MPRI: 2.12.2

F. MORAIN

Exercise sheet #2; October 7, 2019

Exercises

Exercise 1. Let w_1, w_2, ..., w_k be integers such that their product $w_1 w_2 \cdots w_k$ is known to be a perfect square Z^2 whose square root must be computed. If the w_i's (resp. k) are big, then computing the product, followed by the computation of Z is costly. Show that if the w_i's have common factors, this cost can be reduced using gcd computations. As for a numerical application, compute Z when the w_i's are given by:

i	1	2	3	4	5
w_i	776	1136	2048	3007	2201

What is the interest of this approach for CFRAC?

Exercise 2. Let $N = 91$. Consider the following congruences modulo N :

$$96 \equiv 5, 90 \equiv -1, 88 \equiv -3, 81 \equiv -10, 80 \equiv -11, 75 \equiv -16. \tag{1}$$

Let p be a prime factor of N and g a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. Put

$$-1 = g^{x_1}, 2 = g^{x_2}, 3 = g^{x_3}, 5 = g^{x_4}, 11 = g^{x_5}.$$

Translate congruences (1) into a linear system of congruences whose unknown are the x_i's. Show that $6x_3 \equiv 2x_1 \bmod p - 1$ and that $3^6 \equiv 1 \bmod p$. Deduce from this non-trivial factors of N.

Exercise 3. Suppose that in the course of QS, we find

$$P(x) = \left(\prod_{p \in \mathcal{B}} p \right) \times q$$

with q prime. Using the identity

$$P(x + yq) = P(x) + 2yq(x + g) + y^2 q^2,$$

explain how to find another relation whose factorization also contains q.