MPRI – cours 2.12.2

F. Morain

Tutorial, 2014/09/22

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 $1/5 \bmod 17$.

4. Let $d(n)$ denote the number of divisors of n; hence $d(6) = \#\{1, 2, 3, 6\} = 4$. Characterize the integers n for which $d(n)$ is odd.

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. Characterize the integers N s.t. $\varphi(N) \mid N - 1$.

8. Suppose $N = pq$, p and q distinct primes.
   a) Show that the equation $x^2 \equiv 1 \bmod N$ has four roots modulo N.
   b) Show that two of the solutions yield a factorization of N.

9. Suppose $N = pq$, p and q distinct primes. Let a be prime to N and suppose an oracle gives us the order r of a modulo N. Can we factor N?