MPRI – cours 2.12.2

F. Morain

Tutorial, 2011/10/04

1. Find a multiple of 49 all decimal digits of which are equal to 1.

2. What are the generators of $(\mathbb{Z}/13\mathbb{Z})^*$?

3. Compute 1/5 mod 17.

4. Prove Fermat's and Euler's theorems without using Lagrange's.

5. Let $(e_i)_{1\leqslant i\leqslant n}$ be a sequence of integers and x an element of some group G. Put $E = \prod_{i=1}^n e_i$ and $E_i = E/e_i$. Show that one can compute all $y_i = x^{E_i}$ using $O(n \log n)$ group operations.

6. Let $E(x) = x^e \bmod N$ be the encryption function for RSA with the usual notations. Compute the number of fixed points of E, i.e., the number of x that satisfy $E(x) = x$.

7. Let $f(X) = \prod_{i=1}^n (X - \alpha_i)$ be a polynomial (over some field) of degree n and roots α_i (in a suitable extension). Then the discriminant of f is

$$\mathrm{Disc}(f) = \prod_{i=1, j\neq i}^{n} (\alpha_i - \alpha_j) = \left(\prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j) \right)^2.$$

If $g(X) = \prod_{i=1}^n (X - \beta_i)$ is another polynomial of degree m and roots β_i, the resultant of f and g is

$$\mathrm{Res}(f, g) = \prod_{i,j} (\alpha_i - \beta_j) = \prod_i g(\alpha_i).$$

We remark that $\mathrm{Disc}(f) = (-1)^{n(n-1)/2}\mathrm{Res}(f', f)$.

Let p be an odd prime and $f(X)$ a polynomial with coefficients in $\mathbb{Z}/p\mathbb{Z}$ of degree $n < p$. The aim of the exercise is to prove that if $p \nmid \Delta = \mathrm{Disc}(f)$ and ω the number of irreducible factors of $f(X)$ in $\mathbb{Z}/p\mathbb{Z}$, then

$$\left(\frac{\Delta}{p}\right) = (-1)^{n-\omega}, \qquad (1)$$

where $(./p)$ stands for the Legendre symbol.

a) Prove the result when f is irreducible.

b) Prove the general case.

8. Prove Pocklington's theorem.

9. Prove that N is prime if and only if $\varphi(N) \mid N - 1$.

10. Find a (probable) family of composite integers N satisfying $F(N) = \varphi(N)/4$.