21/01/2018 Number Systems.

Set of all integers (whole number) = $\mathbb{Z}$

Set of all rational numbers (of form $\frac{a}{b}$, $a,b \in \mathbb{Z}$ and $b \neq 0$) = $\mathbb{Q}$

- every integer is a rational number, $b = 1$.
- all terminated decimals are rational.
- all recurring decimals (has a pattern) are rational.

Set of all real numbers = $\mathbb{R}$

Statements: $3 \in \mathbb{Z}$ → "3 is an element of $\mathbb{Z}$"

$\frac{2}{3} \in \mathbb{Q}$, also, $\frac{2}{3} \in \mathbb{R}$

$-10 \cdot 2 \in \mathbb{Q}$

Set of all real and imaginary numbers (complex) = $\mathbb{C}$
(in the form $a+bi$, $a,b \in \mathbb{R}$, and $i = \sqrt{-1}$)

Set of all natural numbers (positive integers) = $\mathbb{N}$
(including 0)

Set of all integers module n ($n \in \mathbb{N}$, $n \geq 2$) = $\mathbb{Z}_n$
(gives remainders, eg 5 mod 3 = 2)

eg $\mathbb{Z}_3 = \{0, 1, 2\}$ → the only possible remainders when integer divided by 3.
∴ in $\mathbb{Z}_n$, set of all possible remainders when integers divided by n: $\{0, 1, 2, \ldots n-1\}$.

choose $n \in \mathbb{Z}$, $m \in \mathbb{N}$, $m \neq 0$.
Theorem: there exists unique integers q and r s.t.
$n = mq + r$ where $0 \leq r < m$

n mod m, $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$

- i.e, q is the quotient, r is the remainder in $\mathbb{Z}_m$ and m is the number you divide n with.

eg. -10 div $3 = q$ $\quad -10 = 3\boxed{-4} + \boxed{2}$
-10 mod $3 = r$
where $n = -10$, $m = 3$, $q = -4$, $r = 2$

eg. -30 div $7 = -5$
-30 mod $7 = 5$, $\quad -30 = 7\overset{q}{\boxed{-5}} + \overset{r}{\boxed{5}}$ and $5 \in \mathbb{Z}_7$

eg: -3 mod $12 = 9$
-3 div $12 = -1$, $\quad -3 = 12\overset{q}{\boxed{-1}} + \overset{r}{\boxed{9}}$ & $9 \in \mathbb{Z}_{12}$

How to solve?
eg: -17 mod 12
⇒ ~~17~~ $12 - (+17 \bmod 12)$
$= 12 - 5$
$= 7 \in \mathbb{Z}_{12}$
Hence, $-17 = 12\boxed{-2} + \boxed{7}$

eg: -21 mod 9
⇒ $9 - (21 \bmod 9)$
$= 9 - 3 = 6 \in \mathbb{Z}_9$
Hence, $-21 = 9\boxed{-3} + \boxed{6}$

eg: -5 mod 5
⇒ $5 - (5 \bmod 5)$
$= 5 - 0 = 5$ & $5 \in \mathbb{Z}_5$ → contradiction.

Know that;
given $n \geq 1$, $m \geq 1$,

1. if n is a multiple of m, then $n \bmod m = 0$ and $-n \bmod m = 0$
   eg in $-5 \bmod 5$ (n, m) $5 \times 1 = 5$
   Hence $5 \bmod 5 = 0$ and $-5 \bmod 5 = 0$.

2. if n is not a multiple of m, then $-n \bmod m = m - (n \bmod m) \in Z_m$

eg: $-30 \bmod 15 = 0$
$-32 \bmod 15 = 15 - (32 \bmod 15)$
$= 15 - 2$
$= 13 \in Z_{15}$

Fact:
let $n, m \geq 1$. Then,
n = multiplication of prime factors of n.
eg: $10 = 5 \times 2$, 5, 2 are prime numbers.

eg: 100.

$$\begin{array}{r|l} 2 & 100 \\ 2 & 50 \\ 5 & 25 \\ 5 & 5 \\ & 1 \end{array} \Rightarrow 100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2 \leftarrow \text{prime factorisation of 100.}$$

eg: 68.

