IDEMPOTENTS AND CONGRUENCE $ax \equiv b \pmod{n}$

Štefan Porubský
Institute of Computer Science, Academy of Sciences of the Czech Republic (Prague, Czech Republic)

We show how idempotents of the factor ring $R/(n)$ of a principal ideal domain R can be used to classify solutions of a congruence $ax \equiv b \pmod{n}$. As a special case we obtain a recently proved condition (cf. [1] and [2]) for the existence of its solutions coprime to n.

References

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

[2] Otokar Grošek and Štefan Porubský. Coprime solutions to $ax \equiv b \pmod{n}$. *J. Math. Cryptol.*, 7:217–224, 2013.