Corollary 7.1 (of the claim) If $a > 0$, p is prime, $t > 0$ and $p^t \left| a \right.$ then p appearsin the factorization of a to a power m such that $t \leq m$.

Proof Exercise 7

Corollary 7.2 If a, b $\in Z^+$ and we write

$$a = p_1^{e_1}\ p_2^{e_2}\cdots p_k^{e_k}\ ,\quad \text{each } e_i \geq 0$$
$$b = p_1^{f_1}\ p_2^{f_2}\cdots p_k^{f_k}\ ,\quad \text{each } f_i \geq 0$$

then

$$\gcd(a, b) = p_1^{\min(e_1,f_1)}\ p_2^{\min(e_2,f_2)}\cdots p_k^{\min(e_k,f_k)}$$

and $\quad \operatorname{lcm}(a, b) = p_1^{\max(e_1,f_i)} p_2^{\max(e_2,f_2)}\cdots p_k^{\max(e_k,f_k)}$

Proof By the previous corollary, if $\gcd(a, b) = q_1^{z_1}\cdots q_\ell^{z_\ell}$, $z_i > 0$

then each q_i is a prime division of a and of b. Futhermore with $\{p_1,\ p_2,...,\ p_k\}$ equal to the union of the prime divisors of a and b, if $p_j = q_i$ then $z_i \leq\ e_j, f_j$, i.e $z_i \leq\ \min(e_j,\ f_j)$. Hence $\gcd(a, b) = p_1^{\alpha_1} p_2^{\alpha_2}\cdot\cdot p_k^{\alpha_k}$

where $\alpha_i \leq \min(e_i,\ f_i)$

But $p_1^{\min(e_1,f_1)}\ p_2^{\min(e_2,\ f_2)}\cdots p_k^{\min(e_k,f_k)} \,|\, a, b$

(WHY?)

so $\gcd(a, b) = p_1^{\min(e_1,\ f_1)}\cdots p_k^{\min(e_k,\ f_k)}$

Next set

$$\ell\text{cm}(a, b) = p_1^{\beta_1}\ p_2^{\beta_2}\cdots\ p_k^{\beta_k}\ c,\ \ \beta_i > 0, c \geq 1$$

since, by the previous corollary each p_i $i = 1,..., k$ must be in the fatorization for ℓcm(a, b). Again by the previous corollary each $\beta_i \geq\ e_i,\ f_i$ (so $\beta_i \geq \max(e_i, f_i)$)

Furthermore,

$$a, b \,\Big|\, p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)}\cdots p_k^{\max(e_k,f_k)}$$

(WHY?)

so

$$\ell\text{cm}(a, b) = \prod_{i=1}^{k}\ p_i^{\max(e_1,f_i)}$$

Remark 5. Use of this result trivializes Exercises 4 and 5.

Example 11. If $a = 24 = 2^3 \cdot 3^1$ and $b = 36 = 2^2\ 3^2$ then

$$\gcd(24, 36) = 2^2\ 3^1 = 12$$

and

$$\ell\text{cm}(24, 36) = 2^3 \cdot\ 3^2 = 72$$

Next we study a function defined on Z^+ which plays an important role in the study of "residue systems" - a topic of concern in the study of cryptography.

<u>Definition</u> (Euler phi function; Euler totient function)

$$\varphi(n) \underline{\underline{\Delta}} \left|\{m \in [n] \,|\, \gcd(m, n) = 1\}\right| \text{ , } n \geq 1.$$

We derive some of the properties of $\varphi(n)$, the first of which is trivial:

(p1) $\forall$ primes p ($\varphi(p) = p - 1$)

The next one is a generalization of p1.

(p2) $\forall$ primes p and $e \geq 1$ ($\varphi(p^e) = p^e(1 - \frac{1}{p})$)

<u>Proof</u> Observe that for $k \in [p^e]$

$$\gcd(k, p^e) > 1 \Leftrightarrow \quad k = pm \text{ such that } 1 \leq m \leq p^{c-1}$$

Thus

$$\left|\{k \in [p^e] \,|\, \gcd(k, p^e) > 1\}\right| = p^{e-1}$$

so

$$\varphi(p^e) = p^e - p^{e-1} = p^e(1 - \frac{1}{p}).$$

Next we prove that φ is "multiplicative".

