* what will be the quotient and reminder when 101 is divided by

we have,

$$101 = 11 \cdot 9 + 2$$

$11 \,|\, 101 \,|\, 9$, 99, 2

Hence the quotient is 9 when 101 is devided by 11 $\therefore 9 = 101$ divide 11

and reminder $= 2$. when 101 mod 11.

* what are the quotient and reminder when -11 is devided by 3?

we have

$$-11 = 3(-4) + 1.$$

$3 \,|\, -11 \,|\, -4$, -12, 1

$\therefore$ qoutent $= -4$ and remider $= 1$.

* Ex-9.4 (9) what are the quotient and reminder of given problem.

a) 19 is devided by 7

$7 \,|\, 19 \,|\, 2$, 14, 5

$19 = 7 \cdot 2 + 5 \quad \therefore q = 2, \ r = 5.$

(b) -111 is divided by 11?

$$-111 = 11(-11) + 10$$

$11 \,|\, -111 \,|\, -11$, -121, 10

$\therefore q = -11, \ r = 10.$

(c) 789 is divided by 23

$23 \,|\, 789 \,)\, 34$, 69, 99, 92, 7

~~789 = 23 · 7 +~~

$789 = 23 \cdot 34 + 7$

$q = 34, \ r = 7.$

(d) 1001 is divided by 13

$13 \,|\, 1001 \,|\, 77$, 91, 91, 95, 6

$1001 = 13 \cdot 75 + 6$

$q = \cancel{77}, \ r = 6$

(e) 0 is devided by 19

$19 \,|\, 0 \,|\, 0$, 0, 0

$0 = 19 \cdot 0 + 0$

* Let a, b and c be integers. Then

1. If $a|b$ and $a|c$, then $a|(b+c)$

Let K_1 and K_2 are integers.

$\therefore a|b = K_1$ $\quad a|c = K_2$

$\therefore b = aK_1$ — (i) $\quad c = aK_2$ — (ii)

(i) + (ii) এর থেকে,

$b+c = a(K_1+K_2)$

$\therefore a|(b+c)$ proved

2. If $a|b$, then $a|bc$ for all integers c.

Let, K be a integer.

$a|b = K$

$b = aK$

$\Rightarrow bc = a(cK)$

$\Rightarrow bc = a \times S$

$\boxed{\therefore a|bc}$ proved

3. If $a|b$ and $b|c$, then $a|c$

Let, s and t be 2 integers.

$a|b = s$ $\quad b|c = t$

$\Rightarrow b = as$ — (i) $\quad \Rightarrow c = bt$.

$\Rightarrow c = ast$

$\Rightarrow c = a \times K$

$\boxed{\therefore a|c}$ proved

* If a, b and c are integers such that $a|b$ and $a|c$, ~~a|mb and a|n~~ : $a|mb+nc$ whenever m and n are integers two.

Let s and t be integers.

$a|b$

so, $b = as$ — (i)

$\Rightarrow mb = mas$

$\Rightarrow mb = a(ms)$ — (1)

again,

$a|c$

so, $c = at$

$\Rightarrow nc = ant$

$\Rightarrow nc = a \times (nt)$ — (11)