$$\begin{array}{r|l} 2 & 68 \\ 2 & 34 \\ 17 & 17 \\ & 1 \end{array} \Rightarrow 68 = 2^2 \times 17 \leftarrow \text{prime factorisation of 68}$$

gcd (n,m) → greatest common divisor / factor.
eg: what is gcd (200, 77) = 1
eg: gcd (20, 28) = 4

How to find gcd (n, m)?
→ Algorithm: take larger number,
divide by smaller.

eg gcd (20,28):

$$\begin{array}{r|l} 20 & 28 \\ & -20 \\ & 8 \end{array} \quad \text{take divisor, divide by remainder} \longrightarrow \quad \begin{array}{r|l} 8 & 20 \\ & -16 \\ & 4 \end{array}$$

$$\begin{array}{r|l} 4 & 8 \\ & -8 \\ & 0 \end{array}$$

→ stop. gcd = divisor (at 0 remainder).
$\therefore$ gcd (20,28) = 4

1. gcd (204, 66)

$$\begin{array}{r|l} 66 & 204 \\ & -198 \\ & 6 \end{array} \rightarrow \begin{array}{r|l} 6 & 66 \\ & -66 \\ & 0 \end{array}$$

$\therefore$ gcd (204, 66) = 6

2 gcd (164, 102)

$$102 \overline{)164}\ 1 \quad 164 - 102 = 62 \rightarrow 62 \overline{)102}\ 1 \quad 102 - 62 = 40 \rightarrow 40 \overline{)62}\ 1 \quad 62 - 40 = 22 \rightarrow 22 \overline{)40}\ 1 \quad 40 - 22 = 18$$

$$18 \overline{)22}\ 1 \quad 22 - 18 = 4 \rightarrow 4 \overline{)18}\ 4 \quad 18 - 16 = 2$$

$\frac{4}{2} = 2$, 4 mod 2 = 0.

∴ gcd (164, 102) = 2

Question: Solve over Z_{12}. $3x = 5$
(otherwise written as : Find an x in Z_{12} s.t (3 × x) mod 12 will result in 5).

calculating in Z_{12} : $5+7 = 0$, $3+8 = 11$, $7+7 = 2$

how? $5+7 = 12 \bmod 12 = 0$, $3+8 = 11 \bmod 12 = 11$, $7+7 = 14 \bmod 12 = 2$

similarly : $3 \times 15 = 9$ how? $3 \times 15 = 45 \bmod 12 = 9$

back to question: $3x = 5$.
try all numbers in Z_{12} (0 – 11) ... no sol°.

Question: Solve over Z_{12}. $7x = 5$
try $7 \times 11 = 77 \bmod 12 = 5$.
hence, $x = 11$

Question: Solve ~~of~~ over Z_5. $-3x = 21$
⇒ Notice : neither −3 nor 21 are in Z_5.
convert : $-3 \bmod 5 = 5 - (3 \bmod 5) = 5 - 3 = 2$ 21 mod 5 = 1.
Rewrite question : $-3x = 21 \longrightarrow 2x = 1$. Now solve.
try x = 3 : $2 \times 3 = 6 \bmod 5 = 1$.
∴ $x = 3 \in Z_5$

Know : Solve over Z_n, $ax = b$. $a, b \in Z_n$.
$ax = b$ in Z_n has a sol° iff $\gcd(a,n) \mid b$ (gcd (a, n) is a factor of b).
Furthermore,
no. of sol° = gcd (a, n)

Question: $3x = 5$ over Z_{12}.
$a = 3, b = 5, n = 12$
⇒ $\gcd(3, 12) = 3$. $3 \nmid 5$ (3 is not a factor of 5)
∴ no sol°.

