MPRI: 2.12.2

F. MORAIN

Exercise sheet #1; September 30, 2019

Exercises

Exercise 1. Consider Fibonacci's sequence defined by the formulas: $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geqslant 2$. Give an algorithm for computing F_n in $O(\log n)$ operations. Program this algorithm. What is the value of F_{100}?

Exercise 2. Let a and b be two integers such that $0 \leqslant a, b < M_n = 2^n - 1$. Explain how to speed up the computation of ab modulo M_n. Same question with $0 \leqslant a, b < P_n = 2^n + 1$ and the computation of $ab \bmod P_n$.

Exercise 3. Let $N > 0$ be an integer and R an integer $> N$ and prime to N. Define ϕ which associates to $x \in \mathbb{Z}/N\mathbb{Z}$ the quantity

$$\phi(x) = (xR \bmod N).$$

(a) Let u and v be two integers satisfying $uR - vN = 1$. Let T be an integer such that $0 < T < RN$. Now consider the function given in Figure 1.

Algorithm 1: The REDC function.

Function *REDC*(N, R, T)
- **Input** : N, R, T three integers
- **Output:** $(TR^{-1}) \bmod N$
- $m \leftarrow ((T \bmod R) * v) \bmod R$;
- $t \leftarrow (T + m * N) \div R$;
- **if** $t \geqslant N$ **then**
  - **return** $t - N$;
- **else**
  - **return** t;

Show that `REDC(N, R, T)` returns the integer $x = (TR^{-1}) \bmod N$, $0 \leqslant x < N$.

(b) Let f be an arithmetical operation (addition, division, etc.). Define $\phi[f]$ as

$$\phi[f](\phi(x), \phi(y)) = \phi(f(x, y)).$$

Compute $\phi[+]$, $\phi[-]$.

(c) Prove that

$$\phi[\times](\phi(x), \phi(y)) = REDC(N, R, \phi(x) \ \times \ \phi(y)).$$

(d) Write a modular exponentiation algorithm using ϕ and implement it.

(e) Suppose that N is odd and written in base $B = 2^{32}$ (or $B = 2^{64}$). Explain how to choose R with care so that computations with `REDC` be the fastest possible. What is the interest of this method?

Exercise 4. Let $n \geqslant 1$, a and e two integers $< 2^n$. Consider the algorithm of Figure 2.

Algorithm 2: Algorithm P.

Function $P(a, e)$

  Input : a, e two integers $< 2^n$

  Output: ?

  $g \leftarrow \gcd(a, e)$;

  if $g = 1$ **then**

    return $(1, a)$;

  $G \leftarrow g^{2^k} \bmod a$ avec $k = \lceil \log n / \log 2 \rceil$;

  $u \leftarrow \mathrm{pgcd}(G, a); v \leftarrow a/u$;

  return (u, v).

(a) Execute the algorithm on $(a, e) = (16, 210)$, $(a, e) = (5040, 231)$.

(b) What does this algorithm compute?

(c) Justify your claim.

Exercise 5. (The $p + 1$ method) For n a positive integer, the n-th Cheyshev polynomial (in $\mathbb{Z}[X]$) is defined as the unique monic polynomial of degree n such that $V_n(x + 1/x) = x^n + 1/x^n$.

(a) Compute $V_n(X)$ for $n \in \{0, 1, 2\}$.

(b) Prove that for all m, n, one has $V_{nm}(X) = V_m(V_n(X))$.

(c) Show that for all $m \geqslant n$:

$$V_m(X)V_n(X) = V_{m+n}(X) + V_{m-n}(X).$$

(d) Compute $V_{2n}(X)$ as a function of $V_n(X)$.

(e) Give an algorithm in $O(\log M)$ for computing $V_M(a) \bmod N$, where a is given and $M \geqslant 0$.

(f) Suppose that p is a prime and a chosen such that $\left(\frac{a^2-4}{p}\right) = -1$. Show that $V_{p+1}(a) = 2 \bmod p$.

(g) Design an algorithm for factoring the integer N, assuming the one of the prime divisors p of N is such that $p + 1$ is smooth.