Exercise: Prove that if d is a common divisor of a and b, then $d = \gcd(a,b)$ if and only if $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Solution:

Suppose first that $d = \gcd(a,b)$. Then, there exist $x, y \in \mathbb{Z}$ such that $d = ax+by$.

Then we can write $\frac{a}{d}.x + \frac{b}{d}.y = 1$. Note that $d|a$, $d|b$ tells us that $\frac{a}{d}$ and $\frac{b}{d}$ are integers. Let $d^* = \gcd\left(\frac{a}{d}, \frac{b}{d}\right)$. We therefore have the numbers $d^* \mid \frac{a}{d}$ and $d^* \mid \frac{b}{d}$ which implies $d^* \mid \frac{a}{d}x + \frac{b}{d}y = 1$. So, $d^* \in \{-1, 1\}$.

Since $d^* > 0$ we thus have $d^* = 1$.

Conversely, if $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ then there exist $s, t \in \mathbb{Z}$ such that $\frac{a}{d}.s + \frac{b}{d}.t = 1$. Then, $a.s + b.t = d$. Let $d^* = (a,b)$.

As d is a common divisor of both a and b, we have $d \leq d^*$.

Moreover, since $d^* | a$ and $d^* | b$ we have $d^* \mid a.s$ and $d^* \mid b.t$.

So, $d^* \mid a.s + b.t$ which implies $d^* | d$. This shows $d^* \leq d$.

We therefore have $d^* = d$.

Exercise: Let $a, b \in \mathbb{Z}$ be coprime. Prove that $\gcd(a+b, a-b) \in \{1, 2\}$.

Solution: Let $d = (a+b, a-b)$. Then, $d \mid a+b$ and $d \mid a-b$.

This implies that $d \mid (a+b)+(a-b) = 2a$ and $d \mid (a+b)-(a-b) = 2b$.

Since $d | 2a$ and $d | 2b$ we have $d \mid (2a, 2b)$. Now, we notice $(2a, 2b) = |2|.(a,b) = 2.(a,b) = 2.1 = 2$ since $(a,b) = 1$. This shows that $d | 2$ and so $d \in \{1, 2\}$. Notice if $a = 3, b = 1$ we have $(a,b) = 1$ and $(a+b, a-b) = (4, 2) = 2$. Similarly, if $a = 3$ and $b = 2$, the numbers $(a,b) = 1$ and $(a+b, a-b) = (5, 1) = 1$.

So, both possible values of d can occur.

Exercise: Let $a,b \in \mathbb{Z}$ be coprime. Find $\gcd(2a+b, 3a-2b)$.

Solution: Let $d = (2a+b, 3a-2b)$. Then,

$$\begin{cases} d \mid 2a+b \\ d \mid 3a-2b \end{cases} \Rightarrow \begin{cases} d \mid (2a+b)3 \\ d \mid (3a-2b)\cdot 2 \end{cases} \Rightarrow \begin{cases} d \mid 6a+3b \\ d \mid 6a-4b \end{cases} \Rightarrow d \mid 7b$$

Similarly, we have

$$\begin{cases} d \mid 2a+b \\ d \mid 3a-2b \end{cases} \Rightarrow \begin{cases} d \mid (2a+b)\cdot(-2) \\ d \mid 3a-2b \end{cases} \Rightarrow \begin{cases} d \mid -4a-2b \\ d \mid 3a-2b \end{cases} \Rightarrow d \mid 7a.$$

Since $d \mid 7a$ and $d \mid 7b$ we have $d \mid (7a, 7b)$. Next, we observe the number $\gcd(7a, 7b) = |7| \cdot \gcd(a,b) = 7 \cdot 1 = 7$ since a and b are coprime. This shows that $d \in \{1, 7\}$. We will now show that both possible values can occur. If $a=1, b=0$ we have $(2a+b, 3a-2b) = (2,3) = 1$ while if $a=3, b=1$ the number $(2a+b, 3a-b) = (7,7) = 7$. The result follows.

Exercise: Let $a,b \in \mathbb{Z}$ coprime. Prove the following (i) – (ii) hold:
(i) $\gcd(a+b, a^2+b^2) = 1$. (ii) $\gcd(a+b, ab) = 1$.

Solution:

(i) Let $d = (a+b, a^2+b^2)$. Note that $d \mid a+b$ and $d \mid a^2+b^2$. So, $d \mid (a+b)(a-b) = a^2-b^2$. We therefore have $d \mid (a^2+b^2)+(a^2-b^2)$ which implies $d \mid 2a^2$. Similarly, $d \mid (a^2+b^2)-(a^2-b^2)$. So, $d \mid 2b^2$. This shows that $d \mid (2a^2, 2b^2)$. Notice now $(2a^2, 2b^2) = |2|\,(a^2, b^2) = 2\cdot(a,b)^2 = 2$. Recall whenever $(a,b)=1$ we proved $(a^m, b^m)=1$ for every $m \in \mathbb{N}$. Hence $d \mid 2$. This means $d \in \{1,2\}$. Note if $a=b=1$ then $d=(2,2)=2$ while if $a=2, b=1$ then $d=(3,5)=1$. Thus, both possible value for d can occur. This shows either $d=1$ or $d=2$.