Homework:

1. gcd(104, 54)

Answer:
$$54 \overline{)104}\ 1 \quad -54 \quad 50 \rightarrow 50 \overline{)54}\ 1 \quad -50 \quad 4 \rightarrow 4 \overline{)50}\ 12 \quad -48 \quad 2 \rightarrow \frac{4}{2} = 2$$

$\therefore$ gcd(104, 54) = 2

2. Find prime factorisation of 308

Ans:
$$2 \overline{)308} \quad 2 \overline{)154} \quad 7 \overline{)77} \quad 11 \overline{)11} \quad 1$$

$\therefore 308 = 2^2 \times 7 \times 11$

3. Solve ~~of~~ over Z_6 (find no. of sol°)

i. $2x = 4$

Ans: gcd(2,6) = 2, $2 \mid 4$. $\therefore$ there are 2 sol°.

$Z_6 = \{0, 1, 2 \ldots 5\}$

try $x = 2 \rightarrow 2 \times 2 = 4 \bmod 6 = 4$.

try $x = 5 :\rightarrow 2 \times 5 = 10 \bmod 6 = 4$.

$\therefore$ sol° are : $x = 2, x = 5$

ii. $-4x = 22$

Ans: $-4 \bmod 6 = 6 - (4 \bmod 6) = 6 - 4 = 2$

$22 \bmod 6 = 4$

$-4x = 22 \rightarrow 2x = 4$

gcd(2,6) = 2, $2 \mid 6$

sol° are $x = 2, x = 5$

iii. $4x = 5$

gcd(4,6) = 2, $2 \nmid 5$

$\therefore$ no sol°

4. i. $-23 \bmod 19$

Ans: $19 - (23 \bmod 19) = 19 - 4 = 15$

ii. $-40 \bmod 27$

Ans: $27 - (40 \bmod 27) = 27 - 13 = 14$

25/01/15

Result:
$ax = b$ over Z_n has a sol° if and only if $\gcd(a,n) \mid b$.
If we have a sol°, then they ~~exact~~ must have exactly $\gcd(a,n)$ sol° over Z_n

eg. Solve of over $Z_4 = \{0, 1, \cdots, 13\}$
$4x = 10 \quad : 4 \in Z_{14},\ 10 \in Z_{14}$

$\gcd(4,14)$

$$\begin{array}{r|l} & 3 \\ 4 & 14 \\ & -12 \\ \hline & 2 \end{array}$$

$\gcd(4,14) = 2$ which is a factor of 10.
Hence, exactly 2 distinct sol°.

Find sol°: try 6: $4 \times 6 = 24 \bmod 14 = 10$.
try 13: $4 \times 13 = 52 \bmod 14 = 10$.
∴ Sol° are $x = 6$ & $x = 13$.

Q Find all integers (over Z), say x, st. $4x \equiv 10 \pmod{14}$
↳ congruent
meaning all integers, say x, s.t, $4x$ with ~~x~~ divided by 14, remainder = 10

Theorem ⇒ $(a+b) \bmod n$
$= [(a \bmod n) + (b \bmod n)] \bmod n$ (if needed.)

eg $(7+5) \bmod 5$
$= 12 \bmod 5$
$= 2$

$7 \bmod 5 + 5 \bmod 5$
$= 2 + 0$
$= 2$

⇒ $(7 + 5k) \bmod 5 = 7 \bmod 5 + \underbrace{5k \bmod 5}_{0}$

$= 7 \bmod 5$

Ans → Solve it over Z_{14}.
$4x = 10$
by previous question, we have 2 sol°: $x = 6$ & $x = 13$

→ Sol° to given question, x have to be $6 + 14k = x,\ k \in Z$
OR $x = 13 + 14m,\ m \in Z$.

bc. $x = [6 + 14k] \bmod 14$
$= 6 \bmod 14$
$= 6$

Q1 Solve over Z_9
$2x = 7$

Q2 Describe all integers st. $2x = 7 \pmod 9$

Ans: 1 $Z_9 = \{0, 1, \ldots 8\}$.
$\gcd(2,9) = 1 \mid 7$, Hence, 1 sol°
$x = 8$

⇒ Theorem: $ab \bmod n$
$= (a \bmod n)(b \bmod n)$

2 $8 + 9k = x,\ k \in Z$
Check eg $k = -4,\ x = -28$
$2(-28) \bmod 9 = 2 \bmod 9 \cdot 9 - 28 \bmod 9$
$= 2 \cdot (9-1) = 16 \bmod 9 = 7$

