Feuille d'exercices 6

Avertissement : tous les exercices ne seront pas traités durant les séances; pour en suivre l'avancement veuillez consulter mon site personnel dans la rubrique *Forum.*

1. Méthode ρ de Pollard

Exercice 1. — *Factoriser les nombres n en utilisant la méthode ρ de Pollard avec la fonction $f(x)$ et $x_0 = 2$ dans les situations suivantes*

1. $n = 91$, $f(x) = x^2 + 1$ *et* $x_0 = 1$;
2. $n = 4087$, $f(x) = x^2 + x + 1$ *et* $x_0 = 2$;
3. $n = 8051$, $f(x) = x^2 + 1$ *et* $x_0 = 1$.

Exercice 2. — *Soit S un ensemble de cardinal r et f une permutation de S. On considère la suite $x_0 \in S$ et $x_{j+1} = f(x_j)$ d'éléments de S associée à la paire (x_0, f) et soit k le premier indice tel qu'il existe $j < k$ pour lequel $f(x_k) = f(x_j)$. Montrer que :*

1. $k \leq r$ *et pour tout* $1 \leq i \leq r$ *la probabilité que* $k = i$ *est égale à* $1/r$;
2. *la valeur moyenne de k est égale à* $(r + 1)/2$.
3. *Expliquer pourquoi un polynôme linéaire $ax + b$ ne doit pas être utilisé dans la méthode ρ de Pollard.*

Exercice 3. — *Supposons que l'on utilise la méthode ρ de Pollard pour factoriser un entier divisible par un nombre premier noté r et que l'on utilise la fonction $f(x) = x^2$. Soit k le plus petit indice tel qu'il existe $0 \leq l < k$ avec $x_k \equiv x_k \mod r$. On suppose que x_0 est un générateur de $(\mathbb{Z}/r\mathbb{Z})^\times$ et on pose $r - 1 = 2^s t$ avec t impair.*

1. *Ecrire une congruence modulo $r - 1$ qui est équivalente à $x_k \equiv x_l \mod r$;*
2. *Trouver les valeurs de k et l au moyen de s et du développement en base 2 de $1/t$.*
3. *Commenter le choix de $f(x) = x^2$.*

2. Factorisation de Fermat

Exercice 4. — *Montrer que si n a un diviseur a tel que $|a - \sqrt{n}| \leq \sqrt[4]{n}$ alors l'algorithme de Fermat fonctionne dès le premier cran, i.e. pour $t = \sqrt{n} + 1$.*

Exercice 5. — *Factoriser* 200819 *en l'exprimant comme une différence de* 2 *carrés.*

Exercice 6. — *En utilisant* $118^2 \equiv 25 \mod 4633$ *factoriser* $n = 4633$.

Exercice 7. — *En étudiant les carrés de* 67, 68 *et* 69 *modulo* 4633, *factoriser* $n = 4633$.

Exercice 8. — *Factoriser* $n = 4633$ *en utilisant* $68^2 \equiv -9 \mod 4633$, $69^2 \equiv 128 \mod 4633$ *et* $96^2 \equiv -50 \mod 4633$.

Exercice 9. — *Factoriser* $n = 1829$.

3. Fractions continuées

On utilise toujours le principe que n n'est pas premier si et seulement si l'équation $x^2 \equiv 1 \mod n$ a au moins 4 solutions. Evidemment on disposait d'un bon algorithme $\mathcal{A}$ « racine carrée », on factoriserait N comme suit : on prend a au hasard, puis on calcule a^2 dont on prend la racine carrée par l'algorithme $\mathcal{A}$: il y a alors au moins une chance sur deux pour que le résultat b soit différent de a de sorte que $n \wedge (a \pm b)$ fournit un diviseur non trivial de n. Evidemment on ne dispose pas de tel algorithme et il est raisonnable de penser qu'il n'en existe pas.

