Corrigé de l'examen de M.A.O. Calcul Formel

Lundi 12 juin 2017
Master 1 M.F.A., Orsay

Exercice.

1. ($\star$) Considérons $A(X,Y,T) = X^2 - 2(2T-1)T$ et $B(X,Y,T) = Y^2 - 2(2T-1)(1-T)$ dans $\mathbb{Q}[X,Y,T]$, et notons $R(X,Y) = \mathrm{Res}_T(A,B)$ leur résultant calculé par rapport à T (c'est-à-dire qu'on considère A et B dans $\mathbb{Q}[X,Y][T]$). Le calcul suivant donne $R = 16(X^4 + Y^4 + 2X^2Y^2 - 2X^2 + 2Y^2)$.

```
sage: PXYT.<X, Y, T> = PolynomialRing(QQ)
sage: A = 2 * (2 * T - 1) * T - X^2
sage: B = 2 * (2 * T - 1) * (1 - T) - Y^2
sage: R = A.resultant(B, T)
sage: R
16*X^4 + 32*X^2*Y^2 + 16*Y^4 - 32*X^2 + 32*Y^2
```

   Pour tous $x, y \in \mathbb{C}$ on a alors $\mathrm{Res}(A(x,y,T), B(x,y,T)) = R(x,y)$ puisque $A(x,y,T)$ et $B(x,y,T)$ sont de degré 2 en T pour tous $x, y \in \mathbb{C}$. Comme $\mathbb{C}$ est algébriquement clos, on a bien $R(x,y) = 0$ si, et seulement si, les polynômes $A(x,y,T)$ et $B(x,y,T)$ ont une racine commune $t \in \mathbb{C}$, ce qui signifie que $(x,y) \in \mathcal{C}_1$.

2. Soit $(x,y) \in \mathbb{R}^2$. Si il existe $t \in \mathbb{R}$ vérifiant (1) alors $(x,y) \in \mathcal{C}_1$ donc la question précédente montre que $R(x,y) = 0$. Réciproquement, supposons que $R(x,y) = 0$. La question précédente montre que $(x,y) \in \mathcal{C}_1$: il existe $t \in \mathbb{C}$ vérifiant (1). Si $y = 0$ alors on a $t = 1/2$ ou $t = 1$, donc $t \in \mathbb{R}$. Si $y \neq 0$ alors $\frac{x^2}{y^2} = \frac{t}{1-t}$ donc $\frac{x^2}{y^2} + 1 = \frac{1}{1-t} \in \mathbb{R}$ d'où $t \in \mathbb{R}$.

3. ($\star$) Notons $P(Y) = \mathrm{Res}_X(R(X,Y), S(X,Y))$ le résultant de R et S vus dans $\mathbb{Q}[Y][X]$. Par spécialisation on a $\mathrm{Res}(R(X,y), S(X,y)) = P(y)$ puisque $\deg R(X,y) = 4$ et $\deg S(X,y) = 2$. Comme $\mathbb{C}$ est algébriquement clos, il existe $x \in \mathbb{C}$ tel que $R(x,y) = S(x,y) = 0$ si et seulement si $P(y) = 0$.

```
sage: S = X^2 - Y^2 - 2/9
sage: P = R.resultant(S, X)
sage: P
4096*Y^8 + 16384/9*Y^6 - 16384/27*Y^4 - 131072/729*Y^2 + 262144/6561
```

4. Soit (x,y) un couple de réels appartenant à $\mathcal{C}_1 \cap \mathcal{C}_2$. La question précédente montre que $P(y) = 0$. On peut factoriser cette équation dans $\mathbb{Q}[Y]$:

```
sage: PY.<Y> = PolynomialRing(QQ)
sage: P = PY(P)
sage: P
4096*Y^8 + 16384/9*Y^6 - 16384/27*Y^4 - 131072/729*Y^2 + 262144/6561
sage: P.factor()
(4096) * (Y^2 - 2/9)^2 * (Y^2 + 4/9)^2
```

Les racines réelles de P sont donc $y = \pm\frac{\sqrt{2}}{3}$. Comme $S(x, y) = 0$ on en déduit $x = \pm\frac{2}{3}$: le couple (x, y) est l'un des 4 couples $(\pm\frac{2}{3}, \pm\frac{\sqrt{2}}{3})$ (les choix des signes pour chacune des coordonnées étant indépendants). Réciproquement on vérifie que ces couples sont tels que $R(x, y) = S(x, y) = 0$.

