MPRI – cours 2.12.2

F. Morain

Exercise list 2011/10/11

1. Use the Pohlig-Hellman reduction to compute $\log_5(13)$ in $\mathbb{F}_{73}^*$.

2. Compute $\log_7(2) \bmod p$ where $p = 10^6 + 81$. Try the different algorithms given during the lecture.

3. Let p be an odd prime number, $e \geq 2$ an integer and g a generator of $(\mathbb{Z}/p^e\mathbb{Z})^*$. Show how to compute the discrete logarithm in $(\mathbb{Z}/p^e\mathbb{Z})^*$, given an algorithm that computes it in $(\mathbb{Z}/p\mathbb{Z})^*$. Try it on $p = 10^6 + 81$, $e = 2$, $g = 7$, $a = 2$.

4. Let p be a prime and g a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. Suppose that $z = \log_g a$ belongs to the interval $[A, B]$. Show how to modify the baby-steps giant-steps algorithm of Shanks to speed up the computation of z. Give the complexity of your algorithm.