Chercher les points d'une courbe sur un corps fini

Erwan Biland - 10 février 2011

On s'intéresse à la courbe projective C d'équation $x^4 + y^4 + z^4 = 0$, définie sur le corps F_5 à 5 éléments. Pour simplifier, vu le rôle symétrique des variables, on prendra $z = 1$. La courbe C n'a clairement pas de point de degré 1 sur F_5.

On trouve facilement, sur F_{5^2}, le point $\left[\sqrt{2} : 0 : 1\right]$, qui fournit un point de degré 2 sur F_5.

On cherche ensuite un point de degré 3. Le corps F_{5^3} est le corps de rupture du polynôme irréductible $t^3 + t + 1$. Notons en a une racine, et commençons par déterminer l'ordre de a dans le groupe multiplicatif $F_{5^3}^*$.

```
i := 1 : b := a :
while (i < 5^3 and b ≠ 1) do
    i := i + 1 :
    b := rem(a·b, a^3 + a + 1, a) mod 5
od :
print(i)
```

62 **(1)**

Comme $5^3 - 1 = 124 = 4 \cdot 31$, on obtient que a^2 engendre le sous-groupe des éléments d'ordre impair dans $F_{5^3}^*$, qui est aussi l'ensemble des éléments admettant une racine quatrième dans $F_{5^3}^*$. On va donc chercher x_0 et y_0 dans ce sous-groupe tels que $x_0 + y_0 + 1 = 0$.

```
i := 1 : j := 1 :
x_0 := a^2 : y_0 := a^2 : somme := 2·a^2 + 1 :
while (i < 31 and somme ≠ 0) do
    if j = i then i := i + 1 : j := 1 :
                  x_0 := rem(a^2·x_0, a^3 + a + 1, a) : y_0 := a^2 :
              else j := j + 1 :
                  y_0 := rem(a^2·y_0, a^3 + a + 1, a) :
    fi :
    somme := x_0 + y_0 + 1 mod 5 :
od :
if somme = 0 then print(i, j)
             else print("Aucun point trouvé")
 fi:
```

12, 2 **(2)**

$rem\left(a^{24}+a^4+1, a^3+a+1, a\right) \bmod 5$

0 **(3)**

On a donc trouvé sur F_{5^3} le point $\left[a^6 : a : 1\right]$, ce qui vérifie le résultat annoncé dans l'exposé (toute courbe projective lisse sur un corps fini possède des points de degrés premiers entre eux dans leur ensemble).

A noter que j'avais annoncé qu'il n'y avait pas dans C de point de degré 3, mais qu'il y en avait de degré 5 ; la première partie est fausse (erreur de programmation...), mais la deuxième est vraie comme on le vérifie ci-dessous (avec le polynôme irréductible $x^5 - x - 1$).

$i := 1 : b := a :$
while $\left(i < 5^5 \text{ and } b \neq 1\right)$ **do**
$i := i + 1 :$
$b := rem\left(a \cdot b, a^5 - a - 1, a\right) \bmod 5$
od :
$print(i)$

781 **(4)**

$i := 1 : j := 1 :$
$x_0 := a : y_0 := a : somme := 2 \cdot a + 1 :$
while $(i < 781 \text{ and somme} \neq 0)$ **do**
if $j = i$ **then** $i := i + 1 : j := 1 :$
$x_0 := rem\left(a \cdot x_0, a^5 - a - 1, a\right) : y_0 := a :$
else $j := j + 1 :$
$y_0 := rem\left(a \cdot y_0, a^5 - a - 1, a\right) :$
fi :
$\text{somme} := x_0 + y_0 + 1 \bmod 5 :$
od :
if $somme = 0$ **then** $print(i, j)$
else $print(\text{"Aucun point trouvé"})$
fi

163, 90

$$\frac{(781 + 163)}{4}$$

236

$$\frac{(781 \cdot 2 + 90)}{4}$$

413

$rem\left(a^{236 \cdot 4} + a^{413 \cdot 4} + 1, a^5 - a - 1, a\right) \bmod 5$

0 **(8)**

D'où le point $\left[a^{236} : a^{413} : 1\right]$.