MPRI: 2.12.2

F. MORAIN

Exercise sheet #3; October 14, 2019

Exercises

Exercise 1. Let p be an odd prime, e an integer, $e \geq 2$, and g a generator of $(\mathbb{Z}/p^e\mathbb{Z})^*$. Suppose that we dispose of an algorithm that computes discrete logarithms in $(\mathbb{Z}/p\mathbb{Z})^*$. Give an algorithm which computes $x = \log_g(a)$ for $a \in (\mathbb{Z}/p^e\mathbb{Z})^*$.

Numerical Application: : $p = 10^6 + 81, e = 2, g = 7, a = 2$.

Exercise 2. Let p be a prime number and g a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. Suppose we know that discrete logarithm z of a to base g belongs to the interval $[A, B]$. Show how to modify the baby steps giant steps algorithm to benefit from this knowledge. What is the complexity of your algorithm?