Progressive Education Society's
Modern College of Arts, Science and Commerce(Autonomuous), Shivajinagar, Pune-5
Department of Mathematics
M.Sc.(Mathematics) Part-II
Subject: Number Theory
Prof. Smita Gajul

Chapter 1: Divisibility

Divisibility

Definition: An integer b is divisible by an integer a, not zero, if there is an integer x such that $b = ax$.
Notation: $a|b$

Theorem:

1. If $a|b$ then $a|bc$ for any integer c.
Proof: Suppose $a|b$ so by definition there exists x such that $b = ax$
multiply by c on both side we get $bc = axc$ say $xc = y \Rightarrow bc = ay \Rightarrow a|bc$.

2. If $a|b$ and $b|c$ then $a|c$.
Proof: Suppose $a|b \Rightarrow b = ax$ and $b|c \Rightarrow c = by$
Consider $c = by \Rightarrow c = axy = az$, where $z = xy$ so $a|c$.

3. If $a|b$ and $a|c$ then $a|bx + cy$ for any integers x and y.
Proof: Suppose $a|b \Rightarrow b = am$ and $a|c \Rightarrow c = an$
Multiply first equation by x and second by y we have
$bx = amx$ and $cy = any$ after adding we get
$bx + cy = amx + any \Rightarrow bx + cy = a(mx + ny)$.
say $mx + ny = z \Rightarrow bx + cy = az \Rightarrow a|bx + cy$.

4. If $a|b$ and $b|a$ then $a = \pm b$.
Proof: Suppose $a|b \Rightarrow b = ax$ and $b|a \Rightarrow a = by$
Consider $b = ax \Rightarrow b = byx \Rightarrow 1 = yx \Rightarrow y = x = 1$ or $y = x = -1$
Therefore $a = \pm b$

5. If $a|b, a > 0, b > 0$, then $a \leq b$.
Proof: Suppose $a|b \Rightarrow b = ax$ for $x \in Z$
since $a > 0, b > 0$ so $x > 0$, As $b = ax$ so $b \leq a$.

6. If $m \neq 0, a|b$ then $ma|mb$.
Proof: Suppose $a|b \Rightarrow b = ax$ now multiply by m on both side
we get $mb = max \Rightarrow ma|mb$.

Division algorithm: Given any integers a and b, with $a > 0$, there exist unique integers
q and r such that $b = aq + r$ where $0 \leq r < a$.
If a is not divisible by b, then r satisfies a stronger inequalities $0 < r < a$.

Common divisor: The integer a is called a common divisor of b and c if $a|b$ and $a|c$.

Note: Since there is only finite number of divisors of any nonzero integers, so there is only finite number of common divisors of b and c, except in the case $b = c = 0$.

Greatest Common divisor: the greatest among all common divisors of b and c is called greatest common divisor of b and c.
Notation: (b, c).
Note: The greatest common divisor (b, c) is defined for every pair of integers b, c excpet $b = c = 0$ so $(b, c) \geq 1$.

Theorem: If g is greatest common divisor of b and c, then there exist integers x_0 and y_0 such that $g = (b, c) = bx_0 + cy_0$.

Proof: Consider the linear combinations $bx + cy$, where $x, y \in Z$
That is $A = \{bx + cy | x, y \in Z\}$ so this set contains positive, negative values and also 0.
Choose x_0, y_0 so that $bx_0 + cy_0$ is the least positive integer say $l = bx_0 + cy_0$
To prove $l = g$
Suppose l does not divides b so there exist integers q and r such that $b = lq + r$ with $0 < r < l$ so we have $r = b - lq = b - q(bx_0 + cy_0) = b(1 - qx_0) + c(-qy_0)$ so $r \in A$ but $r < l$ which is contradiction to the choice of l so l divides b.
Similarly we can prove that l divides c so l is common multiple of b and c.
Since g is greatest common divisor of b and c so $b = gx$ and $c = gy$
As $l = bx_0 + cy_0 = gxx_0 + cyy_0 = g(xx_0 + yy_0) = gz$, where $z = xx_{0+yy_0}$.
So $g|l \Rightarrow g \leq l$ but since g is greatest common divisor and l is common divisor so $g < l$ is not posiible therefore $g = l = bx_0 + cy_0$.

