Q. Show that if $a | b$ and $b | a$, where a and b are integers, then $a = b$ or $a = -b$.

Solution: Given conditions imply that there are integers 's' and 't' such that

$$a = bs \quad \text{and} \quad b = at$$

Combining these two we get,

$$a = ats$$

Since $a \neq 0$, we conclude $st = 1$.

Now, only way this would happen is when $s = t = 1$

or

$$s = t = -1$$

Therefore either $a = b$ or $a = -b$

Q/ Show that if a, b and c are integers, where $a \neq 0$ and $c \neq 0$ such that $ac \mid bc$, then $a \mid b$

Solution: This implies that $bc = t(ac)$ for some integer 't'.

Since $c \neq 0$, we divide both sides by 'c'.

$$\boxed{b = at}$$

This is the definition of $a \mid b$, as desired.

Q Suppose a and b are integers

$a \equiv 4 \pmod{13}$ and $b \equiv 9 \pmod{13}$.

Find integer c with $0 \leq c \leq 12$ such that:

a) $c \equiv 9a \pmod{13}$

b) $c \equiv 11b \pmod{13}$

c) $c \equiv a+b \pmod{13}$

d) $c \equiv 2a+3b \pmod{13}$

e) $c \equiv a^2+b^2 \pmod{13}$

f) $c \equiv a^3-b^3 \pmod{13}$

a) 10 b) 8 c) 0 d) 9

e) 6 f) $-665 \bmod 13 \Rightarrow 11$

because $(-665 = -52 \cdot 13 + 11)$

Remainder cannot be '-ve'.

Q. **Find**

a) $-17 \bmod 2$

b) $144 \bmod 7$

c) $-101 \bmod 13$

d) $199 \bmod 19$

a) 1 b) 4 c) 3 d) 9

Q Find

a) $(19^2 \bmod 41) \bmod 9$

b) $(32^3 \bmod 13)^2 \bmod 11$

c) $(7^3 \bmod 23)^2 \bmod 31$

d) $(21^2 \bmod 15)^3 \bmod 22$

a) 6 b) 9 c) 7 d) 18

Q Use extended Euclidean algorithm to express $\gcd(26, 91)$ as a linear combination of 26 and 91.

Solution

By applying Euclidean we obtain following quotients & remainders

$q_1 = 0$, $r_2 = 26$, $q_2 = 3$, $r_3 = 13$, $q_3 = 2$. Note that $n = 3$. Thus we compute the successive s's and t's as follows, using given recurrences.

$s_2 = s_0 - q_1 s_1 = 1 - 0.0 = 1$

$t_2 = t_0 - q_1 t_1 = 0 - 0.1 = 0$

$s_3 = s_1 - q_2 s_2 = 0 - 3.1 = -3$

$t_3 = t_1 - q_2 t_2 = 1 - 3.0 = 1$

Thus we have $s_3 a + t_3 b = (-3).26 + 1.91$

which is the gcd of $(26, 91) \Longrightarrow 13$