(ii) Let $d = (a+b, ab)$. Note that $d \mid a+b$ and $d \mid ab$. So, $d \mid (a+b)a - ab$ which shows that $d \mid a^2$. Similarly we have $d \mid (a+b)b - ab$, that is $d \mid b^2$. We thus have $d \mid (a^2, b^2)$. Since $(a,b)=1$ we have $(a^2,b^2)=1$. So $d \mid 1$ which shows that $d=1$.

Exercise: Let $a, b \in \mathbb{Z}$, $a \neq 0, b \neq 0$ and let $m \in \mathbb{N}$. Show that $a \mid b$ if and only if $a^m \mid b^m$.

Solution:

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$. Since $a \mid b$ then there exists $k \in \mathbb{Z}$ such that $ak = b$. Then, we have $b^m = (ak)^m = a^m \cdot k^m$ with $k^m \in \mathbb{Z}$. This shows that $a^m \mid b^m$. Conversely, assume that $a^m \mid b^m$. Then we can write $a^m \cdot q = b$ for some $q \in \mathbb{Z}$. Let $d = \gcd(a,b)$. Then, there exist $s, t \in \mathbb{Z}$ such that $a = d \cdot s$, $b = d \cdot t$ and $(s,t) = 1$. This implies that

$$d^m \cdot s^m \cdot q = (ds)^m q = a^m q = b^m = d^m t^m \Rightarrow d^m \cdot (s^m q - t^m) = 0 \underset{d>0}{\Rightarrow} s^m \cdot q = t^m.$$

This shows that $s^m \mid t^m$. We therefore have that $\gcd(s^m, t^m) = |s^m| = |s|^m$. However, since $(s,t) = 1$ we have $(s^m, t^m) = 1$ which implies that $|s|^m = 1$ and so $s \in \{-1, 1\}$. Next, we observe either $a = d$ or $a = -d$. Consequently, either $b = a \cdot t$ or $b = a \cdot (-t)$. Hence, $a \mid b$ as we wanted to show.

Exercise: Prove that if $\gcd(a,b) = 1$, then $\gcd(a+b, ab) = 1$.

Solution:

Let $a, b \in \mathbb{Z}$ such that $(a,b) = 1$. Let $d = (a+b, ab)$. Then, we note

$$\begin{cases} d \mid a+b \\ d \mid ab \end{cases} \Rightarrow \begin{cases} d \mid (a+b) \cdot a \\ d \mid ab \end{cases} \Rightarrow \begin{cases} d \mid a^2 + ab \\ d \mid ab \end{cases} \Rightarrow d \mid (a^2 + ab) - ab \Rightarrow d \mid a^2.$$

Similarly, we observe

$$\begin{cases} d \mid a+b \\ d \mid ab \end{cases} \Rightarrow \begin{cases} d \mid (a+b) \cdot b \\ d \mid ab \end{cases} \Rightarrow \begin{cases} d \mid ab + b^2 \\ d \mid ab \end{cases} \Rightarrow d \mid (ab + b^2) - ab \Rightarrow d \mid b^2.$$

Now, notice that $d \mid a^2$ and $d \mid b^2$. This shows that $d \mid (a^2, b^2)$. Since $(a,b) = 1$ we therefore have $(a^2, b^2) = 1$. Hence $d \mid 1$ which means $d \in \{-1, 1\}$. Since $d > 0$ we have $d = 1$. The result follows.

THE NOTION OF GREATEST COMMON DIVISOR CAN BE EXTENDED TO MORE THAN TWO INTEGERS IN AN OBVIOUS WAY. IN THE CASE OF THREE INTEGERS $a,b,c \in \mathbb{Z}$, NOT ALL ZERO, THE NUMBER $\gcd(a,b,c)$ IS DEFINED TO BE THE POSITIVE INTEGER d HAVING THE FOLLOWING PROPERTIES:

(i) d IS A DIVISOR OF EACH OF a, b, c.

(ii) IF $h|a$, $h|b$, $h|c$ THEN $h \leq d$.

Exercise: LET a,b,c BE INTEGERS, NO TWO OF WHICH ARE ZERO AND LET $d = (a,b,c)$. SHOW THAT $d = ((a,b),c) = (a,(b,c)) = ((a,c),b)$.

