Date: / /

Divisibility Theory

Divisibility :- An integer a is said to be divisible by an integer $b(\neq 0)$ if there exits an integer q such that $a = bq$
denoted by $b|a$
we can also say that a is a multiple of b
ex - 45 is divisible by 15 as $45 = 15 \times 3$,
$a \quad b$

Thus $15|45$.
If b divides a then $-b$ also divides a
because $a = bq = (-b)\cdot(-q)$
we also have
(i) $a|0$, $1|a$ and $a|a$
(ii) $a|b$ and $c|d \Rightarrow ac|bd$
(iii) $a|b$ and $b|c \Rightarrow a|c$ (Transitivity)
(iv) $a|b$ and $b|a \Rightarrow a = \pm b$
(v) $a|b$ and $a|c \Rightarrow a|bx+cy$ $\forall$ integers x, y

Thm 1 :- If $c = ax+by$ and $d|a$ but $d \nmid c$ then $d \nmid b$

Proof :- we have
$d|a \Rightarrow \exists$ an integer q_1 such that
$a = dq_1$
Therefore $c = ax+by = dq_1x + by$
Also $d|b \Rightarrow \exists$ an int q_2 such that
$b = dq_2$
$\Rightarrow c = dq_1x + dq_2y$
$= d(q_1x + q_2y) \Rightarrow d|c$.
Hence $d \nmid c \Rightarrow d \nmid b$

H.W. **The 2 :-** If integer b divides a positive integer a then b is not numerically greater than a

Proof :- We have

$b|a \Rightarrow \exists$ an integer q such that $a = bq$

also $a = |a| = |bq|$

$= |b||q| \geq |b|$

H.W. **Division Algorithm :-** For given integer a and $b > 0$, there exist unique integer q and r such that

The 1 :- $a = bq + r \quad ; 0 \leq r < b$

q and r are called quotient and remainder → remainder

The 2 :- For any integer $a \geq b > 0$, $\exists$ q_1, r_1 Do yourself : $a = bq_1 + cr_1$, $0 \leq r_1 < b/2$, $c = \pm 1$ or -1

Only Statement

The 3 :- Every integer is of the form

(i) $3q$ or $(3q \pm 1)$

(ii) $4q$, $(4q \pm 1)$ or $(4q \pm 2)$

(iii) $5q$, $(5q \pm 1)$ or $(5q \pm 2)$

(i) Let 'a' be an integer

we know that $a_1 = bq_1 + cr_1$ — (1)

Putting $b = 3$ in (1) above we get

$a = 3q_1 + cr_1$, $0 \leq r_1 < \frac{3}{2}$, $c = \pm 1$

it means $r_1 = 0$ or 1, we have

$a = 3q$ or $3q \pm 1$

Similarly (ii) & (iii)