Adding with bases.

eg: $(7654)_8$
$+ (2177)_8$
$(12053)_8$

$\rightarrow 4+7 = 11 \bmod 8 = 3$ (write down)
$11 \text{ div } 8 = 1$ (carry forward)

$(215)_{10}$
$+ (397)_{10}$ basic addition
$(612)_{10}$

Multiplying w/ bases:

eg: $(23)_5$
$\times (34)_5$
202
$+1240$
$(1442)_5$

$3 \times 4 = 12 \bmod 5 = 2$
$12 \text{ div } 5 = 2$

$4 \times 2 = 8 + 2 = 10 \bmod 5 = 0$
$10 \text{ div } 5 = 2$

and so on...

eg $(123)_8$
$-(017)_8$
$(104)_8$

borrow '1' eight from 2
$\rightarrow 3 + 8 = 11 - 7 = 4 \bmod 8 = 4$
$\rightarrow 2 \Rightarrow 1$

Question → Solve over Z_{20}
$4x = 12$

→ Describe all integers, say x, s.t $4x \equiv 12 \pmod{20}$

→ Find $(561)_7 + (3446)_7$

→ Find $(7372)_8 - (1427)_8$

→ Find ~~$(851)_{15} \times 3244$~~ $(321)_5 \times (43)_5$

Answers: → $Z_{20} = \{0, 1, 2 \ldots, 19\}$
$\gcd(4, 20) = 4$, & $4 \mid 12$ (4 is a factor of 12)
Hence there are 4 sol°.

$4x = 12$, i-e $4x \bmod 20 = 12$
try $x = 3$: $4(3) = 12 \bmod 20 = 12$ ✓
try $x = 8$ $4(8) = 32 \bmod 20 = 12$ ✓
try $x = 13$ $4(13) = 52 \bmod 20 = 12$ ✓
try $x = 18$ $4(18) = 72 \bmod 20 = 12$ ✓

∴ sol° are: $x = 3$, $x = 8$, $x = 13$, $x = 18$

→ $x = 3 + 20k$, $x = 8 + 20k$, $x = 13 + 20k$, $x = 18 + 20k$, $k \in Z$
check, eg $k = -3$

$x = -57$
$4(-57) \bmod 20$
$= (4 \bmod 20)(-57 \bmod 20)$
$= 4 \cdot (20 - 57 \bmod 20)$
$= 4 \times 3$
$= 12$ ✓

$x = -52$
$4(-52) \bmod 20$
$= 4 \cdot (20 - 52 \bmod 20)$
$= 4 \cdot 8$
$= 32 \bmod 20$
$= 12$ ✓

$x = -47$
$4(-47) \bmod 20$
$= 4 \times (20 - 47 \bmod 20)$
$= 4 \times 13$
$= 52 \bmod 20$
$= 12$ ✓

$x = -42$
$4(-42) \bmod 20 = 4 \times (20 - 42 \bmod 20) = 4 \times 18 = 72 \bmod 20 = 12$. ✓

→ $(561)_7 + (3446)_7 = (4340)_7$

$\therefore (561)_7 + (3446)_7 = (4340)_7$

→ $(7372)_8 - (1427)_8 = (5743)_8$

$\therefore (7872)_8 - (1427)_8 = (5743)_8$

→ $(321)_5 \times (43)_5 = (30403)_5$

$\therefore (321)_5 \times (43)_5 = (30403)_5$

28/01/18

Q: x = number of people in an event.

information; x is even.

