Coprime solutions to $ax \equiv b \pmod{n}$

Štefan Porubský

It is well known that a congruence $ax \equiv b \pmod{n}$ has a solution iff $\gcd(a,n)|b$, and, if the condition is satisfied, the number of incongruent solutions equals $\gcd(a,n)$. In [1] the authors noticed the following result which seems not to appear previously explicitly in the literature: Given a non-zero $a \in \mathbb{Z}_n$, the ring of residues modulo n, such that $\gcd(a,n) = \gcd(b,n)$, there exists an invertible element $x \in \mathbb{Z}_n^*$ satisfying the congruence $ax \equiv b \pmod{n}$. They gave a very long elementary proof of this result which played a key role in a problem related to an electronic signature. In the talk we give a concise proof of this result, together with a closed formula for the number of incongruent solutions coprime to n as well. We also give a bound on the probability that this congruence, for randomly chosen $a, b \in \mathbb{Z}$, possesses at least one solution coprime to n. This talk is based on a joint paper [2] with O.Grošek (Bratislava).

References

[1] B. Alomair, A. Clark, and R. Poovendran. The power of primes: security of authentication based on a universal hash-function family. *J. Math. Cryptol.*, 4(2):121-148, 2010.

[2] O. Grošek and Š. Porubský. Coprime solutions to $ax \equiv b \pmod{n}$. *J. Math. Cryptol.*, to appear in 2013