Note:

I. We can generlize the theorem as for given integers $b_1, b_2, ...b_n$ not all zero, with greatest common divisor g , there exist $x_1, x_2, ...x_n$ such that
$g = (b_1, b_2, ...b_n) = \sum_{j=1}^{n} b_j x_j$
II. The greatest common divisor g of b and c can be characterized in the following two ways:
1. It is the least positive value of $bx + cy$, where $x, y \in Z$.
2. It is the positive common divisor of b and c that is divisible by every common divisor.

Theorem: For any positive integer m, $(ma, mb) = m(a, b)$.
Proof: Since $(ma, mb) =$ least positive value of $max + mby$
$= m$. least positive value of $ax + by$ $=m(a, b)$

Theorem: If $d|a$ and $d|b$and $d > 0$, then $(\frac{a}{d}, \frac{b}{d}) = \frac{1}{d}(a, b)$
If $(a, b) = g$, then $(\frac{a}{g}, \frac{b}{g}) = 1$
Proof: Since $(ma, mb) = m(a, b)$ so here $m = d, a = a/d, b = b/d$
So we have $(a, b) = (d\frac{a}{d}, d\frac{b}{d}) = d(\frac{a}{d}, \frac{b}{d}) \Rightarrow (\frac{a}{d}, \frac{b}{d}) = \frac{1}{d}(a, b)$
Since $(\frac{a}{g}, \frac{b}{g}) = \frac{1}{g}(a, b) \Rightarrow (\frac{a}{g}, \frac{b}{g}) = \frac{1}{g}.g = 1$

Theorem: If $(a,m)=(b,m)=1$, then $(ab,m)=1$.
Proof: Suppose $(a,m)=(b,m)=1$ so there exists x_0, y_0, x_1, y_1 such that
$ax_0+my_0=1$ and $bx_1+my_1=1$
So we have $ax_0+by_0=bx_1+my_1$ and $ax_0=1-my_0$ and $bx_1=1-my_1$
So that $ax_0bx_1=(1-my_0)(1-my_1)=1-my_1-my_0+m^2y_0y_1=1-my_2$,
where $y_2=y_0+y_1-my_0y_1$
$abx_0x_1+my_2=1$
If $g|ab$ and $g|m$ so $g|abx_0x_1+my_2 \Rightarrow g|1$
so any common divisor of ab and m divides 1 and $1|g$
therefore $g=1$ that is $(ab,m)=1$.

Relatively Prime:
Definition: An integers a and b are said to be relatively prime if $(a,b)=1$.
An integers $a_1, a_2, ..., a_n$ are said to be relatively prime if $(a_1, a_2, ..., a_n)=1$.
An integers $a_1, a_2, ..., a_n$ are said to be relatively prime in pairs if $(a_i, a_j)=1$ for all $i=1,2,...,n$ and $j=1,2,...,n$ with $i \neq j$.

Theorem: For any integer x, $(a,b)=(b,a)=(a,-b)=(a,b+ax)$.
Proof: Let $(a,b)=g$ so $g|a$ and $g|b$ such that g is greatest common divisor of a and b So we can say that $(b,a)=g$
And as $g|b$ so $g|-b$ so g is common divisor of a and $-b$.
If suppose h is another common divisor of a and $-b$ so $h|b$
that is h is common divisor of a and b also.
but $(a,b)=g$ so that $h|g$ so any common divisor of a and $-b$ divides g
so g is greatest common divisor of a and $-b$ therefore $(a,-b)=g=(a,b)$.
Now suppose $(a,b)=g$ and $(a,b+ax)=d$
So there exists x_0 and y_0 such that
$g=ax_0+by_0 \Rightarrow g=ax_0-axy_0+by_0+axy_0 \Rightarrow g=a(x_0-xy_0)+(b+ax)y_0$.
Since $(a,b+ax)=d$ so d is the least positive value of linear combination of a and $b+ax$ so $d|g$
Since $(a,b)=g \Rightarrow g|a$ and $g|b$ so $g|b+ax$
so g is a common divisor of a and $b+ax$ therefore $g|d$
hence $g=d$.