$x \equiv 3 \pmod{11}$ and

$x \equiv 2 \pmod{5}$. i) Find x, if $0 < x < 110$.

ii) Find x, if $110 < x < 220$.

x is even can be written as: $x \equiv 0 \pmod{2}$

Chinese remainder theorem:

$x \equiv \underset{r_1}{0} \pmod{\underset{m_1}{2}}$ $\quad x \equiv \underset{r_2}{3} \pmod{\underset{m_2}{11}}$ $\quad x \equiv \underset{r_3}{2} \pmod{\underset{m_3}{5}}$

gcd between any m_i's = 1

gcd (2, 11) = 1

gcd (2, 5) = 1

gcd (5, 11) = 1

CRT: if gcd betw. any m_i's = 1, then we must have a unique sol° x, $0 \le x < m_1 m_2 m_3$ i.e $0 \le x < 110$.

Solution: Algorithm: → Find $(m_1 m_2)^{-1} \bmod (m_3) = d_3$

→ Find $(m_1 m_3)^{-1} \bmod (m_2) = d_2$

→ Find $(m_2 m_3)^{-1} \bmod (m_1) = d_1$

→ $x = \left[(m_1 m_2) d_3 r_3 + (m_1 m_3) d_2 r_2 + (m_2 m_3) d_1 r_1\right] \bmod (m_1 m_2 m_3)$

(i) [1] $55^{-1} \bmod 2$

$55x = 1$ in Z_2

$x = 1$ in Z_2

$1 \bmod 2 = 1$ $\quad d_1 = 1$

[2] $(10)^{-1} \bmod 11$

$10x = 1$ in Z_{11}

put $x = 10$: $100 \bmod 11 = 1$

$x = 10$ in Z_{11}

$d_2 = 10$

[3] $22^{-1} \bmod 5$

$22x = 1$ in Z_5

reduced $2x = 1$ in Z_5

$x = 3$; $6 \bmod 5 = 1$

$d_3 = 3$

$x = 55(1)(0) + 10(10)(3) + 22(3)(2)$

$= 300 + 132$

$= 432 \bmod 110$

$x = 102$ this is unique sol° $0 < x < 110$

(ii) $x = 102 + 110$

$x = 212$, $110 < x < 220$.