L'idée usuelle est de considérer des paires « aléatoires » d'entiers (x, y) telles que $x^2 \equiv y^2 \mod n$ de sorte que n divise $(x-y)(x+y)$ de sorte que « moralement » il y a une chance sur 2 pour que les facteurs premiers de n se répartissent sur les deux facteurs $(x-y)$ et $(x+y)$. Ainsi le pgcd $(x-y) \wedge (x+y)$ a de bonnes chances de donner un diviseur non trivial de n.

Pour construire de telles paires systématiquement, on utilise les fractions continues : si t est petit avec $x^2 \equiv t \mod n$, alors $x = t + kd^2n$ et donc $(x/d)^2 - kn = t/d^2$ est petit, autrement dit x/d est une bonne approximation de $\sqrt{kn}$. Or on sait que les fractions continues sont de bonnes approximations rationnelles : ainsi on calcule via les fractions continues de bonnes approximations P/Q de $\sqrt{kn}$ pour divers k et on essaie de factoriser $t = P^2 - Q^2kn$ via la base de petits nombres premiers que l'on considère.

Concrètement voici l'algorithme : soit $b_{-1} = 1$, $b_0 = a_0 = \lfloor \sqrt{n} \rfloor$ et $x_0 = \sqrt{n} - a_0$. On calcule $b_0^2 \mod n$ en prenant le représentant de module minimal. Puis pour $i = 1, 2, \cdots$ on construit :

- $a_i = \lfloor \frac{1}{x_{i-1}} \rfloor$ et $x_i = x_{i-1}^{-1} - a_i$;
- $b_i = a_i b_{i-1} + b_{i-2}$ modulo n ;
- $b_i^2 \mod n$,

où modulo n on prend toujours le représentant de module minimal. On regarde ensuite les nombres $b_i^2 \mod n$ qui s'écrivent comme ± 1 fois un produit de petit nombres premiers ; soit B la base de ces nombres premiers auquel on rajoute -1 et on associe à chacune de ces $b_i^2 \mod n$ un vecteur $\overrightarrow{\epsilon_i}$ de $\mathbb{F}_2^k$. On construit ensuite une combinaison linéaire nulle de ces $\overrightarrow{\epsilon_i}$ à laquelle on associe $b = \prod_i b_i$ et $c = \prod_j p_j^{\gamma_j}$ et on espère que $(b \pm c) \wedge n$ nous fournit un facteur non trivial.

Exercice 10. — *Utilisez l'algorithme ci-dessus pour factoriser* 9073.

Exercice 11. — *Utilisez l'algorithme ci-dessus pour factoriser* 17873.

4. Solutions

1 (1) On a $x_1 = 2$, $x_2 = 5$, $x_3 = 26$ et $x_4 \equiv 40 \mod 91$ et $(x_4 - x_3) \wedge n = 14 \wedge 91 = 7$.

(2) On trouve

$$\begin{array}{rlr} x_1 = f(2) = 7 & & (x_1 - x_0) \wedge n = (7-2) \wedge 4087 = 1 \\ x_2 = f(7) = 57 & & (x_2 - x_1) \wedge n = (57-7) \wedge 4087 = 1 \\ x_3 = f(57) = 3307 & & (x_3 - x_1) \wedge n = (3307-7) \wedge 4087 = 1 \\ x_4 = f(3307) \equiv 2745 & \mod 4087 & (x_4 - x_3) \wedge n = (2745-3307) \wedge 4087 = 1 \\ x_5 = f(2745) \equiv 1343 & \mod 4087 & (x_5 - x_3) \wedge n = (1343-3307) \wedge 4087 = 1 \\ x_6 = f(1343) \equiv 2626 & \mod 4087 & (x_6 - x_3) \wedge n = (2626-3307) \wedge 4087 = 1 \\ x_7 = f(2626) \equiv 3734 & \mod 4087 & (x_7 - x_3) \wedge n = (3374-3307) \wedge 4087 = 61 \end{array}$$

et donc $4087 = 61 \times 67$.

(3) On obtient $(x_6 - x_3) \wedge n = (2839 - 26) \wedge 8051 = 97$ et $8051 = 83.97$.

