Proof of a conjecture stated in A000010

Sela Fried

For $n \in \mathbb{N}$ let $\varphi(n)$ be Euler's totient function and set $[n] = \{1, \ldots, n\}$. The statement in the following theorem was conjectured by Irwin in A000010.

Theorem 1. *Let $n \geq 2$ be an integer and let $\mathcal{S}(n) = \{(a, b, c) \in [n]^3 : nc - ab = 1\}$. Then $\#\mathcal{S}(n) = \varphi(n)$.*

Proof. Let
$$\mathcal{U}(n) = \{a \in [n] \ : \ \gcd(a, n) = 1\}.$$
We claim that the map $(a, b, c) \mapsto a$ is a bijection from $\mathcal{S}(n)$ to $\mathcal{U}(n)$. Since $\#\mathcal{U}(n) = \varphi(n)$, this would prove the assertion. To see this, let $(a, b, c) \in \mathcal{S}(n)$ and let $d = \gcd(a, n)$. Thus, $d \mid a$ and $d \mid n$ and therefore d divides $nc - ab = 1$. Hence, $\gcd(a, n) = d = 1$ and therefore $a \in \mathcal{U}(n)$. This proves that the map is well-defined.

We now show that the map is injective. To this end, let $a \in \mathcal{U}(n)$ and assume there are $b, b', c, c' \in [n]$ such that $(a, b, c), (a, b', c') \in \mathcal{S}(n)$. Then $nc - ab = 1 = nc' - ab'$. Thus, $n(c - c') = a(b - b')$. In particular, $n \mid a(b - b')$. Since $\gcd(a, n) = 1$, necessarily $n \mid (b - b')$. But $b, b' \in [n]$. Thus, $b - b' = 0$, i.e., $b = b'$. From this it follows that $n(c - c') = 0$ and therefore $c = c'$, concluding the proof of the injectivity.

It remains to show that the map is surjective. To this end, let $a \in \mathcal{U}(n)$. Since $\gcd(a, n) = 1$, by Bézout's identity there are integers u, v such that $ua + vn = 1$. Multiplying by -1 and reducing modulo n, we obtain $(-u)a \equiv -1 \pmod{n}$. Let $b \in [n]$ such that $b \equiv -u \pmod{n}$. Then $ab \equiv -1 \pmod{n}$, i.e., there exists an integer c such that $ab = nc - 1$, i.e., $nc - ab = 1$. It remains to show that $c = (ab + 1)/n \in [n]$. Since $a, b \in [n]$, we have $2/n \leq c \leq (n^2 + 1)/n$. Since $n \geq 2$ and c is an integer, necessarily $c \in [n]$. □

References

[1] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences, OEIS Foundation Inc., `https://oeis.org`.