Solution: LET $a,b,c \in \mathbb{Z}$, NO TWO OF WHICH ARE ZERO. LET $d = (a,b,c)$, $d_1 = (a,b)$ AND $D_1 = (d_1, c)$. WE FIRST PROVE THAT $D_1 = d$. NOTE THAT BY DEFINITION OF D_1 WE HAVE $D_1|c$ AND $D_1|d_1$. SIMILARLY, BY DEFINITION OF d_1 WE HAVE $d_1|a$ AND $d_1|b$. THEN, SINCE $D_1|d_1$ AND $d_1|a$ WE HAVE $D_1|a$. MOREOVER, AS $D_1|d_1$ AND $d_1|b$ WE HAVE $D_1|b$. THEREFORE, D_1 DIVIDES a,b,c. THIS IMPLIES THAT $D_1 \leq d$. NOW, WE OBSERVE $d_1 = ax+by$ FOR SOME $x,y \in \mathbb{Z}$ SINCE $d_1 = (a,b)$. IN ADDITION, AS $d|a$ AND $d|b$ WE HAVE $d|ax$, $d|by$ AND SO $d|ax+by = d_1$. SINCE $d|d_1$ AND $d|c$ WE THEREFORE HAVE $d|(d_1,c)$. THAT IS, $d|D_1$ AND SO $d \leq D_1$. THIS SHOWS THE NUMBERS $d = D_1$.

LET $d_2 = (b,c)$ AND LET $D_2 = (a, d_2)$. WE NEXT SHOW THAT $D_2 = D_1$. BY DEFINITION OF D_2 WE HAVE $D_2|a$ AND $D_2|d_2$. SIMILARLY, BY DEFINITION OF d_2, WE HAVE $d_2|b$ AND $d_2|c$. THEN, $D_2|b$ AND $D_2|c$. SINCE $D_2|a$ AND $D_2|b$ WE HAVE $D_2|(a,b) = d_1$. SO, $D_2|d_1$ AND $D_2|c$ IMPLIES $D_2|(d_1,c) = D_1$. THAT IS $D_2|D_1$. ON THE OTHER HAND, BY DEFINITION OF D_1 WE HAVE $D_1|d_1$ AND $D_1|c$. BY DEFINITION OF d_1, WE KNOW $d_1|a$ AND $d_1|b$. THIS SHOWS THAT $D_1|a$, $D_1|b$ AND $D_1|c$. SO, $D_1|a$ AND $D_1|(b,c) = d_2$. SINCE $D_1|a$ AND $D_1|d_2$ WE THUS HAVE THAT

$D_1 \mid (a, d_2) = D_2$. HENCE, $D_1 \mid D_2$ AND $D_1 = D_2$.

LET $d_3 = (a, c)$ AND $D_3 = (d_3, b)$. WE NEXT SHOW THAT $D_2 = D_3$. BY DEFINITION OF D_2, NOTICE $D_2 \mid d_2$ AND $D_2 \mid a$. SIMILARLY, BY DEFINITION OF d_2 WE HAVE $d_2 \mid b$ AND $d_2 \mid c$. THIS IMPLIES THAT $D_2 \mid a$, $D_2 \mid b$ AND $D_2 \mid c$. SINCE $D_2 \mid a$ AND $D_2 \mid c$ WE HAVE $D_2 \mid (a, c) = d_3$. THEN, AS $D_2 \mid d_3$ AND $D_2 \mid b$ WE HAVE $D_2 \mid (d_3, b) = D_3$. THIS SHOWS $D_2 \leq D_3$.

ON THE OTHER HAND, BY DEFINITION OF D_3, WE HAVE $D_3 \mid d_3$ AND $D_3 \mid b$. SINCE d_3 IS A COMMON DIVISOR OF a AND c, $d_3 \mid a$, $d_3 \mid c$ WHICH IMPLIES $D_3 \mid a$, $D_3 \mid c$. AS $D_3 \mid b$ AND $D_3 \mid c$ WE HAVE $D_3 \mid (b, c) = d_2$. THEN, SINCE $D_3 \mid d_2$ AND $D_3 \mid a$ WE HAVE $D_3 \mid (d_2, a)$. THAT IS $D_3 \mid D_2$ AND $D_3 \leq D_2$. THEREFORE, $D_2 = D_3$.

CONSEQUENTLY, $d = D_1 = D_2 = D_3$. THE RESULT FOLLOWS.

The Euclidean Algorithm (EA)

THE GREATEST COMMON DIVISOR OF TWO INTEGERS CAN BE FOUND BY LISTING ALL THEIR POSSITIVE DIVISORS AND CHOOSING THE LARGEST ONE COMMON TO EACH. HOWEVER, THIS IS NOT A GOOD IDEA FOR LARGE NUMBERS! A MORE EFFICIENT PROCESS IS THE EUCLIDEAN ALGORITHM (E.A.) WHICH INVOLVES REPEATED APPLICATIONS OF THE ALGORITHM DIVISION THEOREM (A.D.T.). THE E.A. IS BASICALLY BASED ON THE NEXT RESULT:

Exercise: LET $a, b \in \mathbb{Z}$, $b \neq 0$. SHOW THAT IF $a = b.q + r$, WITH $q, r \in \mathbb{Z}$ THEN

$$(a, b) = (b, r).$$

Solution:

LET $d = (a, b)$ AND LET $d^* = (b, r)$. WE OBSERVE $r = a - bq$. SO, SINCE $d \mid b$ THEN $d \mid bq$ WITH $q \in \mathbb{Z}$. AS $d \mid a$ WE THUS HAVE $d \mid a - bq = r$. THIS SHOWS THAT d IS A COMMON DIVISOR OF b AND r. SO, IT MUST BE $d \leq d^*$. SIMILARLY, SINCE $d^* \mid b$ THEN $d^* \mid bq$ WITH $q \in \mathbb{Z}$. SO, AS $d^* \mid r$ WE HAVE $d^* \mid bq + r = a$. THIS SHOWS d^* IS A

COMMON DIVISOR OF a AND b WHICH IMPLIES $d^* \leq d$. HENCE $d = d^*$.

THIS LAST RESULT NOT ONLY ALLOW US TO COMPUTE THE GREATEST COMMON DIVISOR OF TWO INTEGERS $a, b, b \neq 0$ BUT ALSO GIVES US A WAY TO FIND A LINEAR COMBINATION $ax + by$ OF SUCH NUMBER.

LET $a, b \in \mathbb{Z}$, $b \neq 0$. THE FIRST STEP IS TO APPLY THE ADT TO a AND b TO GET $a = q_1 . b + r_1$ WITH $0 \leq r_1 < b$. IF IT HAPPENS THAT $r_1 = 0$ THEN $b | a$ AND $(a,b) = |b|$. WHEN $r_1 \neq 0$, DIVIDE b BY r_1 TO PRODUCE INTEGERS q_2, r_2 SATISFYING $b = q_2 r_1 + r_2$ WITH $0 \leq r_2 < r_1$. IF $r_2 = 0$ THEN $(a,b) = (b, r_1) = (r_1, 0) = r_1$, OTHERWISE WE PROCEED AS BEFORE. THIS STEPS CAN BE DONE UNTIL SOME ZERO REMAINDER APPEARS, SAY, AT THE $(m+1)$-TH STAGE WHERE r_{m-1} IS DIVIDED BY r_m. NOTE A ZERO REMAINDER OCCURS SOONER OR LATER BECAUSE THE DECREASING SEQUENCE $|b| > r_1 > r_2 > \ldots \geq 0$ CANNOT CONTAINS MORE THAN $|b|$ INTEGERS. WE THEREFORE HAVE

$$
\begin{aligned}
a &= q_1 b + r_1, & 0 < r_1 < b \\
b &= q_2 . r_1 + r_2, & 0 < r_2 < r_1 \\
r_1 &= q_3 . r_2 + r_3, & 0 < r_3 < r_2 \\
&\vdots \\
r_{m-2} &= q_m . r_{m-1} + r_m, & 0 < r_m < r_{m-1} \\
r_{m-1} &= q_{m+1} . r_m + 0
\end{aligned}
$$

SO, WE HAVE $(a,b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{m-1}, r_m) = (r_m, 0) = r_m$.

THIS SHOWS THAT r_m, THE LAST NONZERO REMAINDER THAT APPEARS, EQUALS (a,b).

Exercise: USE THE EUCLIDEAN ALGORITHM TO FIND $x, y \in \mathbb{Z}$ SUCH THAT

(i) $(990, 187) = 990x + 187y$ (ii) $(2532, 63) = 2532x + 63y$

Solution:

(i) THE APPROPRIATE APPLICATIONS OF THE ADT PRODUCE THE NEXT EQUALITIES:

$$
\begin{aligned}
990 &= 187 . 5 + 55 \\
187 &= 55 . 3 + 22 \\
55 &= 22 . 2 + 11 \\
22 &= 11 . 2 + 0
\end{aligned}
$$

THEN, WE OBSERVE

$$(990, 187) = (187, 55) = (55, 22) = (22, 11) = (11, 0) = 11.$$

TO WRITE 11 AS A LINEAR COMBINATION OF 990 AND 187 WE START THE NEXT-TO-LAST EQUATION $55 = 22.2 + 11$ AND SUCCESSIVELY ELIMINATE THE REMAINDERS 22 AND 55 AS FOLLOWS:

$$\begin{aligned} 11 = 55 - 2.22 &= 55 - 2.(187 - 3.55) \\ &= 55 - 2.187 + 6.55 \\ &= 7.55 - 2.187 \\ &= 7.(990 - 187.5) - 2.187 \\ &= 7.990 - 35.187 - 2.187 \\ &= 7.990 - 37.187 = 990.7 + 187.(-37) \end{aligned}$$

WE THEREFORE HAVE $(990, 187) = 990X + 187Y$ WITH $X = 7$, $Y = -37$.

