MPRI – cours 2.12.2

F. Morain

Lab, 2018/90/25

1. Describe all composite numbers N for which all elements $a \in (\mathbb{Z}/N\mathbb{Z})^* - \{1\}$ have even order.

2. Let G be a finite Abelian group, and $x \in G$. Prove that the order of x is ω if and only if
   i) $a^\omega = 1_G$;
   ii) for all prime $p \mid \omega$, $a^{\omega/p} \neq 1_G$.

3. Assume the following result: $(\mathbb{Z}/N\mathbb{Z})^*$ is cyclic iff $N = 2, 4, p^\alpha, 2p^\alpha$ for odd p.

a) Prove that N is prime if and only if $(\mathbb{Z}/N\mathbb{Z})^*$ is cyclic of ordre $N-1$, or in other words iff there exists a s.t.

$$\left.\begin{array}{l} a^{N-1} \equiv 1 \bmod N \\ \forall\, p \mid N-1,\ a^{\frac{N-1}{p}} \not\equiv 1 \bmod N \end{array}\right\}$$

b) What is the complexity of the algorithm that you can deduce from a)? What is the complexity of checking the data?

4. For N an integer, put $P(N) = \#\{a \in (\mathbb{Z}/N\mathbb{Z})^*, a^{N-1} \equiv 1 \bmod N\}$.

a) Compute $P(N)$ for $N = \prod_i p_i^{\alpha_i}$.

b) Prove that there are numbers for which $P(N) = \varphi(N)$.

Consider the following function:
function isComposite(N)

1. Choose a at random in $\mathbb{Z}/N\mathbb{Z} - \{0\}$.
2. Compute $g = \gcd(a, N)$; **if** $g > 1$, **then** return $(\texttt{yes}, g \mid N)$.
3. **if** $a^{N-1} \not\equiv 1 \bmod N$, **then** return $(\texttt{yes}, a)$
   otherwise return I don't know.

i) What happens when N is prime?

ii) What is the probability that the test answers *I don't know*?

5. a) Let N be a composite number and suppose $p \mid N$ and $p - 1 \mid B!$. How can we factor N?

b) Suppose $p \mid N$, but $p - 1 = Qs$ with $Q \mid B!$ and s prime in $]B, B']$. Show how one can factor N.

c) Compute the complexity of the preceding algorithm for finding s. Can you do better?

6. DLP: Given $h \in G = \langle g \rangle$ of order N, find an integer n, $0 \leq n < N$ such that $h = g^n$.

a) Show that finding n is equivalent to finding $n \bmod p^\alpha$ for each $p^\alpha \,||\, N$.

b) Give a simple algorithm to solve the problem.

c) Give a faster algorithm. What is its complexity?