Q: x = number of defected eggs

info: $x \equiv 3 \bmod 6 \rightarrow m_1$

$x \equiv 5 \bmod 7 \rightarrow m_2$

$x \equiv 2 \bmod 13 \rightarrow m_3$

1. Find x such that $0 < x < 546$
2. Find x such that $546 < x < 1092$.

Solution: i) $\gcd(6,7) = \gcd(7,13) = \gcd(13,6) = 1$

CRT: must have unique sol°

$\rightarrow (m_2 m_3)^{-1} \bmod m_1$

$91^{-1} \bmod 6$

$91x = 1$ in Z_6

$1x = 1$ in Z_6

$d_1 = 1$

$\rightarrow (m_1 m_3)^{-1} \bmod m_2$

$78^{-1} \bmod 7$

$78x = 1$ in Z_7

$x = 1$ in Z_7

$d_2 = 1$

$\rightarrow (m_1 m_2)^{-1} \bmod m_3$

$42^{-1} \bmod 13$

$42x = 1$ in Z_{13}

$3x = 1$ in $Z_{13} = \{0, \dots 12\}$

$x = 9$ in Z_{13}

$d_3 = 9$

$x = 91(1)(3) + 78(1)(5) + 42(9)(2)$

$= 1419 \bmod 546$

$= 327$ in $0 < x < 546$

ii) $x = 873$, $546 < x < 1092$

Q1 x = number of defective computers

$x \equiv 5 \bmod 9 \rightarrow m_1$

$x \equiv 10 \bmod 22 \rightarrow m_2$

$x \equiv 4 \bmod 5 \rightarrow m_3$, $0 < x < 990$

Q2 Solve for x, $0 \le x < 260$

$x \equiv 19 \bmod 20 \rightarrow m_1$

$x \equiv 12 \bmod 13 \rightarrow m_2$

Solution1 i) $\gcd(9,22) \Rightarrow \gcd(22,5) \Rightarrow \gcd(9,55) = 1$

Hence, there is a unique sol°

$(m_2 m_3)^{-1} \bmod m_1$

$110^{-1} \bmod 9$

$110x = 1$ in Z_9

$2x = 1$ in Z_9

$x = 5 = d_1$

$(m_1 m_3)^{-1} \bmod m_2$

$45^{-1} \bmod 22$

$45x = 1$ in Z_{22}

$1x = 1$ in Z_{22}

$x = 1 = d_2$

$(m_1 m_2)^{-1} \bmod m_3$

$198^{-1} \bmod 5$

$198x = 1$ in Z_5

$3x = 1$

$x = 2 = d_3$

$x = 110(5)(5) + 45(1)(10) + 198(2)(4)$

$= 4784 \bmod 990$

$x = 824 \in 0 \le x < 990.$

Solution2 $\gcd(20,13) = 1$

Hence, there is a unique sol°

$m_2^{-1} \bmod m_1$

~~$22x = 1$ in Z_{20}~~

~~$2x = 1$ in Z_{20}~~

$13^{-1} \bmod 20$

$13x = 1$ in Z_{20}

$x = 17 \in Z_{20}$

$= d_1$

$m_1^{-1} \bmod m_2$

$20^{-1} \bmod 13$

$20x = 1$ in Z_{13}

$7x = 1$ in Z_{13}

$x = 2 \in Z_{13}$

$= d_2$

$x = 13(17)(19) + 20(2)(12)$

$= 4679 \bmod 260$

$x = 259 \in 0 \le x < 260$

30/01/18 Another example:

$x \equiv 1 \pmod 7 \rightarrow m_1$
$x \equiv 7 \pmod 9 \rightarrow m_2$
$x \equiv 10 \pmod{10} \rightarrow m_3$
$x \equiv 1 \pmod{11} \rightarrow m_4$

CRT : unique sol° from $0 < x < 6930$.

$\rightarrow (m_2 m_3 m_4)^{-1} \bmod m_1$ $\rightarrow (m_1 m_3 m_4)^{-1} \bmod m_2$ $\rightarrow (m_1 m_2 m_4)^{-1} \bmod m_3$

$\rightarrow (m_1 m_2 m_3)^{-1} \bmod m_4$

$\rightarrow$ $990x = 1$ in Z_7 $\rightarrow$ $770x = 1$ in Z_9
$3x = 1$ in Z_7 $5x = 1$ in Z_9
$x = 5 = d_1 \in Z_7$ $x = 2 = d_2 \in Z_9$

$\rightarrow$ $693x = 1$ in Z_{10} $\rightarrow$ $630x = 1$ in Z_{11}
$3x = 1$ in Z_{10} $3x = 1$ in Z_{11}
$x = 7 = d_3 \in Z_{10}$ $x = 4 = d_4 \in Z_{11}$

$x = 990(5)(1) + 770(2)(7) + 693(7)(10) + 630(4)(1)$
$= 66760 \bmod 6930$
$x = 439. \in 0 < x < 6930.$

Result: $d = \gcd(n, m)$, $n, m \in N$ (includes 0)
$\exists\ k_1, k_2 \in Z$ s.t $d = k_1 n + k_2 m$
↳ exists
i.e gcd can be written as a linear combination.

eg: gcd (5, 7) :

1	2	2
5 | 7	2 | 5	(1) | 2
-5	-4	gcd. -2
2	1	0 stop.

gcd (5, 7) = 1 = $k_1(5) + k_2(7)$
Find k_1, k_2.
$1 = 5 - (2 \times 2)$
$= 5 - (7 - (5 \times 1))(2)$
$= 5 - (2 \times 7) + (2 \times 5)$
$= 5(1+2) + 7(-2)$
$= (3)5 + (-2)7$

Hence, $k_1 = 3$, $k_2 = -2$

example: gcd (20, 28) :

1	2	2
20 | 28	8 | 20	4 | 8
-20	-16	-8
8	4	0

gcd = 4 = $k_1 20 + k_2 28$, Find k_1, k_2.

