Racines carrées et cubiques modulo p

La racine carrée

En utilisant la méthode de Shanks, écrire la procédure

```
> sqroot := proc(a,x)
```

qui rend la liste, eventuellement vide, des racines carrées de a dans $\mathbb{F}_p$.

La racine cubique

Le cas $p-1 \neq 0 \pmod 3$

Montrer que chaque élément a de $\mathbb{F}_p$ a une unique racine cubique, et que la fonction racine cubique est une fonction monôme que vous expliciterez.

Ecrire la fonction

```
> cbroot1 := proc(x,p)
```

qui rend la racine cubique de x dans $\mathbb{F}_p$.

Le cas $p-1 = 0 \pmod 3$

1. Montrer que a est un cube dans $\mathbb{F}_p$ si et seulement si $a^{\frac{p-1}{3}} = 1$. Soit b un élément de $\mathbb{F}_p$ qui n'est pas un cube, et $j = b^{\frac{p-1}{3}}$.

2. Montrer qu'il existe des entiers naturels *pairs* e_1, e_2 tels que

$$a^{e_1} b^{e_2} = 1 \pmod p \tag{1}$$

   Montrer que si e_1, e_2 sont deux entiers vérifiant (1) alors e_2 est multiple de 3.

3. Montrer que si $e_1 \equiv 2 \pmod 3$,

$$a^{\frac{e_1+1}{3}} b^{\frac{e_2}{3}}$$

   est une racine cubique de a, et que si $e_1 \equiv 1 \pmod 3$, l'un des deux nombres

$$\pm\, a^{\frac{e_1+2}{6}} b^{\frac{e_2}{6}}$$

   est une racine cubique de a. En déduire un algorithme de résolution de $x^3 = a$ dans $\mathbb{F}_p$. Ecrire la fonction

```
> cbroot2 := proc(x,p)
```

   qui rend la liste des 3 racines cubiques de x ou la liste vide, selon que x est, ou n'est pas, un cube dans $\mathbb{F}_p$, avec p de la forme $3k+1$.

4. Écrire la procédure

```
> cbroot := proc(a,p)
```

qui rend la liste, eventuellement vide, des racines cubiques de a modulo p.