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 $\varphi(25)$.

Solution. $\varphi(5) = 4$ and $\varphi(25) = 25$. ◯

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

Solution. $\varphi(p) = p - 1$, since all elements of $\mathbb{Z}_p^*$ are invertible. ◯

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

Solution. An element x of $\mathbb{Z}_{p^e}$ is coprime to p^e if and only if $x \not\equiv 0 \pmod{p}$. Hence, only multiples of p are not units modulo p^e. As there are p^{e-1} multiples of p in $\mathbb{Z}_{p^e}$, we have $\varphi(p^e) = (p-1)p^{e-1}$. ◯

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

Solution. Remember that thanks to the Chinese remainder theorem, we have an isomorphism between $\mathbb{Z}_{a\cdot b}$ and $\mathbb{Z}_a \times \mathbb{Z}_b$. Moreover, since for all x in $\mathbb{Z}_{a\cdot b}$, $\gcd(x, a \cdot b) = 1$ if and only if $\gcd(x, a) = 1$ and $\gcd(x, b) = 1$, we also have a one-to-one mapping between $\mathbb{Z}_{a\cdot b}^\times$ and $\mathbb{Z}_a^\times \times \mathbb{Z}_b^\times$. Hence $\varphi(a \cdot b) = \#(\mathbb{Z}_a^\times \times \mathbb{Z}_b^\times) = \varphi(a) \cdot \varphi(b)$. ◯

(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 $\varphi(n)$.

Solution. $\varphi(n) = (p_1 - 1)p_1^{e_1-1} \cdot (p_2 - 1)p_2^{e_2-1} \cdot \ldots \cdot (p_k - 1)p_k^{e_k-1}$. ◯

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

Solution. N is chosen to be the product of two primes p and q. Hence $\varphi(N) = (p-1)(q-1)$. ◯

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.

Solution. Suppose we have y and y' in $\mathbb{Z}_n^\times$ such that $f_x(y) = f_x(y')$. We have $x \cdot y = x \cdot y'$, which gives $y = y'$ when multiplying both sides by x^{-1}. ◯

(ii) Show that f_x is surjective.

Solution. $\mathbb{Z}_n^\times$ is finite and f_x is injective. Hence f_x is surjective. ◯

(iii) Show that

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

Solution. Since f_x is surjective, when y ranges over all the set $\mathbb{Z}_n^\times$, so does $f_x(y)$. Hence the equality. ◯

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

Solution.

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

◯

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

Solution. We obtain $x^{\varphi(n)} = 1$. Therefore, for all integer x coprime to n, $x^{\varphi(n)} \equiv 1 \pmod{n}$. ◯

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.

Solution. Since 101 is prime, $\varphi(101) = 100$. And 3 being coprime to 101, we have $3^{100} \bmod 101 = 1$. Hence $3^{1\,000\,003} \bmod 101 = 3^3 \cdot 3^{1\,000\,000} \bmod 101 = 3^3 = 27$. ◯