2 (1) Montrons par récurrence sur $1 \leq k \leq r$ que la probabilité que $x_0, \cdots, x_{k-1}$ soient distincts alors que x_k est égal à l'un des x_j pour $0 \leq j < k$ est égale à $1/r$. Pour $k = 1$ il y a une probabilité $1/r$ que $f(x_0) = x_0$. Supposons le résultat acquis jusqu'au rang $k-1$ et traitons le cas de k. La probabilité que $x_0, \cdots, x_{k-2}$ soient distincts est donc $1 - \frac{k-1}{r}$ et alors comme $f(x_{k-1})$ peut prendre $r - k + 1$ valeurs dont l'intersection avec $\{x_0, \cdots, x_{k-1}\}$ est réduit à x_0 de sorte qu'il y a une probabilité $\frac{1}{r-(k-1)}$ que $f(x_k) = x_0$ et donc la probabilité cherché est le produit $\frac{r-(k-1)}{r} \frac{1}{r-(k-1)} = \frac{1}{r}$.

(2) La moyenne cherchée est l'espérance $\frac{1}{r} \sum_{k=1}^{r} k == \frac{1}{r} r(r+1)/2 = (r+1)/2$.

(3) Supposons que $a \wedge n = 1$ (sinon on a une factorisation !) alors $f(x) = ax + b$ est une bijection de $\mathbb{Z}/r\mathbb{Z}$ pour tout $r|n$ et donc le nombre de pas attendu est d'ordre $r/2$ au lieu de $\sqrt{r}$ dans la méthode habituelle.

3 (1) On a $2^k \equiv 2^l \mod r-1$.

(2) On a $l = s$ et $k = s + m$ où m est l'ordre de 2 modulo t, i.e. le plus petit entier tel que $2^m \equiv 1 \mod t$ et donc la période du développement 2-adique de $1/t$.

(3) On voit que k peut être aussi grand que r ; par exemple si $r - 1 = 2p$ avec 2 un générateur de $\mathbb{F}_p^\times$.

4 Soit $n = ab$ avec $a > b$; si $a < \sqrt{n} + \sqrt[4]{n}$ alors $b > \frac{n}{\sqrt{n}+\sqrt[4]{n}} > \sqrt{n} - \sqrt[4]{n}$. De même si $b > \sqrt{n} - \sqrt[4]{n}$ alors on a $a < \sqrt{n} + \sqrt[4]{n} + 2$ sinon $n = ab > (\sqrt{n} + \sqrt[4]{n} + 2)(\sqrt{n} - \sqrt[4]{n}) = n + \sqrt{n} - 2\sqrt[4]{n} > n$ si $n > 15$. Dans tous les cas on a $a - b < 2(\sqrt[4]{n} + 1)$. Or si la factorisation de Fermat ne marche pas au premier cran alors $t > \sqrt{n} + 1$ et donc $s = \sqrt{t^2 - n} > \sqrt{(\sqrt{n}+1)^2 - n} = \sqrt{2\sqrt{n}+1} > \sqrt{2}\sqrt[4]{n}$ ce qui contredit la relation $s = (a-b)/2 < \sqrt[4]{n} + 1$ dès que $n > 33$.

5 On a $\lfloor \sqrt{200819} \rfloor + 1 = 449$ et $449^2 - 200819 = 782$ qui n'est pas un carré parfait. On essaye avec $450^2 - 200819 = 1681 = 41^2$ et donc $200819 = 450^2 - 41^2 = 491.409$.

6 On calcule $(118 + 5) \wedge 4633 = 41$ (ou aussi $(118 - 5) \wedge 4633 = 113$) ce qui donne $4633 = 41.113$.

7 On a $67^2 \equiv -144 \mod 4633$ et $68^2 \equiv -9 \mod 4633$ ainsi que $69^2 \equiv 128 \mod 4633$. Ainsi pour $B = \{-1, 2, 3\}$ on est dans la situation de l'algorithme où le vecteur de $\mathbb{F}_2^3$ associé à 67 (resp. 68, resp. 69) est $(1,0,0)$ (resp. $(1,0,0)$, resp. $(0,1,0)$) ce qui suggère de considérer $67.68 \equiv -77 \mod 4633$ et $c = 2^2 3^2 = 36$ ainsi que $(-77+36) \wedge 4633 = 41$.