(1) + (11) নং সমীকরণ হতে পাই

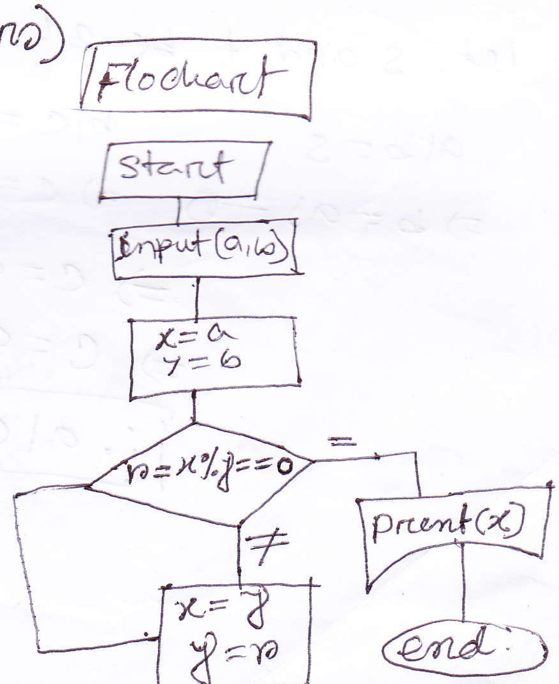
$mb + nc = a(ms) + a(nt)$

$\Rightarrow mb + nc = a(ms + nt)$

$\boxed{\therefore a | (mb + nc)}$ proved

* The Euclidean algorithm :

```
Producer gcd (a, b: positive integers)
  x: = a
  y: = b
while y ≠ 0.
begin
  r: = x mod y
  x: = y
  y: = r
end { gcd(a, b) is x }
```



* Theorem: a and b are congruent modulo m ~~and~~ if and only if there is an integer K. then $a = b + Km$.

Proof: If m devids a-b then $a-b/m = K$

বা, $a-b = Km$ $\boxed{\therefore a = b + Km}$ proved

* Let m be an integer if $a \equiv b \mod m$ and $c \equiv d \mod m$ then $a+c \equiv b+d \mod m$ and $ac \equiv bd \mod m$.

Proof: Let, s and t are two integer.

$a-b/m = s$

$\Rightarrow a-b = ms$

$\therefore a = b + ms$ — (i)

and $c-d/m = t$

$\Rightarrow c-d = mt$.

$\therefore c = d + mt$ — (ii)

(i) + (ii) হতে পাই,

$a+c = b+d+ms+mt$

$= b+d+m(s+t)$

$\therefore (a+c) \equiv (b+d) \mod m$

(i) × (ii) হতে পাই,

$a*c = (b+ms)*(d+mt)$

$\Rightarrow ac = bd + bmt + dms + m^2st$

$= bd + m(bt + ds + mst)$

$\therefore ac = bd \mod m$.

* Mathematical terem: $\underset{a}{7} \equiv \underset{b}{2} (\mod 5)$ and $\underset{c}{11} \equiv \underset{d}{1} (\mod 5)$ follow this theorem.

$7+11 = 18$ $18 \equiv 3 \mod 5$

$2+1 = 3$

$\therefore \frac{18-3}{5} = 3$.

$7 \cdot 11 = 77$, $\therefore 77 \equiv 2 (\mod 5)$

$2 \cdot 1 = 2$ $\therefore \frac{77-2}{5} = 15$

$\therefore$ ~~7~~ $\frac{7-2}{5} = 1$

$\therefore 7 = 2 + 5 \cdot 1$ — (i)

$\frac{11-1}{5} = 2$

$11 = 1 + 5 \cdot 2$ — (ii)

(c) Use Fermat's little theorem to complete

(i) $5^{2003} \mod 7$ (ii) $5^{2003} \mod 11$ and (iii) $5^{2003} \mod 13$.

(d) What is Mersenne prime? Give some examples of Mersenne prime.

Find the ~~Bo~~ greatest common divisor of 414 & 662 using the Eucledean algorithm.

$662 = 414 \cdot 1 + 248$

$414 = 248 \cdot 1 + 166$

$248 = 166 \cdot 1 + 82$

$166 = 82 \cdot 2 + 2$

$82 = 41 \cdot 2 + 0$

Hence gcd(414 & 662) = 2. since 2 is the last nonzero remainder.

set $x = a, y = b$
while $y \neq 0$.
$r = x \% y$;
$x = y$;
$y = r$;
end.
process x

* What is gcd?

The largest integer that divides both of two integers is called greatest common divisor.

Law:

$\{(2a+1)p + (2a+b)\} \bmod 26$

* gcd of (252, 198.)

