TD2 : The group $(\mathbb{Z}/N\mathbb{Z})^*$

Key points

— Elementary algorithms for $(\mathbb{Z}/N\mathbb{Z})$, and their complexities,
— Fast exponentiation,
— The order of the group of invertible elements in $(\mathbb{Z}/N\mathbb{Z})$,
— Fermat's criterion,
— Subgroup generated by an elements of a group,
— Order of an element in a group,
— Cyclic groups,
— If $N \geqslant 2$ is prime then $(\mathbb{Z}/N\mathbb{Z})^*$ is a cyclic group,
— Lagrange's theorem,

⋆⋆⋆

Prove that an integer $N \geqslant 2$ is prime if and only if $\#(\mathbb{Z}/N\mathbb{Z})^* = N-1$,
Compute $2^{12345678987654321} \bmod 101$.

⋆⋆⋆

An integer N is said to be a Carmichael number if and only if N is composite and for every prime to N integer x one has $x^{N-1} = 1 \bmod N$.

Check that 561 is a Carmichael number.

Can you explain this phenomenon ?

⋆⋆⋆

Give the list of invertible elements in $\mathbb{Z}/35\mathbb{Z}$. Is the group $(\mathbb{Z}/35\mathbb{Z})^*$ a cyclic group ?

⋆⋆⋆

Compute by hand the inverse of 7 modulo 12 using extended euclidean algorithm.

⋆⋆⋆

Give a generator g of $(\mathbb{Z}/11\mathbb{Z})^*$. Write the table of the exponential function with basis g. Write the table of the logarithm function with basis g.

⋆⋆⋆

Let G be an abelian group. Let $g \in G$ be an element with order M. Let $h \in G$ be an element with order N. Assume that $\gcd(M,N) = 1$.

What can you say about the order of gh ?

What if G is not abelian ?

⋆⋆⋆

Find a prime integer p in $[10^{100}, 2.10^{100}]$ such that $(p-1)/2$ is a prime. Give a generator of $(\mathbb{Z}/p\mathbb{Z})^*$.

⋆⋆⋆

Implement the primality test of Miller and Rabin.