Algorithmique de base

Master 1, Université de Rennes

22/11/2024 – TD 9

Exercise 1. Let $\mathbb{F}_5 = \mathbb{Z}_5$ be the finite field with 5 elements.

(i) Compute a polynomial $f \in \mathbb{F}_5[x]$ of degree at most 2 satisfying:

$$f(0) = 1, \quad f(1) = 2, \quad f(2) = 4. \tag{$*$}$$

(ii) List all polynomials $f \in \mathbb{F}_5[x]$ of degree at most 3 satisfying $(*)$. How many of degree at most 4 are there? Generalize your answer to solutions of degree at most n for $n \in \mathbb{N}$.

Exercise 2. Let R be an integral domain, and let $u_0, u_1, \ldots, u_{n-1} \in R$. Define the Vandermonde matrix V of order n as follows:

$$V = \begin{pmatrix} 1 & u_0 & u_0^2 & \cdots & u_0^{n-1} \\ 1 & u_1 & u_1^2 & \cdots & u_1^{n-1} \\ 1 & u_2 & u_2^2 & \cdots & u_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & u_{n-1} & u_{n-1}^2 & \cdots & u_{n-1}^{n-1} \end{pmatrix} \in R^{n \times n}.$$

Prove that the determinant of the Vandermonde matrix V is given by:

$$\det V = \prod_{0 \le j < i \le n-1} (u_i - u_j).$$

Hint: Replace u_{n-1} by an indeterminate and proceed by induction on n.

Exercise 3. (a) Find an integer a between 1 and 12 such that $a \equiv 27^{103} \pmod{13}$.

(b) Find an integer b between 1 and 10 such that $b \equiv 27^{103} \pmod{11}$.

(c) Using the Chinese Remainder Theorem, determine the value of $27^{103} \pmod{143}$.

Exercise 4. 1. Suppose $p \geq 5$ is a prime, $f \in \mathbb{F}_p[x]$ has degree 4, and

$$\gcd(x^p - x, f) = \gcd(x^{p^2} - x, f) = 1.$$

What can you say about the factorization of f in $\mathbb{F}_p[x]$?

2. Let $q \in \mathbb{N}$ be a prime power. Prove that if r is a prime number, then there are $\frac{q^r - q}{r}$ distinct monic irreducible polynomials of degree r in $\mathbb{F}_q[x]$. (Observe that, by Fermat's Little Theorem, $\frac{q^r-q}{r}$ is an integer.)

Exercise 5. Let e be an integer whose binary representation is:

$$e = \sum_{i=0}^{t-1} e_i 2^i \quad \text{with } e_{t-1} = 1.$$

The following algorithm is called "square and multiply" and takes as input $g \in \mathbb{Z}/n\mathbb{Z}$ and the binary representation of e. It returns g^e.

Algorithm 1 Square and Multiply

---

function SquareMultiply($g, e_0, ..., e_{t-1}$):
  $h = 1$
  $i = t - 1$
  while $i \geq 0$ **do**:
    $h = h^2$
    if $e_i = 1$ **then**:
      $h = hg$
    $i = i - 1$

This algorithms consists in t squarings and $t/2$ multiplications on average.

1. Show that after j steps, we have:

$$h = g^{E_j} \quad \text{with } E_j = \sum_{k=1}^{j} e_{t-k} 2^{j-k}.$$

2. Deduce that the "square and multiply" algorithm correctly computes g^e.
3. Use this method to compute 8^{13} in $\mathbb{Z}/17\mathbb{Z}$.
4. Knowing that $641 = 2^7 \cdot 5 + 1 = 2^4 + 5^4$, show that 641 divides the fifth Fermat number $F_5 = 2^{2^5} + 1$.