$252 = 198 \cdot 1 + 54$

$198 = 162 \cdot 1 + 36$

$162 = 144 \cdot 1 + 18$

$252 = 198 \cdot 1 + 54$

$198 = 54 \cdot 3 + 36$

$54 = 36 \cdot 1 + 18$

$36 = 18 \cdot 2 + 0$

$18 = 54 - 36 \cdot 1$

$= 54 - 1(198 - 3 \cdot 54)$

$= 4 \cdot 54 - 1 \cdot 198$

$= 4(252 - 1 \cdot 198) - 1 \cdot 198$

$= 4(252 - 1 \cdot 198$

CSE ~~DEPT~~

~~$c = (ap+b) \bmod 26$ where $a=7, b=4$.~~

Let, m, a, b are integers of $ac = bc \pmod m$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod m$.

Solution: Since, $ac \equiv bc \pmod m$ so, $(ac - bc)$ must be divided by m.

$\therefore a \equiv b \bmod m$.

* $\gcd(252, 198) = ??$ by $sa+bt$ form.

$252 = 1 \cdot 198 + 54$

$198 = 3 \cdot 54 + 36$

$54 = 1 \cdot 36 + 18$

$36 = 2 \cdot 18 + 0$

$18 = 54 - 1 \cdot 36$

$= 54 - 1 \cdot (198 - 3 \cdot 54)$

$= 4 \cdot 54 - 1 \cdot 198$

$= 4(252 - 1 \cdot 198) - 1 \cdot 198$

$= \underset{s}{4} \cdot \underset{a}{252} - \underset{t}{5} \cdot \underset{b}{198}$

$\therefore \gcd(252, 198) = (4 \cdot 252 - 5 \cdot 198)$

$\therefore \gcd(a, b) = sa + tb$

Inverse function: $f(x) = 2x-3$.

Let, $y = f(x) = 2x-3$

$\therefore x = f^{-1}(y) = 2x-3$

$\therefore y = 2x-3$

$\Rightarrow 2x = y+3$

$\Rightarrow x = \frac{y+3}{2}$

$\therefore f^{-1}(y) = \frac{y+3}{2}$.

* **Function composition:**

$f(x) = 2x+1$.

$g(x) = x^2-2$,

i) $g\circ f = g(f(x))$

$= g(2x+1)$

$= (2x+1)^2 - 2$

$= 4x^2+4x+1-2$

$= 4x^2+4x-1$

ii) $f\circ g = f(g(x))$

$= f(x^2-2)$

$= 2(x^2-2)+1$

$= 2x^2-3$

$\cancel{f(g)}(f\circ g)(2)$

$= 2(2)^2-3$

$= 2\times4-3$

$= 5$

* Let,

m, a, b are integer. If $ac \equiv bc$ mod m and $\gcd(c, m) = 1$, then $a \equiv b$ mod m

Since $ac \equiv bc$ mod m. So m must devide $(a-b)c$.

$\frac{ac-bc}{m} = k$

$\therefore ac - bc = mk$ — (1)

As, $\gcd(c,m) = 1$.

so, m devides $a-b$

$\boxed{\therefore a \equiv b \text{ mod } m}$ proved

* $7 \equiv 2 \pmod 5$ and $11 \equiv 1 \pmod 5$

$\frac{7-2}{5} = 1$

$\therefore 7 = 2+5\cdot1$ — (i)

$\frac{11-1}{5} = 2$

$\therefore 11 = 1+5\cdot2$ — (ii)

(i) + (ii) $\Rightarrow$,

$7+11 = 2+1+5\cdot1+5\cdot2$

$\Rightarrow 18 = 3+5(1+2)$

$\Rightarrow \frac{15}{5} = 3$

(i) $\times$ (ii) $\Rightarrow$,

$7\cdot11 = (2+5\cdot1)(1+5\cdot2)$

$= 2\cdot1+2\cdot5\cdot2+5\cdot1\cdot1+5\cdot1\cdot5\cdot2$

$= 2+5(4+1+10)$

$77 = 2+5\cdot15$

$77-2$