MATH-3420 - Assignment 1

Jonathon Meney

September 2023

1. Use the Extended Euclidean Algorithm to find an integer solution to the equation $852x + 1740y = \gcd(852, 1740)$.

   Euclidean Algorithm:

$$\begin{aligned} 1740 &= 852(2) + 36 \\ 852 &= 36(23) + 24 \\ 36 &= 24(1) + 12 \\ 24 &= 12(2) + 0 \end{aligned}$$

   Solve for remainders:

$$\begin{aligned} 36 &= 1740 - 852(2) \\ 24 &= 852 - 36(23) \\ 12 &= 36 - 24(1) \end{aligned}$$

   Back substitute:

$$\begin{aligned} 12 &= 36 - 24(1) \\ 12 &= 1740(1) - 852(2) - (852 - 36(23)) \\ 12 &= 1740(1) + 852(-3) + 36(23) \\ 12 &= 1740(1) + 852(-3) + (1740 - 852(2))(23) \\ 12 &= 1740(1) + 852(-3) + 1740(23) + 852(-46) \\ 12 &= 1740(24) + 852(-49) \end{aligned}$$

   Therefore $x = -49$ and $y = 24$.

2. For each of the following, find **all** integer solutions or explain why no solution exists, using methods from Section 3.1 of the text. (You don't need to explain how you found the initial solution.)

   (a) $852x + 1740y = -22$
   Since $c = -22$ and is not a multiple of $d = \gcd(1740, 852) = 12$ (as per the previous question) there is no solutions.

   (b) $21x + 56y = 7$
   Euclidean Algorithm:

$$\begin{aligned} 56 &= 21(2) + 14 \\ 21 &= 14(1) + 7 \\ 14 &= 7(2) + 0 \end{aligned}$$

   Since $d = \gcd(56, 21) = 7 = c$ there is infinitely many solutions.
   Solve for remainders:

$$\begin{aligned} 14 &= 56 - 21(2) \\ 7 &= 21 - 14(1) \end{aligned}$$

   Back substitute:

$$\begin{aligned} 7 &= 21 - 14(1) \\ 7 &= 21 - (56 - 21(2)) \\ 7 &= 21 - 56 + 21(2) \\ 7 &= 21(3) + 56(-1) \end{aligned}$$

   Therefore our initial solution is $x = 3$ and $y = -1$.
   Thus, $x = 3 + \frac{56}{7}n$ and $y = -1 - \frac{21}{7}n$ which simplifies to $x = 3 + 8n$ and $y = -1 - 3n$ where $n \in \mathbb{Z}$ will generate all solutions.

   (c) $5x - 12y = 0$
   Euclidean Algorithm:

$$\begin{aligned} -12 &= 5(-3) + 3 \\ 5 &= 3(1) + 2 \\ 3 &= 2(1) + 1 \\ 2 &= 1(2) + 0 \end{aligned}$$

   Since $d = \gcd(5, -12) = 1$ is a multiple $c = 0$, we have infinitely many solutions.
   Therefore, using the trivial solution $x = 0$, $y = 0$, and $5(0) - 12(0) = 0$, we have that, $x = 12n$ and $y = 5n$ where $n \in \mathbb{Z}$, will generate all solutions.

3. Suppose you have been saving quarters (\$0.25), loonies (\$1) and toonies (\$2) in a jar. You have 82 coins and \$70 total. How many different collections of coins can you have?

   Define x as the number of quarters, y as the number of loonies, and z as the number of toonies.

   Total coins can be defined as:

$$x + y + z = 82$$
$$x = 82 - y - z$$

   Total value can be defined as:

$$\begin{aligned} 0.25x + y + 2z &= 70 \\ 4(0.25x + y + 2z) &= 4(70) \\ x + 4y + 8z &= 280 \end{aligned}$$

   Substitute total coin equation into total value equation:

$$\begin{aligned} x + 4y + 8z &= 280 \\ 82 - y - z + 4y + 8z &= 280 \\ 3y + 7z &= 198 \end{aligned}$$

   Euclidean Algorithm:

$$\begin{aligned} 7 &= 3(2) + 1 \\ 3 &= 1(3) + 0 \end{aligned}$$

   Solve for remainders:

$$1 = 7 + 3(-2)$$

   Therefore our initial solution is $y = -2$ and $z = 1$. Since $c = 198$ is a multiple of $d = \gcd(3, 7) = 1$ we have that:

$$\begin{aligned} d &= 3y + 7z \\ 1 &= 3y + 7z \\ 1 &= 3(-2) + 7(1) \\ 198(1) &= 198(3(-2) + 7(1)) \\ 198 &= 3(-396) + 7(198) \end{aligned}$$

   Which gives us that $y = -396 + 7n$ and $z = 198 - 3n$ where $n \in \mathbb{Z}$. It also follows that $57 \leq n \leq 66$ as we cannot have negative amounts of coins. Therefore, we can conclude that there is 10 different collections of coins possible.

4. Suppose a, b, and c are positive integers. From Proposition 2.4.10., we know that if $\gcd(a, b) = 1$ and $a|bc$, then $a|c$. We can generalize that result as follows:

$$\text{If } \gcd(a, b) = d \text{ and } a|bc, \text{ then } a|dc.$$

Prove this generalization.

Proof. Suppose a, b, and c are positive integers. From Proposition 2.4.10., we know that if $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

To prove the generalization first assume $\gcd(a, b) = d$ and $a|bc$.

We know that from $\gcd(a, b) = d$:

$$d = ax + by$$

and therefore multiplying by c we have that:

$$dc = acx + bcy$$

and since $a|bc$ there exists some integer k such that $bc = ak$ therefore:

$$\begin{aligned} dc &= acx + aky \\ dc &= a(cx + ky) \end{aligned}$$

Thus we see that $a|dc$.

Therefore we've proven the generalization that, if $\gcd(a, b) = d$ and $a|bc$, then $a|dc$. $\square$