Cryptography

JOACHIM VON ZUR GATHEN, JÉRÉMIE DETREY

3. Tutorial: Euler and RSA

Exercise 3.1 (Euler's totient function).

We defined Euler's totient function φ by $\varphi(n) = \#\mathbb{Z}_n^\times$, that is the number of units (invertible elements) in $\mathbb{Z}_n$.

(i) Compute $\varphi(5)$ and $\varphi(25)$.

(ii) Compute $\varphi(p)$ for a prime p.

(iii) Compute $\varphi(p^e)$ for a prime p and a positive integer e.

(iv) Given two coprime number a and b, compute $\varphi(a \cdot b)$ in function of $\varphi(a)$ and $\varphi(b)$.

(v) Given a number n and its factorisation $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$, compute $\varphi(n)$.

(vi) Recall the value of N and $\varphi(N)$ in RSA.

Exercise 3.2 (Euler's theorem).

Let n be a positive integer and x an integer coprime to n. Let's consider the map f_x defined from $\mathbb{Z}_n^\times$ to $\mathbb{Z}_n^\times$, which maps to any element y the value $f_x(y) = x \cdot y$.

(i) Show that f_x is injective.

(ii) Show that f_x is surjective.

(iii) Show that

$$\prod_{y \in \mathbb{Z}_n^\times} y = \prod_{y \in \mathbb{Z}_n^\times} x \cdot y.$$

(iv) Factor as many x's as you can out of the right-hand product.

(v) Multiply both sides by $\left(\prod_{y \in \mathbb{Z}_n^\times} y\right)^{-1}$. Conclude.

Exercise 3.3 (Power of 3).

Compute $3^{1\,000\,003} \bmod 101$ by hand.
Hint: try to use the previous result to avoid unnecessary computations.