$4 = 20 - (8 \times 2)$
$= 20 - [28 - (20 \times 1)](2)$
$= 20 - [(2 \times 28) - (2 \times 20)]$
$= 20(1+2) + 28(-2)$
$= (3)20 + (-2)28$ Hence $k_1 = 3$, $k_2 = -2 \in Z$

(eg) gcd (164, 102)

$$102\overline{)164}\ 1,\ 102,\ 62$$
$$62\overline{)102}\ 1,\ 62,\ 40$$
$$40\overline{)62}\ 1,\ 40,\ 22$$
$$22\overline{)40}\ 1,\ 22,\ 18$$
$$18\overline{)22}\ 1,\ 18,\ 4$$
$$4\overline{)18}\ 4,\ 16,\ 2$$
$$2\overline{)4}\ 2,\ 4,\ 0$$

$\gcd = 2 = k_1(164) + k_2(102)$

Find k_1, k_2.

$2 = 18 - (4\times 4)$
$= 18 - (4)(22 - (18\times 1))$
~~$= 18 - 4(22 - 40 - 22)$~~
$= (40 - 22) - [22 - (1\times 18)](4)$
$= (40 - 22) - [22 -$
my goodness.

$2 = 18 - (4\times 4)$
$= 18 - 4(22 - (18\times 1))$
$= 18 - 4(22) + 4(18)$
$= 5(18) - 4(22)$
$= 5(40-22) - 4(22)$
$= 5(40) - 5(22) - 4(22)$
$= 5(40) - 9(22)$
$= 5(40) - 9(62 - 40)$
$= 5(40) - 9(62) + 9(40)$
$= 14(40) - 9(62)$
$= 14(102 - 62) - 9(62)$
$= 14(102) - 14(62) - 9(62)$
$= \underbrace{14(102)}_{\text{keep.}} - 23(62)$

$= 14(102) - 23(164 - 102)$
$= 14(102) - 23(164) + 23(102)$
$= 37(102) - 23(164)$

Hence: $k_1 = -23$ $k_2 = 37$. $\because k_1, k_2 \in \mathbb{Z}$.

$$\text{LCM}(164, 102) = \frac{164\times 102}{\gcd(164, 102)} = \frac{16728}{2} = 8364$$

HW: [1] Find $\gcd(37, 44)$, then find k_1, k_2 st $\gcd(37,44) = 37k_1 + 44k_2$. $k_1, k_2 \in \mathbb{Z}$

[2] Find LCM (112, 56)

Solution: [1] gcd (37, 44):

$$37\overline{)44}\ 1,\ 37,\ 7 \rightarrow 7\overline{)37}\ 5,\ 35,\ 2 \rightarrow 2\overline{)7}\ 3,\ 6,\ 1 \rightarrow 1\overline{)2}\ 2,\ 2,\ 0$$

Hence, gcd = 1

$1 = k_1(37) + k_2(44)$
$1 = 2 - (1\times 2)$
$= 2 - (7 - (2\times 3))(2)$
$= (37 - (7\times 5)) - (7 - [(37 - (7\times 5))\times 3])(2)$
$= 37 - (7\times 5) - (7 - 3(37) - (3\times 5)7)(2)$
$= 37 - 5(7) - (7 - 3(37) - 15(7))(37 - 5(7))$
$= 37 - 5(7) - [37 - 5(7)$
why.

gcd (37,44) : $37\overline{)44}$ (1), -37, 7 → $7\overline{)37}$ (5), -35, 2 → $2\overline{)7}$ (3), -6, 1 → $1\overline{)2}$ (2), -2, 0

gcd (37, 44) = 1

$1 = 7 - 2(3)$
$= 7 - 37(7 \times 7 5)$
$= 7 - (37 - 7(5))(3)$
$= 7 - (3)(37) + 15(7)$
$= 16(7) - 3(37)$
$= 16(44 - 37) - 3(37)$
$= 16(44) - 16(37) - 3(37)$
$1 = 16(44) - 19(37)$

Hence $1 = \underbrace{16}_{k_1}(44) - \underbrace{19}_{k_2}(37)$

2 LCM (112, 56) : $56\overline{)112}$ (2), -112, 0 gcd (56, 112) = 56.

$\text{LCM}(112, 56) = \frac{112 \times 56}{56} = 112$

BRUNNEN