Examen Partiel - Courbes Elliptiques

Vendredi 2 décembre 2016, 9h – 11

Exercice 1. Quel algorithme utilisiez-vous pour trouver un facteur d'un nombre n si vous saviez que

(1) n a un petit facteur premier.
(2) n a un facteur premier p tel que $p-1$ n'a que des petits facteurs premiers (p est *powersmooth*.

Dans les deux cas, décrire l'algorithme (en pseudo-code).

Solution.

(1) L'algorithme ρ de Pollard.
Entrée : Un entier n.
Sortie : Un facteur non-trivial de n, ou échec.

```
let x := 2, Y := 2, d := 1
while d = 1
   x := x^2 + 1%n
   y := y^2 + 1%n
   y := y^2 + 1%n
   d := pgcd(|x - y|, n)
if d = n return "échec" else return d
```

(2) L'algorithme $p-1$ de Pollard.
Entrée : Un nombre n et une borne B.
Sortie : Un facteur non-trivial de n, ou échec.

```
let a :=random(2,...,n), m = a, g = 1, i = 1
while (k < B and g = 1)
   k := k + 1
   m := m^k%n
   d = pgcd(m - 1, n)
if 1 < d < n return d
if d = 1 return "échec, augmenter B"
if d = n return "échec, réduire B"
```

Exercice 2. Décrire l'algorithme de Dixon.

Solution. Un algorithme sous-exponentiel pour trouver un facteur non-trivial d'un entier composé.
Entrée : Un entier n et une borne B.
Sortie : Un facteur non-trivial de n.
Soit $\mathcal{P}$ l'ensemble des nombres premiers bornés par B, et $n = |\mathcal{P}|$.
On cherche des entiers z_i pour $i \leq n$ tels que

$$z_i^2 = \prod_{p \in \mathcal{P}} p^{k(i,p)} \mod n.$$

Il y a alors une relation lineaire nontriviale (qu'on peut trouver avec le pivot de Gauss, par exemple) entre les $k(i,p)$ modulo 2. Ceci signifie qu'il y a $\emptyset \neq I \subseteq \{0, \ldots, n\}$ tel que

$$k(p) := \sum_{i \in I} k(i,p) \equiv 0 \mod 2 \qquad \text{pour tout } p \in \mathcal{P}.$$

Ceci signifie que $Z := \prod_{i \in I} z_i$ et $P = \prod_{p \in \mathcal{P}} p^{k(p)/2}$ satisfait

$$Z^2 \equiv P^2 \mod n.$$

Alors $\mathrm{pgcd}(Z+P, n)$ est soit un facteur non-trivial de n, soit n ; dans ce cas on continue avec d'autres z_i.

Exercice 3. On considère le polynôme $P(X) = X^4 + X^3 - 1$ sur $\mathbb{F}_3$, et une racine ϑ de P dans une extension $K \geq \mathbb{F}_3$.

(1) Montrer que le polynôme $P(X) = X^4 + X^3 - 1$ est irréductible dans $\mathbb{F}_3[X]$.
(2) Construire le corps $\mathbb{F}_{81}$ à l'aide de P.
(3) Montrer que $\mathbb{F}_{81} = \mathbb{F}_3(\vartheta)$, et donner la forme des éléments de $\mathbb{F}_3(\vartheta)$.
(4) Calculer ϑ^{16} et ϑ^{40}. En déduire que ϑ est un générateur de $\mathbb{F}_{81}^\times$.
(5) Quels sont les sous-corps de $\mathbb{F}_{81}$? Donner une générateur sur $\mathbb{F}_3$ pour chacun.
(6) Donner ϑ^{-1}.
(7) Calculer $(1+\vartheta)^{-1}$.
(8) Résoudre le problème de logarithme discrèt $\vartheta^n = 1 + \vartheta$.

Solution.

