Assignment: Number Theory theorems - Part 1

1. Bezout Theorem Proof and Example

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

Proof: Let, $a,b \in \mathbb{Z}$, not both zero, so

$$S = \{ax+by \mid x, y \in \mathbb{Z}, ax+by > 0\}$$

Hence not both zero, and it consists of positive integers. & smallest positive integer in S call it d,

so $d = ax_0 + by_0$. ——— (1)

Now we want to show that

$d = \gcd(a,b)$.

Let $r = a \mod d$

$\therefore a = qd + r$

$\Rightarrow r = a - qd$

then

$r = a - d(ax_0 + by_0)$ —— from (i)

$= a(1 - qx_0) + b(-qy_0)$

So r is also in the set S, but if $r > 0$, then $r < d$, contradicting the minimality of d, So $r = 0$, ie. $d \mid a$. Similarly, $d \mid b$, so d is a common divisor.

Now suppose c is another common divisor of a and b, then $c \mid ax_0 + by_0 = d$.

So d is the greatest common divisor

Hence, $\gcd(a, b) = d = ax_0 + by_0$

(proved).

Example:

Inverse of 101 mod 9620

Here $101x \equiv 1 \mod 9620$

we have to find out x which is inverse of this mode.

Here if $x = 1601$ then

$$9620 \,\big|\, \begin{array}{r} 161701 \\ 161700 \\ \hline 1 \leftarrow x \end{array} \,\big|\, 35$$

So Inverse is 1601 Ans: