Number Theory Exercises 5

Jason Sass

June 18, 2023

Linear Diophantine Equations

Exercise 1. Find a general solution to the linear Diophantine equation $172x + 20y = 1000$.

Solution. We use Euclid's algorithm to compute $\gcd(172, 20)$.
Observe that

$$\begin{aligned} 172 &= 20 * 8 + 12 \\ 20 &= 12 * 1 + 8 \\ 12 &= 8 * 1 + 4 \\ 8 &= 4 * 2 + 0. \end{aligned}$$

Thus, $\gcd(172, 20) = 4$.
We express the gcd as a linear combination of 172 and 20.

$$\begin{aligned} 4 &= 12 - (8)1 \\ &= 12 - (20 - 12 * 1)1 \\ &= (12) * 2 - 20 * 1 \\ &= (172 - 20 * 8) * 2 - 20 * 1 \\ &= 172 * 2 - 20(17) \\ &= 172 * 2 + 20(-17). \end{aligned}$$

Thus, $\gcd(172, 20) = 4 = 172 * 2 + 20(-17)$, so $1000 = 250 * 4 = 250(172 * 2 + 20(-17)) = 500 * 172 + 20(-4250)$.
Hence, a particular solution is $x_0 = 500$ and $y_0 = -4250$.
Therefore, a general solution is $x = 500 + (\frac{20}{4})t = 500 + 5t$ and $y = -4250 - (\frac{172}{4})t = -4250 - 43t$ for some integer t. ☐

Exercise 2. Find a general solution to the linear Diophantine equation $5x + 22y = 18$.

Solution. A particular solution is $x_0 = 8$ and $y_0 = -1$ since $18 = 5(8)+22(-1)$.

Since $\gcd(5, 22) = 1$, then a general solution is $x = 8 + 22t$ and $y = -1 - 5t$ for arbitrary integer t. $\square$

Exercise 3. Let $a, b \in \mathbb{Z}^+$.

If a and b are relatively prime, then the Diophantine equation $ax - by = c$ has infinitely many solutions in $\mathbb{Z}^+$.

Proof. Suppose a and b are relatively prime.

Then $\gcd(a, b) = 1$.

Since $\gcd(a, -b) = \gcd(a, b) = 1$ and $c = ax - by = ax + (-b)y$ and $1|c$, then a solution exists to the Diophantine equation $ax - by = c$.

Let $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ be a particular solution to the equation $ax - by = c$.

Then $x_0 \in \mathbb{Z}$ and $y_0 \in \mathbb{Z}$ and $ax_0 - by_0 = c$.

Let $m = \min(\frac{x_0}{b}, \frac{y_0}{a})$.

Then $m \leq \frac{x_0}{b}$ and $m \leq \frac{y_0}{a}$.

Let $t \in \mathbb{Z}$ such that $t < m$.

Let $x = x_0 - bt$ and $y = y_0 - at$.

To prove the equation $ax - by = c$ has infinitely many solutions in $\mathbb{Z}^+$, we must prove (x, y) is a solution to the equation $ax - by = c$ in $\mathbb{Z}^+ \times \mathbb{Z}^+$ for each $t \in \mathbb{Z}$.

Thus, we must prove $ax - by = c$ and $x > 0$ and $y > 0$ for each $t \in \mathbb{Z}$.

Observe that

$$\begin{aligned} ax - by &= a(x_0 - bt) - b(y_0 - at) \\ &= ax_0 - abt - by_0 + bat \\ &= ax_0 - abt - by_0 + abt \\ &= ax_0 - by_0 \\ &= c. \end{aligned}$$

Therefore, $ax - by = c$.

Since $t < m$ and $m \leq \frac{x_0}{b}$, then $t < \frac{x_0}{b}$.

Since $b > 0$, then $bt < x_0$, so $0 < x_0 - bt = x$.

Therefore, $x > 0$.

Since $t < m$ and $m \leq \frac{y_0}{a}$, then $t < \frac{y_0}{a}$.

Since $a > 0$, then $at < y_0$, so $0 < y_0 - at = y$.

Therefore, $y > 0$. $\square$

Proposition 4. *Let $a, b, c \in \mathbb{Z}^*$ and $d \in \mathbb{Z}^+$.*

If $d = \gcd(a, b, c)$, then $d = \gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c)) = \gcd(\gcd(a, c), b)$.

Proof. Suppose $d = \gcd(a, b, c)$.

We first prove $d = \gcd(\gcd(a, b), c)$.

Let $x = \gcd(a, b)$.

Then $x \in \mathbb{Z}^+$ and $x|a$ and $x|b$, and for any integer n, if $n|a$ and $n|b$, then $n|x$.

Since $d = \gcd(a, b, c)$, then $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$ and $d|c$, and for any integer n, if $n|a$ and $n|b$ and $n|c$, then $n|d$.

Since $d|a$ and $d|b$, then $d|x$.

Since $d|x$ and $d|c$, then d is a common divisor of x and c.

Let $n \in \mathbb{Z}$ such that $n|x$ and $n|c$.

Since $n|x$ and $x|a$, then $n|a$.

Since $n|x$ and $x|b$, then $n|b$.

Since $n|a$ and $n|b$ and $n|c$, then $n|d$.

Thus, any common divisor of x and c divides d.

Since $d \in \mathbb{Z}^+$ and d is a common divisor of x and c and any common divisor of x and c divides d, then $d = \gcd(x, c)$.

Therefore, $d = \gcd(x, c) = \gcd(\gcd(a, b), c)$. □

Proof. We next prove $d = \gcd(a, \gcd(b, c))$.

Let $x = \gcd(b, c)$.

Then $x \in \mathbb{Z}^+$ and $x|b$ and $x|c$, and for any integer n, if $n|b$ and $n|c$, then $n|x$.

Since $d = \gcd(a, b, c)$, then $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$ and $d|c$, and for any integer n, if $n|a$ and $n|b$ and $n|c$, then $n|d$.

Since $d|b$ and $d|c$, then $d|x$.

Since $d|a$ and $d|x$, then d is a common divisor of a and x.

Let $n \in \mathbb{Z}$ such that $n|a$ and $n|x$.

Since $n|x$ and $x|b$, then $n|b$.

Since $n|x$ and $x|c$, then $n|c$.

Since $n|a$ and $n|b$ and $n|c$, then $n|d$.

Thus, any common divisor of a and x divides d.

Since $d \in \mathbb{Z}^+$ and d is a common divisor of a and x and any common divisor of a and x divides d, then $d = \gcd(a, x)$.

Therefore, $d = \gcd(a, x) = \gcd(a, \gcd(b, c))$. □

Proof. We next prove $d = \gcd(\gcd(a, c), b)$.

Let $x = \gcd(a, c)$.

Then $x \in \mathbb{Z}^+$ and $x|a$ and $x|c$, and for any integer n, if $n|a$ and $n|c$, then $n|x$.

Since $d = \gcd(a, b, c)$, then $d \in \mathbb{Z}^+$ and $d|a$ and $d|b$ and $d|c$, and for any integer n, if $n|a$ and $n|b$ and $n|c$, then $n|d$.

Since $d|a$ and $d|c$, then $d|x$.

Since $d|x$ and $d|b$, then d is a common divisor of x and b.

Let $n \in \mathbb{Z}$ such that $n|x$ and $n|b$.

Since $n|x$ and $x|a$, then $n|a$.

Since $n|x$ and $x|c$, then $n|c$.

Since $n|a$ and $n|b$ and $n|c$, then $n|d$.

Thus, any common divisor of x and b divides d.

Since $d \in \mathbb{Z}^+$ and d is a common divisor of x and b and any common divisor of x and b divides d, then $d = \gcd(x, b)$.

Therefore, $d = \gcd(x, b) = \gcd(\gcd(a, c), b)$. □

Proposition 5. *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$ and $b \neq 0$ and $c \neq 0$ and $d \in \mathbb{Z}$.*

Then the Diophantine equation $ax + by + cz = d$ is solvable in the integers iff $\gcd(a, b, c) \mid d$.

Proof. We prove the statement : if $\gcd(a, b, c) \mid d$, then $ax + by + cz = d$ is solvable in the integers.

Suppose $\gcd(a, b, c) \mid d$.

To prove $ax + by + cz = d$ is solvable in the integers, we must prove there exist integers x_0, y_0, z_0 such that $ax_0 + by_0 + cz_0 = d$.

Let $r = \gcd(a, b, c)$.

Let $s = \gcd(a, b)$.

Then $r|d$, so $d = rk$ for some integer k.

Since $r = \gcd(a, b, c) = \gcd(\gcd(a, b), c) = \gcd(s, c)$, then r is a linear combination of s and c, so there exist integers m and n such that $ms + nc = r$.

Since $s = \gcd(a, b)$, then s is a linear combination of a and b, so there exist integers p and q such that $pa + qb = s$.

Observe that

$$\begin{aligned}
d &= rk \\
&= (ms + nc)k \\
&= [m(pa + qb) + nc]k \\
&= (mpa + mqb + nc)k \\
&= mpak + mqbk + nck \\
&= a(mpk) + b(mqk) + c(nk).
\end{aligned}$$

Let $x_0 = mpk$ and $y_0 = mqk$ and $z_0 = nk$.

Then $x_0, y_0, z_0 \in \mathbb{Z}$ and $d = ax_0 + by_0 + cz_0$. □

Proof. We prove the statement: if $ax + by + cz = d$ is solvable in the integers, then $\gcd(a, b, c) \mid d$.

Suppose $ax + by + cz = d$ is solvable in the integers.

Then there exist integers x_0, y_0, z_0 such that $ax_0 + by_0 + cz_0 = d$, so d is a linear combination of a, b, c.

Since $\gcd(a, b, c)$ is a common divisor of a and b and c, then $\gcd(a, b, c)$ divides any linear combination of a and b and c, so $\gcd(a, b, c) \mid d$. □

Exercise 6. Find all solutions in the integers of the equation $15x+12y+30z = 24$.

Solution. The linear diophantine equation $15x + 12y + 30z = 24$ has a solution in the integers iff $\gcd(15, 12, 30)|24$.

Since $\gcd(15, 12, 30) = \gcd(\gcd(15, 12), 30) = \gcd(3, 30) = 3$ and $3|24$, then the equation $15x + 12y + 30z = 24$ has a solution in the integers.

Since $15x + 12y + 30z = 24$, then $12y + 30z = 24 - 15x$.

The linear diophantine equation $12y + 30z = 24 - 15x$ has a solution for a fixed integer x iff $\gcd(12, 30) \mid (24 - 15x)$.

Since $\gcd(12, 30) = 6$ and $6 \mid (24 - 15x)$ iff $3 * 2 \mid 3(8 - 5x)$ iff $2 \mid (8 - 5x)$ iff $8 - 5x = 2s$ for some integer s, then $12y + 30z = 24 - 15x$ has a solution for a fixed integer x iff $8 - 5x = 2s$ for some integer s.

Let $s \in \mathbb{Z}$ such that $8 - 5x = 2s$.

Then $5x = 8-2s$, so $24-15x = 24-3(5x) = 24-3(8-2s) = 24-24+6s = 6s$.

We find a solution to the equation $12y + 30z = 24 - 15x$.

We first use the Euclidean algorithm to find $\gcd(12, 30)$.

Observe that

$$\begin{aligned} 30 &= 12 * 2 + 6 \\ 12 &= 6 * 2 + 0. \end{aligned}$$

Thus, $\gcd(12, 30) = 6 = 30 - (12)2 = 12(-2) + 30(1)$.

Hence,

$$\begin{aligned} 24 - 15x &= 6s \\ &= \gcd(12, 30) * s \\ &= [12(-2) + 30(1)] * s \\ &= 12(-2s) + 30s. \end{aligned}$$

Therefore, a particular solution to the equation $12y + 30z = 24 - 15x$ is $(-2s, s)$, so a general solution is $y = -2s + \frac{30t}{6} = -2s + 5t$ and $z = s - \frac{12t}{6} = s - 2t$ for any integer t.

Since $8 - 5x = 2s$, then $5x = 8 - 2s$, so $x = \frac{8-2s}{5}$.

Since $x \in \mathbb{Z}$, then $5|(8 - 2s)$, so $5|2(4 - s)$.

Since $\gcd(5, 2) = 1$, then this implies $5|(4 - s)$, so $4 - s = 5k$ for some integer k.

Thus, $s = 4 - 5k$.

Hence, $z = (4-5k)-2t = 4-5k-2t$ and $y = -2(4-5k)+5t = -8+10k+5t$ and $x = \frac{8-2(4-5k)}{5} = \frac{10k}{5} = 2k$.

Observe that

$$\begin{aligned} 15x + 12y + 30z &= 15(2k) + 12(-8 + 10k + 5t) + 30(4 - 5k - 2t) \\ &= 30k - 96 + 120k + 60t + 120 - 150k - 60t \\ &= -96 + 120 \\ &= 24. \end{aligned}$$

Therefore, a general solution to the equation $15x + 12y + 30z = 24$ is $x = 2k$ and $y = -8 + 10k + 5t$ and $z = 4 - 5k - 2t$ for integers k and t. $\square$

Exercise 7. A man has \$4.55 in change composed entirely of dimes and quarters. What are the maximum and minimum number of coins that he can have? Is it possible for the number of dimes to equal the number of quarters?

Solution. Let d be the number of dimes and q be the number of quarters.

Then $10d + 25q = 455$, so this is a linear Diophantine equation.

This equation has a solution iff $\gcd(10, 25) \mid 455$.

Since $\gcd(10, 25) = 5$ and $5|455$, then the equation $10d + 25q = 455$ has a solution in the integers.

We find a particular solution using the Euclidean algorithm.

Observe that

$$\begin{aligned} 25 &= 10 * 2 + 5 \\ 10 &= 5 * 2 + 0. \end{aligned}$$

Thus, $\gcd(10, 25) = 5 = 25 - (10)2 = 10(-2) + 25(1)$.

Hence,

$$\begin{aligned} 455 &= 91 \cdot 5 \\ &= 91 \cdot \gcd(10, 25) \\ &= 91[10(-2) + 25(1)] \\ &= 10(-182) + 25(91). \end{aligned}$$

Therefore, a particular solution to the equation $10d+25q = 455$ is $(-182, 91)$, so a general solution is $d = -182+(\frac{25}{5})t = -182+5t$ and $q = 91-(\frac{10}{5})t = 91-2t$ for any integer t.

Since $d \geq 0$ and $q \geq 0$, then $-182 + 5t \geq 0$ and $91 - 2t \geq 0$.

This leads to $t \geq 36.4$ and $t \leq 45.5$, so $37 \leq t \leq 45$.

We compute the various values of d and q for each t in the integer range $[37, 45]$.

The maximum number of coins is 44 coins, with 43 dimes and 1 quarter.

The minimum number of coins is 20 coins, with 3 dimes and 17 quarters.

There can be an equal number of dimes and quarters, with 13 dimes and 13 quarters. □

Exercise 8. A theatre charges \$1.80 for adult admissions and 75 cents for children. On a particular evening the total receipts were \$90. Assuming that more adults than children were present, how many people attended?

Solution. Let x be the number of adults and y be the number of children that attended.

Then $180x + 75y = 9000$, so this is a linear Diophantine equation.

This equation has a solution iff $\gcd(180, 75) \mid 9000$.

Since $\gcd(180, 75) = 15$ and $15|9000$, then the equation $180x + 75y = 9000$ has a solution in the integers.

We find a particular solution using the Euclidean algorithm.

Observe that

$$\begin{aligned} 180 &= 75 * 2 + 30 \\ 75 &= 30 * 2 + 15 \\ 30 &= 15 * 2 + 0. \end{aligned}$$

Thus,

$$\begin{aligned} \gcd(180, 75) &= 15 \\ &= 75 - (30)2 \\ &= 75 - (180 - 75 * 2)2 \\ &= 75 - 180 * 2 + 75 * 4 \\ &= 75(5) - 180(2) \\ &= 180(-2) + 75(5). \end{aligned}$$

Hence,

$$\begin{aligned} 9000 &= 600 \cdot 15 \\ &= 600 \cdot \gcd(180, 75) \\ &= 600[180(-2) + 75(5)] \\ &= 180(-1200) + 75(3000). \end{aligned}$$

Therefore, a particular solution to the equation $180x+75y = 9000$ is $(-1200, 3000)$, so a general solution is $x = -1200+(\frac{75}{15})t = -1200+5t$ and $y = 3000-(\frac{180}{15})t = 3000 - 12t$ for any integer t.

Since $x \geq 0$ and $y \geq 0$, then $-1200 + 5t \geq 0$ and $3000 - 12t \geq 0$.

This leads to $t \geq 240$ and $t \leq 250$, so $240 \leq t \leq 250$.

We compute the various values of x and y for each t in the integer range $[240, 250]$.

There are either 40 adults and 24 children or 45 adults and 12 children or only 50 adults and no children that attended. □