Problem Set 2: GCDs and The Euclidean Algorithm

5) Find an integer solution to the following Diophantine equations:

(a) $4x + 15y = 1$ *(try this one without the Euclidean algorithm - can you quickly guess x and y?)*

Solution: We can guess x and y here. If $x = 4$ and $y = -1$, we have $4x + 15y = 16 - 15 = 1$. ■

(b) $7x + 9y = 1$

Solution: We can also do this one without a Euclidean Algorithm! With $x = 4$ and $y = -3$, we have $7x + 9y = 28 - 27 = 1$. ■

(c) $26x + 38y = 6$

Solution: This one isn't as obvious, so let's use the algorithm. We'll do the workings in tandem with solving for the remainders

Equation	Solved for Remainder
$38 = 1 \cdot 26 + 12$	$12 = 38 - 1 \cdot 26$
$26 = 2 \cdot 12 + 2$	$2 = 26 - 2 \cdot 12$
$12 = 6 \cdot 2 + 0$	*don't rearrange this one*

Therefore, we have

$$\begin{aligned} 2 &= 26 - 2 \cdot 12 \\ &= 26 - 2(38 - 1 \cdot 26) \\ &= 3 \cdot 26 - 2 \cdot 38. \end{aligned}$$

Therefore,

$$26 \cdot 3 + 38 \cdot (-2) = 2.$$

But that's not the equation we wanted! We wanted the right-hand side to be 6. We can simply multiply the entire equation by 3 to achieve this.

$$\begin{aligned} & 3 \cdot (26 \cdot 3 + 38 \cdot (-2)\,) = 3 \cdot 2 \\ \Rightarrow\ & 26 \cdot 9 + 38 \cdot (-6) = 6. \end{aligned}$$

Therefore, with $x = 9$ and $y = -6$, we have $26x + 38y = 6$. ■

6) Compute the following inverses in $\mathbb{Z}_n$. You will want to use your work in Question **5)** for all of these!

(a) 4^{-1} in $\mathbb{Z}_{15}$

Solution: From Question **5**, we had that $4 \cdot 4 + 15 \cdot (-1) = 1$. Modulo 15, this equation becomes $4 \cdot 4 + 0 \equiv 1 \pmod{15}$, so $4^{-1} \equiv 4 \pmod{15}$. ■

(b) 7^{-1} in $\mathbb{Z}_9$

Solution: From Question **5**, we had that $7 \cdot 4 + 9 \cdot (-3) = 1$. Modulo 9, this equation becomes $7 \cdot 4 + 0 \equiv 1 \pmod 9$, so $7^{-1} \equiv 4 \pmod 9$. ■

(c) 2^{-1} in $\mathbb{Z}_7$

Solution: Look back at the equation used in part **(b)**. Modulo 7, we have $9 \equiv 2 \,(\text{mod } 7)$.

So if we reduce the equation $7 \cdot 4 + 9 \cdot (-3) = 1$ modulo 7 instead of 9, we get our result! Thus, modulo 7, we have $2 \cdot -3 \equiv 1 \pmod 7$, so $2^{-1} \equiv -3 \equiv 4 \pmod 7$. *4 is popular in this question!*

(d) 13^{-1} in $\mathbb{Z}_{19}$

Solution: From Question **5**, it doesn't look like we have any information to use on first glance. However, since 13 is half of 26 and 19 is half of 38, we can divide the linear combination for the gcd of 26 and 38 by in the solution to **5 (c)** by 2 to arrive at our answer.

We had $26 \cdot 3 + 38(-2) = 2$. Dividing by 2, we have $13 \cdot 3 + 19(-2) = 1$. Reducing modulo 19, we have $13 \cdot 3 \equiv 1 \pmod{19}$, so $13^{-1} \equiv 3 \pmod{19}$. ■

7) The extended Euclidean algorithm applied to a and b provides **one** solution to the equation $ax + by = g$ where $g = \gcd(a, b)$, but there are many more solutions! To this end, find **three** different pairs of integers (x, y) such that $4x + 3y = 1$.

Solution: First, the obvious: $(x, y) = (1, -1)$ is a solution. From there, think of multiples of 4 and 3 that are one apart. We have $9 - 8 = 1$ and $16 - 15 = 1$. So pairs $(x, y) = (-2, 3)$ and $(4, -5)$ both work here. An infinite number of pairs exist - these are just the "easiest" three to find! ■

8) For a positive integer d and an integer n, remember that if $n \equiv r \pmod d$ where $0 \le r < d$, then $n = qd + r$ for some $q \in \mathbb{Z}$.