Theorem: If $c|ab$ and $(b,c)=1$, then $c|a$.
Proof: Since $(ab,ac)=a(b,c)=a$ as $(b,c)=1$
Since $c|ab$ and $c|ac$ so c is common divisor of ab and ac so $c|(ab,ac) \Rightarrow c|a$.

The Euclidean algorithm:
For integers b and c if we apply division algorithm repetedly
we get series of equations

$$
\begin{gathered}
b=cq_1+r_1, \quad 0<r_1<c, \\
c=cq_2+r_2, \quad 0<r_2<r_1, \\
r_1=r_2q_3+r_3, \quad 0<r_3<r_2, \\
\dots \\
r_{j-2}=r_{j-1}q_j+r_j, \quad 0<r_j<r_{j-1}, \\
r_{j-1}=r_jq_{j+1}
\end{gathered}
$$

The greatest common divisor (b,c) of b and c is r_j, the last nonzero remainder in the division process. Values of x_0 and y_0 in $(b,c)=bx_0+cy_0$ can be obtained by writing each r_i as a linear combination of b and c.

Proof: We can obtained the chain of equations by dividing c into b, r_1 into c, r_2 into r_1,...,r_j into r_{j-1}. This process stops when the remainder is zero.
To prove r_j is the greatest common divisor g of b and c.
Since $(b, c) = (b - cq_1, c) = (r_1, c) = (r_1, c - r_1q_2) = (r_1, r_2) = (r_1 - r_2q_3, r_2) = (r_3, r_2)$.
Continuing in this way $(b, c) = (r_{j-1}, r_j) = (r_j, 0) = r_j$
If we continue by substiting value r_j then r_{j-1} and so on
we get r_j as a linear combination of b and c.

Least Common Multiple:
The nonzero integers $a_1, a_2, ..., a_n$ have a common multiple b if $a_i|b$ for $i = 1, 2, ..., n$.
The least among all positive common multiples is called least common multiple.
Notation: $[a_1, a_2, ..., a_n]$.

Theorem: If m is any common multiple of $a_1, a_2, ..., a_n$, then $[a_1, a_2, ..., a_n]|m$
Proof: Let $a_1, a_2, ..., a_n$ be integers and $h = [a_1, a_2, ..., a_n]$.
Suppose m is common multiple of $a_1, a_2, ..., a_n$.
Apply division algorithm to m and h, there exists q and r such that $m = qh + r$, $0 \leq r < h$.
To prove: $r = 0$
Suppose $r \neq 0$, Since $a_i|h$ and $a_i|m$ for all $i = 1, 2, ..., n$
so $a_i|qh \Rightarrow a_i|m - qh \Rightarrow a_i|r$.
So r is positive common multiple of a_i and $r < h$,
which is contradiction to the fact that h is least common multiple of a_i
so $r = 0$, therefore $[a_1, a_2, ..., a_n]|m$.