Problème.

1. C'est l'exponentiation rapide. Son coût est en $O(\log n)$.

2. Si $x = y^2$ alors $x^{\frac{p-1}{2}} = y^{p-1} = 1$ car le groupe $\mathbb{F}_p^*$ est d'ordre $p - 1$. Donc l'ensemble C des carrés de $\mathbb{F}_p^*$ est contenu dans l'ensemble R des racines du polynôme $X^{\frac{p-1}{2}} - 1$. Or $\operatorname{Card} R \leq \deg(X^{\frac{p-1}{2}} - 1) = \frac{p-1}{2}$ et $\operatorname{Card} C = \frac{p-1}{2}$ (puisque C est l'image du morphisme de groupes $y \mapsto y^2$, de $\mathbb{F}_p^*$ dans lui-même, dont le noyau est formé des 2 éléments 1 et -1, distincts car p est impair) ; donc $C = R$. Une autre preuve consiste à choisir un générateur ω du groupe cyclique $\mathbb{F}_p^*$ et à constater que les carrés sont les puissances paires de ω.

3. Pour tester si $x \in \mathbb{F}_p^*$ est un carré, on calcule $x^{\frac{p-1}{2}}$ par exponentiation rapide et on regarde si on obtient 1. Le coût de ce calcul est en $O(\log p)$ multiplications dans $\mathbb{F}_p$.

4. ($\star$)

```
sage: def detection(p, x):
....:     """
....:     Détecte si ‘x‘ est un carré modulo ‘p‘
....:     """
....:     F = GF(p)
....:     x = F(x)
....:     if x == 0:
....:         return 0
....:     r = x^((p-1)/2)
....:     if r == 1:
....:         return 1
....:     return -1
....:
```

5. Comme $\mathbb{K}$ est de caractéristique différente de 2 et $a \neq 0$, on a

$$P(X) = a\Big((X + \frac{b}{2a})^2 + \frac{c}{a} - \frac{b^2}{4a^2}\Big) = a\Big((X + \frac{b}{2a})^2 - \frac{\Delta}{4a^2}\Big).$$

   Etant donné $x \in \mathbb{K}$, on a donc $P(x) = 0$ si, et seulement si, $\Delta = 4a^2(x + \frac{b}{2a})^2$, c'est-à-dire $\Delta = \delta^2$ avec $\delta = 2a(x + \frac{b}{2a})$. En particulier, si P admet une racine $x \in \mathbb{K}$ alors Δ est un carré dans $\mathbb{K}$. Si $\Delta = 0$ alors $-\frac{b}{2a}$ est l'unique racine de P dans $\mathbb{K}$. Enfin, si Δ est un carré non nul dans $\mathbb{K}$ alors P a deux racines distinctes dans $\mathbb{K}$ qui sont $\frac{-b\pm\delta}{2a}$ où $\delta \in \mathbb{K}$ vérifie $\delta^2 = \Delta$.

6. Le discriminant du polynôme $X^2 + uX + a$ est $\Delta = u^2 - 4a$. Ce polynôme est irréductible dans $\mathbb{F}_p[X]$ si, et seulement si, il n'a pas de racine dans $\mathbb{F}_p$ (car il est de degré 2) ; d'après la question précédente c'est le cas si, et seulement si, $u^2 - 4a$ n'est pas un carré dans $\mathbb{F}_p$.

7. ($\star$)

```
sage: def construction(p, a):
....:     """
....:     Renvoie ‘u‘ dans ‘GF(p)‘ tel que ‘X^2 + u * X + a‘ est irréductible
....:     """
....:     F = GF(p)
....:     a = F(a)
....:     while True:
....:         u = F.random_element()
....:         if detection(p, u^2 - 4 * a) == -1:
....:             return u
....:
```

8. ($\star$) La commande

```
sage: construction(13, 5)
```

   renvoie un des nombres suivants: 0, 1, 3, 5, 8, 10, 12. Pour obtenir la liste complète (ce qui n'est pas demandé) on pourrait faire comme suit :

```
sage: p = 13
sage: F = GF(13)
sage: F = GF(p)
sage: a = F(5)
sage: [u for u in F if detection(p, u^2-4*a) == -1]
[0, 1, 3, 5, 8, 10, 12]
```

9. On a $P(t) = 0$ par construction. Comme P est à coefficients dans $\mathbb{F}_p$, on a aussi $P(t^p) = P(t)^p$, donc $P(t^p) = 0$. Enfin $t^p \neq t$ car $t \notin \mathbb{F}_p$.

