Problem 1
Prove that $\log_{30}(45)$ is irrational.
Solution
Towards a contradiction, suppose $\log_{30}(45)$ were rational. Let $\log_{30}(45) = \frac{p}{q}$ with $p, q \in \mathbb{N}$ (we may assume p, q are positive since we know $\log_{30}(45)$ must be positive). Then, by definition of log,

$$30^{\frac{p}{q}} = 45.$$

Raising both sides to the qth power, we obtain

$$30^p = 45^q.$$

However, 30^p is even for all $p \in \mathbb{N}$, while 45^q is odd for all $q \in \mathbb{N}$. This raises a contradiction.

Problem 2

1. Compute $\gcd(932, 656)$ using the Euclidean algorithm.
2. Compute $\gcd(144, 89)$ using the Euclidean algorithm. What do you notice?

Solution

1.

$$\begin{aligned}
&\gcd(932, 656) \\
=&\gcd(656, 276) && (932 = 1 \cdot 656 + 276) \\
=&\gcd(276, 104) && (656 = 2 \cdot 276 + 104) \\
=&\gcd(104, 68) && (276 = 2 \cdot 104 + 68) \\
=&\gcd(68, 36) && (104 = 1 \cdot 68 + 36) \\
=&\gcd(36, 32) && (68 = 1 \cdot 36 + 32) \\
=&\gcd(32, 4) && (36 = 1 \cdot 32 + 4) \\
=&\gcd(4, 0) && (32 = 8 \cdot 4 + 0) \\
=&4.
\end{aligned}$$

2.

$$\begin{aligned}
&\gcd(144, 89) \\
=&\gcd(89, 55) && (144 = 1 \cdot 89 + 55) \\
=&\gcd(55, 34) && (89 = 1 \cdot 55 + 34) \\
=&\gcd(34, 21) && (55 = 1 \cdot 34 + 21) \\
=&\gcd(21, 13) && (34 = 1 \cdot 21 + 13) \\
=&\gcd(13, 8) && (21 = 1 \cdot 13 + 8) \\
=&\gcd(8, 5) && (13 = 1 \cdot 8 + 5) \\
=&\gcd(5, 3) && (8 = 1 \cdot 5 + 3) \\
=&\gcd(3, 2) && (5 = 1 \cdot 3 + 2) \\
=&\gcd(2, 1) && (3 = 1 \cdot 2 + 1) \\
=&\gcd(1, 0) && (2 = 2 \cdot 1 + 0) \\
=&1.
\end{aligned}$$

Computing $\gcd(144, 89)$ took a lot of iterations (more iterations than $\gcd(932, 656)$): the numbers are descending very slowly. Notice that the sequence of arguments to gcd form the Fibonacci sequence. Indeed, the Fibonacci sequence is the "worst case" input to the Euclidean algorithm.

Problem 3

Recall *Bézout's Identity*: Let $a, b \in \mathbb{Z}$, not both zero. Then there are $m, n \in \mathbb{Z}$ such that

$$am + bn = \gcd(a, b).$$

1. Compute $\gcd(217, 93)$ using the Euclidean algorithm.
2. Find integers $m, n \in \mathbb{Z}$ such that $217m + 93n = \gcd(217, 93)$, using *back substitution* from the previous subquestion.

Solution

1.

$$\begin{aligned} &\gcd(217, 93) \\ =&\gcd(93, 31) && (217 = 2 \cdot 93 + 31) \\ =&\gcd(31, 0) && (93 = 3 \cdot 31 + 0) \\ =&31. \end{aligned}$$

2. From

$$217 = 2 \cdot 93 + 31$$

we get

$$31 = 217 - 2 \cdot 93.$$

Thus $m = 1$ and $n = -2$ works.

Problem 4

Let $a, b \in \mathbb{Z}$, not both zero, and $c \in \mathbb{Z}$. Show that $\gcd(a, b) \mid c$ if and only if there are $m, n \in \mathbb{Z}$ such that

$$am + bn = c.$$

Solution

- ($\Rightarrow$) Suppose $\gcd(a, b) \mid c$. Then we can let $c = k \cdot \gcd(a, b)$ for some $k \in \mathbb{Z}$. By Bézout's Identity there are $x, y \in \mathbb{Z}$ such that

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

Multiplying both sides by k,

$$akx + bky = c.$$

Thus $m = kx$ and $n = ky$ gives $am + bn = c$.

- ($\Leftarrow$) Suppose there are $m, n \in \mathbb{Z}$ with

$$am + bn = c.$$

Notice that by definition of gcd, we have $\gcd(a, b) \mid a$, and $\gcd(a, b) \mid b$. Thus $\gcd(a, b) \mid am + bn$, which shows $\gcd(a, b) \mid c$.