MA080G Cryptography Assignment Block 2

Viktor Rosvall

April 22, 2019

Fermat's Little Theorem

Fermat's Little Theorem is useful in primality testing and in public-key cryptography. It can also be used for find the inverse of an integer a modulo a prime. [1]

Theorem: let a be an integer and p be a prime, then:

$$a^p \equiv a \pmod{p}$$

This can also be rewritten as:

$$a^{p-1} \equiv 1 \pmod{p}$$

If p is a prime then the inverse of a can be calculated as:

$$a^{-1} \equiv a^{p-2} \pmod{p}$$

Proof using modular arithmetic [2]

asd .

The cancellation law

We can cancel out a because p does not divide a, nor k.

The rearrangement property

abada

References

[1] C. Paar, J. Pelzl, *Understanding Cryptography*. 2010 ed. Springer., Chapter 6.3.4

[2] Wikipedia, ”Proofs of Fermat’s little theorem”, `https://en.wikipedia.org/wiki/Proofs_of_Fermat%27s_little_theorem` 18-04-2019