(p3) $\forall$ m, n $\in Z^+$ ($\gcd(m,n) = 1 \Rightarrow \varphi(mn) = \varphi(m) \ \varphi(n)$)

<u>Proof</u> Let $E(t) = \{s \in [t] \,|\, \gcd(s, t) = 1\}$. We obtain the result by proving that $\exists$ a bijection between E (nm) and E(n) X E(m). Consider $x \in E(nm)$. Then there exists unique

$$r_n, r_m \text{ such that } 1 \leq r_n \leq n \quad , \quad 1 \leq r_m \leq m$$

and

$$x = q_n\, n + r_n = q_m\, m + r_m.$$

(<u>Proof</u> <u>Exercise 8</u> - use the Division Algorithm)

Since gcd (x, n m) = 1, we get gcd(x,n) = gcd (x, m) = 1. Thus $r_n \in E(n)$, $r_m \in E(m)$.

Consider the following mapping:

$$f: E(nm) \rightarrow E(n) \times E(m)$$

$$x \rightarrow f(x) \underline{\underline{\Delta}} (r_n, r_m)$$

The following claim establishes bijectivity:

<u>Claim</u> $\forall$ (s, t) $\in$ E(n) x E(m) $\exists$ a unique x $\in$ E(nm)

such that

$$x = q_n\ n + s = q_m\ m + t$$

<u>Proof</u> First we prove the existence of x. Since gcd(n, m) = 1 $\exists\ \alpha, \beta \in$ Z such that

$$\alpha n + \beta m = 1$$

Thus

$$[\alpha(t - s)]\ n + [\beta\ (t-s)]\ m = t - s$$

so $\exists\ q_1, q_2 \in$ Z such that $q_1\ n + q_2 m = t - s$

or

$$q_1\ n + s = (-\ q_2)\ m + t$$

By the division algorithm $\exists\, \eta, r_1$ such that $q_1 = \eta\ m + r_1$ where

$0 \leq r_1 \leq m - 1$

Hence

$$x\ \underline{\underline{\Delta}}\ r_1\ n + s = (q_1 - \eta m)\ n + s = (q_2 - \eta n)\ m + t$$

Clearly

$$1 \leq x \leq (m - 1)\ n + n = mn$$

Also gcd(n, s) = 1 forces gcd (x, n) = 1. Likewise

gcd(x, m) = 1. Hence gcd(x, nm) = 1 as well and x $\in$ E(nm).

As for uniqueness suppose $\exists$ x, $x' \in$ E(nm) such that

$$x = q_n\, n + s = q_m\, m + t$$

and

$$x' = q'_n\, n + s = q'_m\, m + t$$

Then assuming $x > x'$, we get

$$0 < \left(q_n - q'_n\right) n = \left(q_m - q'_m\right) m$$

But then $m \,\Big|\, \left(q_n - q'_n\right) n$; and as gcd(m. n) = 1

$$m \,\big|\, q_n - q'_n$$

i.e $\quad m\,n \,\Big|\, (q_n - q'_n)n$ and $0 < \left(q_n - q'_n\right) n = x - x' < nm$

This contradiction forces $x = x'$.

<u>Remark 6</u> The previous claim is a special case of the Chinese Remainder theorem; a theorem we shall prove in short order.

Finally we obtain the next property by induction

(p4) $\forall n \ge z$ (if $n = p_1^{e_1} \cdots p_k^{e_k}$ then $\varphi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i^e})$)

The conclusion follows from the induction hypothesis and p_2.

<u>Exercise 9</u>. (Submit a) a) Prove (p4) directly using inclusion-exclusion

Hint: With $n = p_1^{e_1}\, p_2^{e_2} \cdots p_k^{e_k}$ set

$$A_i = \left\{ m \in [n] \;\big|\; p_i \mid m \right\}$$

Then

$$E\,(n) = \bigcap_{i=1}^{k} A_i^c$$

b) Using (p4) obtain p_2 and p_3

c) Find $\varphi(n)$ for $n \in \lceil 12 \rceil$