NSUCRYPTO 2020: POLY

Ioan Dragomir[1], Gabriel Tulba-Lecu[2], and Mircea-Costin Preoteasa[3]

[1] ioandr@gomir.pw – Technical University of Cluj-Napoca
[2] gabi_tulba_lecu@yahoo.com – Polytechnic Univeristy of Bucharest
[3] mircea_costin84@yahoo.com – Polytechnic Univeristy of Bucharest

Table of Contents

1 Problem summary

Let f be a polynomial of degree n in $\mathbb{Z}$: $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$
Bob claims $f(20) = 7$ and $f(15) = 5$.
Prove that this is impossible.

2 Solution

$$\begin{aligned}
f(20) &= a_0 + a_1 \cdot 20 + a_2 \cdot 20^2 + \cdots + a_n \cdot 20^n = 7 \\
f(15) &= a_0 + a_1 \cdot 15 + a_2 \cdot 15^2 + \cdots + a_n \cdot 15^n = 5 \\
f(20) - f(15) &= 0 + a_1 \cdot (20 - 15) + a_2 \cdot (20^2 - 15^2) + \cdots + a_n \cdot (20^n - 15^n) = 7 - 5 \\
&= 5(a_1 + 35a_2 + \cdots + (4 \cdot 20^{n-1} - 3 \cdot 15^{n-1}) \cdot a_n) = 2
\end{aligned}$$

In $\mathbb{Z}$, there is no solution to $5x = 2$, therefore such a polynomial cannot exist.