# Worksheet 1: Euclidean Algorithm

7. Let $a, b \in \mathbb{Z}$, not both zero. Prove that there exist $x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a, b) .$$

More generally, prove that

$$ax + by = c$$

has a solution $(x, y) \in \mathbb{Z}^2$ if and only if $\gcd(a, b) \mid c$.

**If gcd(a,b)$|c$ then there exist x,y$\in \mathbb{Z}$ such that ax+by=c**

*Proof.* Let S=$\{am + bn > 0, m, n \in \mathbb{Z}\}$ S is nonempty and $s \subset$ so by the well ordering principle there exists a smallest element denoted$S_{\text{min}}$.
**Lemma:** $S_{\text{min}}$**=gcd(a,b)**

*Proof.* To prove that $S_{\text{min}}$=gcd(a,b) then we must first show that $S_{\text{min}}$ is a common divisor of a and b and that if there exist other common divisors that $S_{\text{min}}$ is greater.

Suppose for the sake of contradiction that $S_{\text{min}} \nmid a$ then by the divison algorithm a can be expressed as the following:

$$a = S_{\text{min}}q + r \quad 0 \leq r < S_{\text{min}}$$

$$\begin{aligned}
&S_{\text{min}} \in S \therefore S_{\text{min}} = am^* + bn^* \\
&a = (am^* + bn^*)q + r \\
&r = a - (am^* + bn^*)q \\
&r = a - am^*q + bn^*q \\
&r = a(1 - qm^*) + b(-qn^*)
\end{aligned}$$

Which implies that $r \in S$ since $r > 0$ by construction, however by the division algorithm $r < S_{\text{min}}$ which contradicts the statement $S_{\text{min}}$ is the smallest element meaning that $S_{\text{min}}$ must divide a, and by a symmetric proof $S_{\text{min}}$ must divide b.

Let $e|a$ and $e|b$ then by the definition of divisibility:

$$\begin{aligned}
&a = ek, k \in \mathbb{Z} \\
&b = el, l \in \mathbb{Z} \\
&S_{\text{min}} = am^* + bn^* \\
&S_{\text{min}} = ekm^* + eln^* \\
&S_{\text{min}} = e(km^* + ln^*) \\
&e|S_{\text{min}}
\end{aligned}$$

So it is shown that $S_{\text{min}} = gcd(a, b)$ $\square$

If $S_{\min} = gcd(a,b)$ then since $gcd(a,b)|c$, $S_{\min}|c$ which implies:

$$\begin{aligned}
c &= S_{\min}k, k \in \mathbb{Z} \\
c &= (am^* + bn^*)k \\
c &= am^*k + bn^*k \\
c &= a(m^*k) + b(n^*k)
\end{aligned}$$

So we have shown the existence of integer multiples x and y such that c=ax+by □

**If ax+by=c then gcd(a,b) | c**

Let d=gcd(a,b) then by the definition of gcd $d|a$ and $d|b$. This implies:

$$c = (dk)x + (dl)y = d(kx + ly), \quad k, l \in \mathbb{Z}$$

Hence, d | c.

8. Andrews 2.3.1.
   The linear diophantine equation has a solution if and only if $gcd(a,b)|c$ for those with solutions the general form of the solution set takes the following form:

   $$x = x_0 + t\frac{b}{gcd(a,b)} \quad y = y_0 - t\frac{a}{gcd(a,b)} \quad t \in \mathbb{Z}$$

   *Proof.* Here are the sample solutions found computationally during our meeting:) The x and y that solve the equation 2x +3y = 4 are -10 and 8 The x and y that solve the equation 17x +19y = 23 are -2 and 2 no solution The x and y that solve the equation 23x +29y = 25 are 9 and -7 The x and y that solve the equation 10x +-8y = 42 are -6 and -8 no solution

   □

9. Experiment with the `sage` command `divmod`. Use it with two arguments, say a 6-digit and a 3-digit number, and check that `sage` gives the correct answer.

   sage: divmod(146329, 846)
   $(172, 817)$

   *Proof.* $172 * 846 + 817 = 145512 + 817 = 146329$

   □

10. Experiment with the `sage` command `xgcd`. Use it with two 5-digit arguments and check that `sage` gives the correct answer.

    sage: xgcd(12345, 67891)
    (1, 15668, -2849)

    sage: xgcd(40921,33333) (271, 22, -27)

    *Proof.* □

# Worksheet 2: Primes

1. Let $a, b \in \mathbb{Z}_{>0}$. Show that, if $g = \gcd(a, b)$ then $\gcd(\frac{a}{g}, \frac{b}{g}) = 1$.

   *Proof.* Let $a, b \in \mathbb{Z}$ and $g = gcd(a, b)$, then

   $a = g \cdot i, i \in \mathbb{Z}$ and $b = g \cdot j, j \in \mathbb{Z}$

   $\frac{a}{g} = i$ and $\frac{b}{g} = j$

   Now we will prove by contradiction that i and j have a gcd of 1.

   Suppose $\gcd(i, j) = g_{ij} > 1$ then $i = g_{ij} \cdot c_i$ and $j = g_{ij} \cdot c_j$ where $c_i, c_j \in \mathbb{Z}$

   Then $a = (g \cdot g_{ij}) \cdot c_i$ and $b = (g \cdot g_{ij}) \cdot c_j$

   But then $(g \cdot g_{ij})|a$ and $(g \cdot g_{ij})|b$ and $(g \cdot g_{ij}) > g$ which is a contradiction since $g = gcd(a, b)$

   So $\gcd(i, j)$ has to be one.

   So $\gcd(\frac{a}{g}, \frac{b}{g}) = 1$ □

2. Give a careful definition of a *prime number*.
   **A prime number is a natural number greater than one such that its only divisors are 1 and itself**

3. Let $a, b, c \in \mathbb{Z}_{>0}$.

   (a) Prove that, if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

   *Proof.* □

   (b) Conclude that if $p$ is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

   *Proof.* □

   (c) Give a counterexample that shows the previous sentence is wrong if $p$ is not prime.

   *Proof.* □