10. Le produit des racines de P, qui est unitaire et de degré 2, est égal à son coefficient constant : $t^{p+1} = a$. En posant $k = \frac{p+1}{2}$ et $b = t^k$ on a donc $b^2 = a$. Comme a est un carré dans $\mathbb{F}_p$, le polynôme $X^2 - a$ est scindé sur $\mathbb{F}_p$: toutes ses racines dans $\mathbb{K}$ appartiennent à $\mathbb{F}_p$, notamment b.

11. ($\star$)

```
sage: def racinecarree(p, a):
....:     """
....:     Renvoie une racine carrée de ‘a‘ mod ‘p‘, ou ‘0‘ s’il n’y en a pas
....:     """
....:     F = GF(p)
....:     a = F(a)
....:     if detection(p, a) == 1:
....:         u = construction(p, a)
....:         T = polygen(F)
....:         K.<t> = GF(p^2, modulus=T^2+u*T+a)
....:         b = F(t^((p+1)/2))
....:         return b
....:     return 0
....:
```

12. ($\star$)

```
sage: p0 = 2^17 - 1sage: a = 80975
sage: b = racinecarree(p0, a)
sage: b
129837
sage: -b
1234
sage: Integer(min(b, -b))
1234
```

13. Notons φ l'application de H_t dans $\mathbb{F}_p^*$ qui à tout couple (x, y) associe $x - y$. Comme l'équation de H_t s'écrit $(x-y)(x+y) = t$, on voit que φ est bien à valeurs dans $\mathbb{F}_p^*$ et qu'elle est bijective (puisqu'en caractéristique différente de 2, la somme et la différence de deux nombres les déterminent de façon unique). On a donc Card $H_t = p - 1$.

14. Notons E_t l'ensemble des $x \in \mathbb{F}_p$ tels que $x^2 - t$ soit un carré de $\mathbb{F}_p$, et $\psi : H_t \to E_t$ la première projection (définie par $(x, y) \mapsto x$). Alors ψ est surjective par construction ; étant donné $x \in E_t$, les antécédents de x par ψ sont les couples (x, y) avec $y \in \mathbb{F}_p$

tel que $y^2 = x^2 - t$. Lorsque $x^2 = t$, ce qui est le cas pour deux valeurs de x, il y a un et seul antécédent (à savoir $(x, 0)$). Pour toutes les autres valeurs de x (il y en a Card $E_t - 2$), il y a deux antécédents. On a donc Card $H_t = 2 \times 1 + (\text{Card } E_t - 2) \times 2$. En utilisant la question précédente on obtient bien Card $E_t = \frac{p+1}{2}$.

15. A chaque fois qu'on choisit aléatoirement un élément $u \in \mathbb{F}_p$, la question précédente montre que la probabilité que $u^2 - 4a$ soit un carré est égale à $\frac{(p+1)/2}{p} \leq 2/3$ (le cas le pire étant $p = 3$; en fait cet algorithme n'est intéressant que lorsque p est grand, et alors cette probabilité est très proche de $1/2$). D'après la question 6, il y a moins de 2 chances sur 3 que le polynôme $X^2 + uX + a$ ne soit pas irréductible. Si on répète l'expérience N fois de façon indépendante, la probabilité de ne trouver aucun u tel que $X^2 + uX + a$ soit irréductible est inférieure ou égale à $(2/3)^N$. Si la fonction `construction` de la question 7 ne termine pas, c'est que pour tout N on est dans ce cas : cela n'arrive qu'avec une probabilité nulle. Comme $(2/3)^{12} < 10^{-2}$, dans 99 cas sur 100 la fonction `construction` trouvera une valeur convenable de u en 12 itérations maximum. Chaque itération coûte $O(\log p)$ opérations arithmétiques dans $\mathbb{F}_p$ d'après la question 3 ; le coût de la fonction `construction` est donc le même dans 99 cas sur 100. C'est aussi le coût de la fonction `racinecarree`, qui utilise l'exponentiation rapide dans $\mathbb{K}$, car chaque multiplication dans $\mathbb{K}$ coûte $O(1)$ opérations arithmétiques dans $\mathbb{F}_p$.