(1) On a $P(0) = -1$, $P(1) = 1$, $P(-1) = -1$, donc P n'a pas de facteur linéaire sur $\mathbb{F}_3$. On essaie des facteurs de degré deux, avec $a, b, c, d \in \mathbb{F}_3$:

$$P(X) = (X^2+aX+b)(X^2+cX+d) = X^4+(a+c)X^3+(b+d+ac)X^2+(ad+bc)X+bd.$$

Alors $a + c = 1$, $b + d + ac = 0$, $ad + bc = 0$ et $bd = -1$. Donc $c = 1 - a$ et $d = -b \neq 0$. Ceci donne

$$a + a^2 = 0, \qquad b(1 - a - a) = 0.$$

Donc $a = 0$ ou $a = 1$ d'après la première équation, mais $a = -1$ d'après la deuxième, une contradiction. Ainsi P est irréductible sur $\mathbb{F}_3$.

(2) Puisque P est irréductible sur $\mathbb{F}_3$ et de degré 4, on a $\mathbb{F}_{81} = \mathbb{F}_{3^4} = \mathbb{F}_3[X]/(P)$.

(3) Puisque p est irréductible sur $\mathbb{F}_3$ et $P(\vartheta) = 0$, le polynôme minimal de ϑ sur $\mathbb{F}_3$ est P. Donc $[\mathbb{F}_3(\vartheta) : \mathbb{F}_3] = 4$ et $\mathbb{F}_3(\vartheta) = \mathbb{F}_{3^4} = \mathbb{F}_{81}$. Alors

$$\mathbb{F}_3(\vartheta) = \{a + b\vartheta + c\vartheta^2 + d\vartheta^3 : a, b, c, d \in \mathbb{F}_3\}.$$

(4) On a

$$\begin{aligned}
\vartheta^4 &= -\vartheta^3 + 1\\
\vartheta^5 &= -\vartheta^4 + \vartheta = \vartheta^3 - 1 + \vartheta = \vartheta^3 + \vartheta - 1\\
\vartheta^6 &= \vartheta^4 + \vartheta^2 - \vartheta = -\vartheta^3 + \vartheta^2 - \vartheta + 1\\
\vartheta^8 &= (-\vartheta^3 + 1)^2 = \vartheta^6 - 2\vartheta^3 + 1 = -\vartheta^3 + \vartheta^2 - \vartheta + 1 + \vartheta^3 + 1 = \vartheta^2 - \vartheta - 1\\
\vartheta^{16} &= (\vartheta^2 - \vartheta - 1)^2 = \vartheta^4 + \vartheta^2 + 1 - 2\vartheta^3 - 2\vartheta^2 + 2\vartheta = -\vartheta^2 - \vartheta - 1 \neq 1\\
\vartheta^{32} &= (-\vartheta^2 - \vartheta - 1)^2 = \vartheta^4 + \vartheta^2 + 1 + 2\vartheta^3 + 2\vartheta^2 + 2\vartheta = \vartheta^3 - \vartheta - 1\\
\vartheta^{40} &= (\vartheta^3 - \vartheta - 1)(\vartheta^2 - \vartheta - 1) = \vartheta^5 - \vartheta^4 + \vartheta^3 - \vartheta + 1 = -1 \neq 1.
\end{aligned}$$

Pusique $o(\vartheta)$ divise $80 = |\mathbb{F}_{81}^\times|$, on en déduit que $o(\vartheta) = 80$ et ϑ est un générateur multiplicatif.

(5) Les sous-corps de $\mathbb{F}_{81} = \mathbb{F}_{3^4}$ sont les $\mathbb{F}_{3^n}$ où n divise 4, notamment
- $n = 1$: $\mathbb{F}_3$ de générateur -1.
- $n = 2$: $\mathbb{F}_{3^2} = \mathbb{F}_9$ avec générateur $\vartheta^{10} = \vartheta^4 - \vartheta^3 - \vartheta^2 = \vartheta^3 - \vartheta^2 + 1$ d'ordre $8 = |\mathbb{F}_9^\times|$.
- $n = 4$: $\mathbb{F}_{3^4} = \mathbb{F}_{81}$ de générateur ϑ.

(6) $1 = \vartheta^4 + \vartheta^3$ et donc $\vartheta^{-1} = \vartheta^3 + \vartheta^2$.
(7) $1 = (1+\vartheta)\vartheta^3$ et donc $(1+\vartheta)^{-1} = \vartheta^3$.
(8) $1 + \vartheta = \vartheta^{-3} = \vartheta^{80-3} = \vartheta^{77}$. Donc $n = 77$.