Let $n \in \mathbb{Z}$ be positive and set $d = 2$. Prove the following statements:

(a) If $n \equiv 0 \pmod 2$, then $\gcd(n, n+2) = 2$. *(if $n \equiv 0 \pmod 2$, what kind of number is n?)*

Proof: If $n \equiv 0 \pmod 2$, then n is even! Let $n = 2k$ for some $k \in \mathbb{Z}$, so $n + 2 = 2k + 2$. Then

$$2k + 2 = 2k \cdot 1 + 2$$
$$2k = k \cdot 2 + 0.$$

Therefore, the gcd is 2 by the Euclidean algorithm. □

(b) If $n \equiv 1 \pmod 2$, then $\gcd(n, n+2) = 1$. *(if $n \equiv 1 \pmod 2$, what kind of number is n?)*

Proof: If $n \equiv 1 \pmod 2$, then n is odd! Let $n = 2k+1$ for some $k \in \mathbb{Z}$, so $n+2 = 2k+3$. Then

$$2k+3 = 1 \cdot (2k+1) + 2$$

$$2k+1 = k \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0.$$

Therefore, the gcd is 1 by the Euclidean algorithm. □

9) For $a, d \in \mathbb{Z}$ where $d \neq 0$, restate the definition of $d \mid a$ in the language of modular arithmetic.

Solution: If $d \mid a$, then $a = qd$ for some $q \in \mathbb{Z}$. Reducing modulo d, we have that $d \mid a$ when $a \equiv 0 \pmod d$. ■

10) Prove that $\mathbb{Z}_p^* = \{1, 2, 3, ..., p-1\}$.

Proof: Since p is a prime, if $\gcd(x, p) \neq 1$, then it **must** be p, since p is prime! Since $p > x$ for all $x \in \mathbb{Z}_p$, we have that $\gcd(x, p) = 1$ for $1 \leq x \leq p-1$, so $\mathbb{Z}_p* = \{1, 2, 3, ..., p-1\}$. □

11) Prove the following for $a, b, d \in \mathbb{Z}$:

(a) If $d \mid a$ then $d \mid ca$ for **any** $c \in \mathbb{Z}$.

Proof: Let $c \in \mathbb{Z}$. If $d \mid a$, then $a \equiv 0 \pmod d$. Thus $ca \equiv c \cdot 0 \equiv 0 \pmod d$, so $d \mid ca$. As c was chosen arbitarily, this holds for all integers $c \in \mathbb{Z}$. □

(b) If $d \mid a$ and $d \mid b$ then $d \mid (a+b)$.

Proof: If $d \mid a$ and $d \mid b$, then $a \equiv 0 \pmod d$ and $b \equiv 0 \pmod d$. Then $a+b \equiv 0+0 \equiv 0 \pmod d$, so $d \mid (a+b)$. □

(c) If $d \mid a$ and $d \mid b$ then $d \mid (ax+by)$ for any $x, y \in \mathbb{Z}$.

Proof: Let $x, y \in \mathbb{Z}$ be arbitrary integers. If $d \mid a$ and $d \mid b$, then $a \equiv 0 \pmod d$ and $b \equiv 0 \pmod d$. Thus $ax + by \equiv 0 \cdot x + 0 \cdot y \equiv 0 \pmod d$, so $d \mid (ax+by)$ for any $x, y \in \mathbb{Z}$. □

(d) Let $k \in \mathbb{Z}$ be a common divisor of a and b; that is, $k \mid a$ and $k \mid b$. Prove that $k \mid \gcd(a, b)$.

Proof: If $d = \gcd(a, b)$ then there exists integers x and y such that $ax + by = d$. From part **(c)** above, if $k \mid a$ and $k \mid b$, then $k \mid (ax + by)$. Therefore, $k \mid d$. $\square$

12) In $\mathbb{Z}_n$, we can't divide by any number that has a common factor with n. However, we *CAN* divide **congruences** by common factors!

Suppose that $a, b, n \in \mathbb{Z}$ have a common factor of k, where $k \in \mathbb{Z}$, $k \neq 0$, and $n \neq 0$. Prove the following statement:

$$\text{If } a \equiv b \pmod{n}, \text{ then } \frac{a}{k} \equiv \frac{b}{k} \left(\text{mod } \frac{n}{k}\right).$$

Proof: Suppose $a \equiv b \pmod{n}$. Then $a - b \equiv 0 \pmod{n}$, so $a - b = qn$ for some $q \in \mathbb{Z}$. Now, if k is a common factor to all of a, b, and n, then we can divide each term in this equation by k and all resulting terms will be integers. We have

$$\frac{a-b}{k} = \frac{qn}{k}.$$

We can rewrite this as

$$\frac{a}{k} - \frac{b}{k} = q \cdot \frac{n}{k}.$$

Since k divides each of a, b, n, these are all integers. Thus, modulo $\frac{n}{k}$, we have

$$\frac{a}{k} - \frac{b}{k} \equiv 0 \left(\text{mod } \frac{n}{k}\right) \quad \Rightarrow \quad \frac{a}{k} \equiv \frac{b}{k} \left(\text{mod } \frac{n}{k}\right). \qquad \square$$

13) Prove that the Euclidean algorithm always results in the greatest common divisor!

Hint: We won't spoil this one! However, here's a few things to think about in considering $\gcd(n, k)$.

- The division algorithm gives $n = q \cdot k + r$. If $d = \gcd(n, k)$, what can you say about d and r?
- Why must this algorithm terminate after a finite number of steps?
- How do you know the last remainder must be the gcd?