Theorem: If $m > 0$, $[ma, mb] = m[a, b]$. Also $[a, b](a, b) = |ab|$.
Proof: Let $H = [ma, mb]$ and $h = [a, b]$. So $a|h$ and $b|h \Rightarrow ma|mh$ and $mb|mh$
so mh is a common multiple of ma and mb but H is least common multiple of ma and mb
so $H|mh$. Now as $ma|H$ and $mb|H$ So $a|H/m$ and $b|H/m$
So H/m is common multiple of a and b but h is least common multiple of a and b
so $h|H/m \Rightarrow mh|H$. Therefore $H = mh$.
Now to prove: $[a, b](a, b) = |ab|$. It is sufficient to prove that $[a, b] = [a, -b]$ and $(a, b) = (a, -b)$.
Case-I: $(a, b) = 1$, Since $[a, b]$ is a multiple of a say ma. Then $b|ma$ and $(a, b) = 1$
so $b|m \Rightarrow ba|ma$. Since $a|ba$ and $b|ba$ So ba is common multiple of a and b
but ma is least common muliple of a and b so $ma|ba \Rightarrow ba = ma = [a, b]$.
Case-II: $(a, b) = g > 1$ so we have $(\frac{a}{g}, \frac{b}{g}) = 1$
If we apply the above result we have $[\frac{a}{g}, \frac{b}{g}](\frac{a}{g}, \frac{b}{g}) = \frac{a}{g}.\frac{b}{g}$.
Multiply by g^2 on both side we get $[a, b](a, b) = ab$.

Primes:

Definition: An integer $p > 1$ is called a prime number, if there is no divisor d of p satisfying $1 < d < p$. If an integer $a > 1$ is not a prime, it is called composite number.

Theorem: Every integer $n > 1$ can be expressed as a product of primes.
Proof: Let n be an integer.
If n is prime then n itself a product of prime.
If not, then $n = n_1 n_2$, where $1 < n_1, n_2 < n$
If n_1 and n_2 both are primes then done.
If n_1 is not a prime then $n_1 = n_3 n_4$, where $1 < n_3, n_4 < n_2$
If n_3, n_4 both are primes then $n = n_3 n_4 n_2$ which is product of primes.
Continuing in this way we have $n = p_1 p_2 ... p_k$ and
since primes are not necessarily distinct so we have $n = p_1^{\alpha_1} p_2^{\alpha^2} ... p_k^{\alpha^k}$
This representation of n as a product of primes is called
the canonical factoring of n into prime powers.

Theorem: If $p|ab$ then $p|a$ or $p|b$.
Generally, if $p|a_1 a_2 ... a_n$, then p divides at least one factor a_i of the product.
Proof: Let $p|ab$ and p does not divides a then $(p, a) = 1$
since we have $a|bc$ and $(a, b) = 1$ then $a|c$ so here $p|b$.
In general if $p|a_1 a_2 ... a_n$ that is $p|a_1 c$ where $c = a_2 ... a_n$
then $p|a_1$ or $p|c$. If $p|c$ then continue the same procedure so we have $p|a_i$ for some i.

Fundamental Theorem of Arithmetic / Uniqe Factorization Theorem:
The factoring of any integer $n > 1$ into primes is unique apart from the order of primes.
Proof: Since every integer can be written as product of primes.
To show: This factorization is unique.
Suppose we have two factorization of n say
$n = p_1 p_2 ... p_r$ and $n = q_1 q_2 ... q_s$
So we have $p_1 p_2 ... p_r = q_1 q_2 ... q_s$ Since $p_1 | p_1 p_2 ... p_r \Rightarrow p_1 | q_1 q_2 ... q_s$
and p_1 is prime,so $p_1 | q_j$ for some $j = 1, 2, ... s$ say $p_1 | q_1$ as both are primes $p_1 = q_1$
Similarly $p_2 | q_2 \Rightarrow p_2 = q_2$ continuing in this way we have
$p_i = q_j$ for all $i = 1, 2, ... r$ and $j = 1, 2, ..., s$

Theorem: The number of primes are infinite.
Proof: Suppose number of primes are finite say $p_1, p_2, ..., p_r$
Consider $n = 1 + p_1 p_2 .... p_r$, since n is not divisible by any of above primes.
Hence any prime divisor p of n is a rime distinct from $p_1, p_2, ..., p_r$.
Since n is either a prime or has a prime factor p
so there is a prime distinct from $p_1, p_2, ..., p_r$
Therefore number of primes is not exactly r that is primes are infinite.