(ii) THE APPROPRIATE APPLICATIONS OF THE DAT GIVE US THE NEXT EQUATIONS:

$$\begin{aligned} 2532 &= 63.40 + 12 \\ 63 &= 12.5 + 3 \\ 12 &= 3.4 + 0. \end{aligned}$$

THIS SHOWS $(2532, 63) = (63, 12) = (12, 3) = (3, 0) = 3$. NEXT, USING THE ABOVE EQUATIONS WE WILL WRITE $(2532, 63)$ AS A LINEAR COMBINATION OF 2532 AND 63.

TO DO THIS, WE OBSERVE

$$(2532, 63) = 3 = 63 - 12.5 = 63 - (2532 - 63.40).5 = 63 - 2532.5 + 63.200.$$

WE THEREFORE HAVE $(2532, 63) = 2532(-5) + 63.201$.

Exercise: FIND $X, Y, Z \in \mathbb{Z}$ SUCH THAT $(990, 187, 512) = 990X + 187Y + 512Z$

Solution:

BY THE PREVIOUS EXERCISE, WE NOTE $(990, 187) = 11 = 990.7 + 187.(-37)$.

NOW, WE OBSERVE $(990, 187, 512) = ((990, 187), 512) = (11, 512)$.

BY THE DAT WE HAVE THE FOLLOWING EQUATIONS:

$$512 = 46 \cdot 11 + 6$$
$$11 = 6 \cdot 1 + 5$$
$$6 = 5 \cdot 1 + 1$$
$$1 = 1 \cdot 1 + 0$$

THIS SHOWS THAT $(512, 11) = (11, 6) = (6, 5) = (5, 1) = (1, 0) = 1$.

MOREOVER, WE CAN WRITE

$$1 = 6 - 5 = 6 - (11 - 6) = 6 \cdot 2 - 11$$
$$= (512 - 46 \cdot 11) \cdot 2 - 11 = 512 \cdot 2 + 11 \cdot (-93).$$

WE THEREFORE HAVE

$$(990, 187, 512) = (11, 512) = 1 = 512 \cdot 2 + 11 \cdot (-93)$$
$$= 512 \cdot 2 + (990 \cdot 7 + 187 \cdot (-37)) \cdot (-93)$$
$$= 512 \cdot 2 + 990 \cdot 7 \cdot (-93) + 187 \cdot 37 \cdot 93$$
$$= 990 \cdot (-651) + 187 \cdot 3441 + 512 \cdot 2.$$

THEN, WE CAN TAKE $x = -651$, $y = 3441$ AND $z = 2$.

The Diophantine Equation ax+by=c

IT IS CUSTOMARY TO APPLY THE TERM DIOPHANTINE EQUATION TO ANY EQUATION IN ONE OR MORE UNKNOWNS THAT IS TO BE SOLVED IN THE INTEGERS. THE SIMPLEST TYPE OF DIOPHANTINE EQUATION THAT WE SHALL CONSIDER IS THE LINEAR DIOPHANTINE EQUATION IN TWO UNKNOWNS: $ax + by = c$ WHERE $a, b, c \in \mathbb{Z}$ WITH a AND b NOT BOTH ZERO. A SOLUTION OF THIS EQUATION IS A PAIR OF INTEGERS (x_0, y_0) SUCH THAT $ax_0 + by_0 = c$. CONDITIONS FOR SOLVABILITY AND FINDING THE SOLUTIONS, IF POSSIBLE, ARE EASY TO STATE AS WE WILL SEE IN THE FOLLOWING THEOREM.

Theorem 1

Let $a, b, c \in \mathbb{Z}$, a, b not both zero. The linear Diophantine Equation $ax + by = c$ has a solution if and only if $d \mid c$, where $d = gcd(a, b)$. If x_0 and y_0 is any particular solution of this equation, then all other solutions are given by

$$x = x_0 + \frac{b}{d} \cdot t, \qquad y = y_0 - \frac{a}{d} \cdot t,$$

where t is an arbitrary integer.

Exercise: WHICH OF THE FOLLOWING DIOPHANTINE EQUATIONS CANNOT BE SOLVED?

(i) $6x + 51y = 22$ (ii) $33x + 14y = 115$ (iii) $14x + 35y = 93$.

Solution:

IN ORDER TO DETERMINE IF THE GIVEN DIOPHANTINE EQUATIONS CAN OR NOT BE SOLVED, WE WILL USE THE THEOREM ABOVE. SINCE $(6, 51) = 3$ AND 3 DOES NOT DIVIDE 22, THE EQUATION $6x + 51y = 22$ HAS NO INTEGERS SOLUTIONS. SIMILARLY, WE HAVE THAT $(14, 35) = 7$ AND 93 IS NOT A MULTIPLE OF 7. THUS, THE EQUATION $14x + 35y = 93$ NEITHER HAS INTEGER SOLUTIONS. HOWEVER, WE OBSERVE $(33, 14) = 1$. AND $1 \mid 115$. HENCE, THE EQUATION $33x + 14y = 115$ HAS INTEGER SOLUTIONS.

Exercise: DETERMINE ALL SOLUTIONS IN THE INTEGERS OF

$$221x + 35y = 11.$$

Solution:

IN ORDER TO SOLVE THE GIVEN EQUATION WE WILL USE THE THEOREM ABOVE. FIRSTLY, APPLYING THE E.A. WE FIND $(221, 35) = 1$. IN FACT, BY THE DAT WE HAVE

$$\begin{aligned} 221 &= 35 \cdot 6 + 11 \\ 35 &= 11 \cdot 3 + 2 \\ 11 &= 2 \cdot 5 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

AND SO, $(221, 35) = (35, 11) = (11, 2) = (2, 1) = (1, 0) = 1$.

THEN, SINCE $(221, 35) = 1$ AND $1 \mid 11$, THE EQUATION $221x + 35y = 11$ HAS INTEGER SOLUTIONS. TO OBTAIN THE INTEGER 1 AS A LINEAR COMBINATION OF 221 AND 35, WE WORK BACKWARD THROUGH THE PREVIOUS CALCULATIONS, AS

FOLLOWS:

$$1 = 11 - 2.5 = 11 - (35 - 11.3).5 = 11 - 35.5 + 11.15 = 16.11 - 35.5$$
$$= 16.(221 - 35.6) - 35.5 = 16.221 - 35.96 - 35.5 = 221.16 + 35.(-101)$$

UPON MULTIPLYING THIS LAST RELATION BY 11, WE GET

$$11 = 11.1 = 11.(221.16 + 35.(-105))$$
$$= 221.(16.11) + 35.(11.(-105)) = 221.176 + 35.(-1111)$$

THIS MEANS THAT $X = 176$ AND $Y = -1111$ PROVIDE ONE SOLUTION TO OUR DIOPHANTINE EQUATION. EVEN MORE, ALL OTHER SOLUTIONS ARE EXPRESSED BY

$$X = 176 + \frac{35}{1}.t = 176 + 35.t,$$
$$Y = -1111 - \frac{221}{1}.t = -1111 - 221.t,$$

WHERE $t \in \mathbb{Z}$.

Exercise: DETERMINE ALL SOLUTIONS IN THE POSITIVE INTEGERS OF THE FOLLOWING EQUATIONS:

(i) $18X + 5Y = 48$. (iii) $123X + 360Y = 99$.

(ii) $54X + 21Y = 906$. (iv) $158X - 57Y = 7$.

(i)

Solution: In order to determine all solutions in the positive integers of the given Diophantine Equation, we will use Theorem 1 to find all integer solutions and then, we will see which of those solutions give us positive integer solutions.
Applying the Euclidean's Algorithm to the evaluation of $gcd(18, 5)$, we find that $gcd(18, 5) = 1$. In fact,

$$\begin{aligned} 18 &= 5 \cdot 3 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

So, since $gcd(18, 5) = 1$ and $1 \mid 48$, the equation $18x + 5y = 48$ has integer solutions. To obtain the integer 1 as a linear combination of 18 and 5, we work backward through the previous calculations, as follows:

$$1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5 = 2 \cdot (18 - 5 \cdot 3) - 5 = 2 \cdot 18 + (-7) \cdot 5.$$

Upon multiplying this last relation by 48, we get

$$48 = 18 \cdot 96 + 5 \cdot (-336).$$

This means that $x = 96$ and $y = -336$ provide one integer solution to our Diophantine equation. Even more, by Theorem 1, all other integer solutions are expressed by

$$x = 96 + 5 \cdot t, \qquad y = -336 - 18 \cdot t,$$

where t is an arbitrary integer.
Now, since we are looking for positive integer solutions, we need to find those $t \in \mathbb{Z}$ such that $x > 0$ and $y > 0$. This means that $96 + 5t > 0$ and $-336 - 18t > 0$. Equivalently, $-96/5 < t < -56/3$ and so $t = -19$. Then, the only positive integer solution of the equation is $x = 96 + 5 \cdot (-19) = 1$ and $y = -336 - 18 \cdot (-19) = 6$.

(ii)

Solution: In order to determine all solutions in the positive integers of the given Diophantine Equation, we will use Theorem 1 to find all integer solutions and then, we will see which of those solutions give us positive integer solutions.
Applying the Euclidean's Algorithm to the evaluation of $gcd(18, 5)$, we find that $gcd(54, 21) = 3$. In fact,

$$\begin{aligned} 54 &= 21 \cdot 2 + 12 \\ 21 &= 12 \cdot 1 + 9 \\ 12 &= 9 \cdot 3 + 3 \\ 9 &= 3 \cdot 3 + 0 \end{aligned}$$

So, since $gcd(54, 21) = 3$ and $3 \mid 906$, the equation $54x + 21y = 906$ has integer solutions. To obtain the integer 3 as a linear combination of 54 and 21, we work backward through the previous calculations and we get:

$$3 = 54 \cdot 2 + 21 \cdot (-5).$$

Upon multiplying this last relation by $906/3 = 302$, we get

$$906 = 3 \cdot 302 = 54 \cdot (2 \cdot 302) + 5 \cdot ((-5) \cdot 302)54 \cdot 604 + 21 \cdot (-1510).$$

This means that $x = 604$ and $y = -1510$ provide one integer solution to our Diophantine equation. Even more, by Theorem 1, all other integer solutions are expressed by

$$x = 604 + 7 \cdot t, \qquad y = -1510 - 18 \cdot t,$$

where t is an arbitrary integer.
Now, since we are looking for positive integer solutions, we need to find those $t \in \mathbb{Z}$ such that $x > 0$ and $y > 0$. This means that $604 + 7t > 0$ and $-1510 - 18t > 0$. Equivalently, $-604/7 < t < -755/9$ and so $t \in \{-86, -85, -84\}$. Then, the only positive integer solution (x, y) of the equation are $(16, 2)$, $(9, 20)$ and $(2, 38)$.

(iii)

Solution: In order to determine all solutions in the positive integers of the given Diophantine Equation, we will use Theorem 1 to find all integer solutions and then, we will see which of those solutions give us positive integer solutions.
Applying the Euclidean's Algorithm to the evaluation of $gcd(123, 360)$, we find that $gcd(123, 360) = 3$. In fact,

$$\begin{aligned} 360 &= 123 \cdot 2 + 114 \\ 123 &= 114 \cdot 1 + 9 \\ 114 &= 9 \cdot 12 + 6 \\ 9 &= 6 \cdot 1 + 3 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

So, since $gcd(360, 123) = 3$ and $3 \mid 99$, the equation $123x + 360y = 99$ has integer solutions. To obtain the integer 3 as a linear combination of 123 and 360, we work backward through the previous calculations and we get:

$$3 = 123 \cdot 41 + 360 \cdot (-14).$$

Upon multiplying this last relation by $99/3 = 33$, we get

$$99 = 123 \cdot 1353 + 360 \cdot (-462).$$

This means that $x = 1353$ and $y = -462$ provide one integer solution to our Diophantine equation. Even more, by Theorem 1, all other integer solutions are expressed by

$$x = 1353 + 120 \cdot t, \qquad y = -462 - 41 \cdot t,$$

where t is an arbitrary integer.
Now, since we are looking for positive integer solutions, we need to find those $t \in \mathbb{Z}$ such that $x > 0$ and $y > 0$. This means that $1353 + 120t > 0$ and $-462 - 41t > 0$. Equivalently, $-1353/120 < t < -462/41$ and so there is no integer t verifying these conditions. Consequently, the equations has no positive integer solutions.

(iv)

Solution: In order to determine all solutions in the positive integers of the given Diophantine Equation, we will use Theorem 1 to find all integer solutions and then, we will see which of those solutions give us positive integer solutions.
Applying the Euclidean's Algorithm to the evaluation of $gcd(158, -57)$, we find that $gcd(158, -57) = gcd(158, 57) = 1$. In fact,

$$\begin{aligned}
158 &= 57 \cdot 2 + 44 \\
57 &= 44 \cdot 1 + 13 \\
44 &= 13 \cdot 3 + 5 \\
13 &= 5 \cdot 2 + 3 \\
5 &= 3 \cdot 1 + 2 \\
3 &= 2 \cdot 1 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