8 On considère donc $B = \{-1, 2, 3, 5\}$ avec les vecteurs de $\mathbb{F}_2^4$ associés à 68, 69 et 96 : $e_1 = (1,0,0,0)$, $e_2 = (0,1,0,0)$ et $e_3 = (1,1,0,0)$. Comme $e_1 + e_2 + e_3 = 0$, on considère $b = 68.69.96 \equiv 1031 \mod 4633$ et $c = 2^4.3.5 = 240$ avec $(240 + 1031) \wedge 4633 = 41$.

9 Pour $k = 1, 2, \cdots$ on calcule $\lfloor \sqrt{1829k} \rfloor$ et $\lfloor \sqrt{1829k} \rfloor + 1$ ce qui donne le tableau suivant :

b_i	-1	2	3	5	7	11	13
42	1			1			1
43		2		1			
61			2		1		
74	1					1	
85	1				1		1
86		4		1			

ce qui fournit $(b_2b_6)^2 \equiv (2^3 5)^2 \mod 1829$ soit $(43.86)^2 \equiv 40^2 \mod 1829$ mais comme $43.86 \equiv 40 \mod 1829$ on obtient une relation triviale.

On cherche alors une autre relation : $(42.43.61.85)^2 \equiv (2.3.5.7.13)^2 \mod 1820$ soit $1459^2 \equiv 901^2 \mod 1829$ et $(1459 + 910) \wedge 1829 = 59$.

10 On établit le tableau suivant :

i	0	1	2	3	4
a_i	95	3	1	26	2
b_i	95	286	381	1119	2619
$b_i^2 \mod n$	-48	139	-7	87	-27

On considère alors $B = \{-1, 2, 3, 7\}$ avec $i = 0, 2, 4$ et les vecteurs $(1, 0, 1, 0)$, $(1, 0, 0, 1)$ et $(1, 0, 1, 0)$. La somme du premier et du troisième vecteur étant nulle, on obtient $b = 95.2619 \equiv 3834 \mod 9073$ et $c = 2^2.3^2$ et donc $3834^2 \equiv 36^2 \mod 9073$ avec $(3834 + 36) \wedge 9073 = 43$ et donc $9073 = 43.211$.

11 On établit le tableau suivant :

i	0	1	2	3	4	5
a_i	133	1	2	4	2	3
b_i	133	134	401	1738	3877	13369
$b_i^2 \mod n$	-184	83	-56	107	-64	161

On considère alors $B = \{-1, 2, 7, 23\}$ avec $i = 0, 2, 4, 5$ et les vecteurs $(1, 1, 0, 1)$, $(1, 1, 1, 0)$ et $(1, 0, 0, 0)$ et $(0, 0, 1, 1)$. La somme du premier, du deuxième et du quatrième étant nulle ce qui donne $b = 133.401.13369 \equiv 1288 \mod 17873$ et $c = 2^3.7.23 = 1288$ mais alors $b \equiv c \mod 17873$. On continue alors la table précédente

i	6	7	8
a_i	1	2	1
b_i	17246	12115	11488
$b_i^2 \mod n$	-77	149	-88

ce qui suggère de rajouter 11 à notre base B avec $i = 0, 2, 4, 5, 6, 8$ et les vecteurs $e_1 = (1, 1, 0, 0, 1)$, $e_2 = (1, 1, 1, 0, 0)$, $e_3 = (1, 0, 0, 0, 0)$, $e_4 = (0, 0, 1, 0, 1)$, $e_5 = (1, 0, 1, 1, 0)$ et $e_6 = (1, 1, 0, 1, 0)$. On a $e_1 + e_2 + e_3 + e_5 + e_6 = 0$ ce qui fournit $b = 7272$ et $c = 4928$ avec $(7272 + 4928) \wedge 17873 = 61$ et $17873 = 61.293$.