MPRI – cours 2.12.2

F. Morain

Tutorial, 2012/10/08

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

5. 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.

6. 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.

7. 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 $E(x) = x$.

8. Prove Pocklington's theorem.

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

10. Find all integers $0 \leq k \leq 100$ for which $2 \cdot k! + 1$ is prime and give a certificate of primality for the corresponding numbers.

11. Program the sieve of Eratosthenes. Enumerate all primes $\leq 2^{32}$ and imagine a way to store them using one character (8 bits) per number in a file.