So, since $gcd(158, -57) = 1$ and $1 \mid 7$, the equation $158x - 57y = 7$ has integer solutions. To obtain the integer 1 as a linear combination of 158 and 57, we work backward through the previous calculations and we get $1 = 158 \cdot (-22) + 57 \cdot 61$. Then,

$$-1 = 158 \cdot 22 + (-57) \cdot 61.$$

Upon multiplying this last relation by -7, we get

$$7 = 158 \cdot (-154) + (-57) \cdot (-427).$$

This means that $x = -154$ and $y = -427$ provide one integer solution to our Diophantine equation. Even more, by Theorem 1, all other integer solutions are expressed by

$$x = -154 - 57 \cdot t, \qquad y = -427 - 158 \cdot t,$$

where t is an arbitrary integer.
Now, since we are looking for positive integer solutions, we need to find those $t \in \mathbb{Z}$ such that $x > 0$ and $y > 0$. This means that $-154 - 57 \cdot t > 0$ and $-427 - 158 \cdot t > 0$. Equivalently, $t < -154/57$ and $t < -427/158$. So, $t \leq -3$. Consequently, there are infinitely many positive integer solutions.

Exercise: FIND THE NUMBER OF MEN, WOMEN AND CHILDREN IN A COMPANY OF 20 PERSONS IF TOGETHER THEY PAY 20 COINS, EACH MAN PAYING 3, EACH WOMAN 2 AND EACH CHILDREN 1/2.

Solution: Let M, W and C denote the number of men, women and children in the company respectively. We observe that $0 < M, W, C < 20$ and

$$M + W + C = 20, \tag{1}$$

$$3M + 2W + \frac{1}{2}C = 20. \tag{2}$$

Consequently, from (1) and (2) we get

$$2 \cdot \left(3M + 2W + \frac{1}{2}C\right) - (M + W + C) = 40 - 20.$$

That is, $5M + 3W = 20$. This means that to solve our problem, we need to find all possible solutions of the Diophantine equation $5M + 3W = 20$ where $0 < M, W < 20$.
Since $gcd(5, 3) = 1$ and $1 \mid 20$, by Theorem 1, the equation $5M + 3W = 20$ has integer solutions. To obtain the integer 1 as a linear combination of 5 and 3, we observe:

$$1 = 5 \cdot (-1) + 3 \cdot 2.$$

Upon multiplying this last relation by 20, we get

$$20 = 5 \cdot (-20) + 3 \cdot 40.$$

This means that $M = -20$ and $W = 40$ provide one integer solution to our Diophantine equation. Even more, by Theorem 1, all other integer solutions are expressed by

$$M = -20 + 3 \cdot t, \qquad W = 40 - 5 \cdot t,$$

where t is an arbitrary integer.
Now, since we are looking for positive integer solutions $0 < M, W < 20.$, we need to find those $t \in \mathbb{Z}$ such that $0 < M < 20$ and $0 < W < 20$. This means that $0 < -20 + 3 \cdot t < 20$ and $0 < 40 - 5 \cdot t < 20$. Equivalently, $20/3 < t < 40/3$ and $4 < t < 8$. so, $t = 7$. Then, the only positive integer solution (M, W) of the equation is $(1, 5)$. Hence, $M = 1$, $W = 5$ and so $C = 14$. Consequently, there are 1 man, 5 women and 14 children in the company.

Exercise: IF a AND b ARE COPRIME POSITIVE INTEGERS, PROVE THE EQUATION $ax-by=c$ HAS INFINITELY MANY SOLUTIONS IN THE POSITIVE INTEGERS.

Solution: Since $gcd(a, -b) = gcd(a, b) = 1$ and $1 \mid c$, by Theorem 1, the equation $ax - by = c$ has integer solutions. Then, there exist integers x_0 and y_0 such that $ax_0 - by_0 = c$. Even more, by Theorem 1, all other integer solutions are expressed by

$$x = x_0 - b \cdot t, \qquad y = y_0 - a \cdot t,$$

where t is an arbitrary integer.
Now, since we are looking for positive integer solutions, we need to find those $t \in \mathbb{Z}$ such that $x > 0$ and $y > 0$. This means that $x_0 - b \cdot t > 0$ and $y_0 - a \cdot t > 0$. Equivalently, as a, b are positive, $t < \frac{x_0}{b}$ and $t < \frac{y_0}{a}$. So, we can take every integer t such that $t < \min\{\frac{x_0}{a}, \frac{y_0}{b}\}$. In fact, if $t < \min\{\frac{x_0}{a}, \frac{y_0}{b}\}$ then $t < \frac{x_0}{b}$ and $t < \frac{y_0}{a}$ which implies that $x_0 - bt > 0$ and $y_0 - at > 0$, i.e., $x > 0$ and $y > 0$. Consequently, there are infinitely many positive integer solutions by choosing $t < \min\{\frac{x_0}{a}, \frac{y_0}{b}\}$.