Cryptographie à clé publique
Cours 7

Julien Lavauzelle

Université Paris 8

Master 1 mathématiques et applications – parcours ACC

18/03/2026

Premiers algorithmes

Divisions successives et méthode de Fermat... en cours !

Plan

Périodicité des suites récurrentes finies

Contexte. Soit E un ensemble fini de cardinal M, et f une fonction $E \to E$. Étant donné $x_0 \in E$, on définit une suite récurrente $(x_t)_{t\geq 0}$ par

$$x_{t+1} = f(x_t)\,.$$

Périodicité des suites récurrentes finies

Contexte. Soit E un ensemble fini de cardinal M, et f une fonction $E \to E$. Étant donné $x_0 \in E$, on définit une suite récurrente $(x_t)_{t\geq 0}$ par

$$x_{t+1} = f(x_t)\,.$$

Alors on sait que $(x_t)_{t\geq 0}$ est ultimement périodique :

$$\exists T \geq 0, \exists \tau \geq 1, \forall t \geq T,\ x_{t+\tau} = x_t\,.$$

Périodicité des suites récurrentes finies

Contexte. Soit E un ensemble fini de cardinal M, et f une fonction $E \to E$. Étant donné $x_0 \in E$, on définit une suite récurrente $(x_t)_{t\geq 0}$ par

$$x_{t+1} = f(x_t)\,.$$

Alors on sait que $(x_t)_{t\geq 0}$ est ultimement périodique :

$$\exists T \geq 0, \exists \tau \geq 1, \forall t \geq T,\ x_{t+\tau} = x_t\,.$$

Déf. Le plus petit τ est appelé la **période**. Le plus petit T est appelé la **prépériode**.

Périodicité des suites récurrentes finies

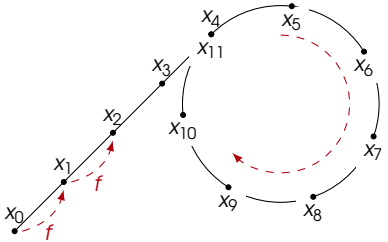
Contexte. Soit E un ensemble fini de cardinal M, et f une fonction $E \to E$. Étant donné $x_0 \in E$, on définit une suite récurrente $(x_t)_{t\geq 0}$ par

$$x_{t+1} = f(x_t)\,.$$

Alors on sait que $(x_t)_{t\geq 0}$ est ultimement périodique :

$$\exists T \geq 0, \exists \tau \geq 1, \forall t \geq T,\ x_{t+\tau} = x_t\,.$$

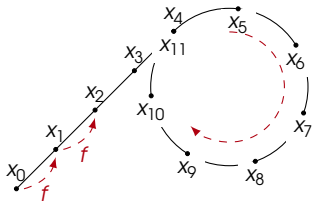
Déf. Le plus petit τ est appelé la **période**. Le plus petit T est appelé la **prépériode**.



Sur l'exemple, on a

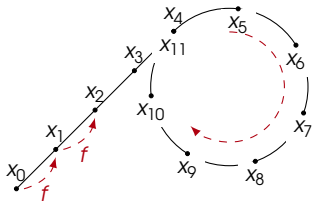
- une période de 7,
- et une prépériode de 11.

Périodicité des suites récurrentes finies



Question. Si f et x_0 sont aléatoires, quelle est la taille typique de T ?

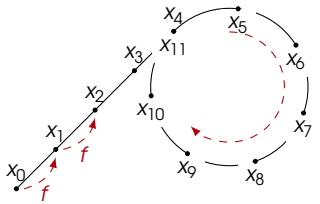
Périodicité des suites récurrentes finies



Question. Si f et x_0 sont aléatoires, quelle est la taille typique de T ?

On a $T > m$, si et seulement si les $\{x_t\}_{t \leq m}$ sont distincts.

Périodicité des suites récurrentes finies

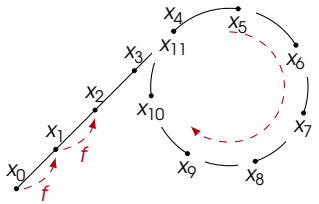


Question. Si f et x_0 sont aléatoires, quelle est la taille typique de T ?

On a $T > m$, si et seulement si les $\{x_t\}_{t \leq m}$ sont distincts.
Si f donne une suite aléatoire, on a donc d'après le **paradoxe des anniversaires** :

$$\begin{aligned}\mathbb{P}(T > m) &= \mathbb{P}(x_1 \neq x_0) \times \mathbb{P}(x_2 \notin \{x_1, x_0\}) \times \cdots \times \mathbb{P}(x_m \notin \{x_{m-1}, \ldots, x_0\}) \\ &= \left(1 - \frac{1}{M}\right)\left(1 - \frac{2}{M}\right) \ldots \left(1 - \frac{m}{M}\right) \simeq e^{-m^2/2M} \quad \text{pour } m \ll M\,.\end{aligned}$$

Périodicité des suites récurrentes finies



Question. Si f et x_0 sont aléatoires, quelle est la taille typique de T ?

On a $T > m$, si et seulement si les $\{x_t\}_{t \leq m}$ sont distincts.
Si f donne une suite aléatoire, on a donc d'après le **paradoxe des anniversaires** :

$$\begin{aligned}\mathbb{P}(T > m) &= \mathbb{P}(x_1 \neq x_0) \times \mathbb{P}(x_2 \notin \{x_1, x_0\}) \times \cdots \times \mathbb{P}(x_m \notin \{x_{m-1}, \ldots, x_0\}) \\ &= \left(1 - \frac{1}{M}\right)\left(1 - \frac{2}{M}\right) \ldots \left(1 - \frac{m}{M}\right) \simeq e^{-m^2/2M} \quad \text{pour } m \ll M\,.\end{aligned}$$

Conséquence. Avec grande probabilité, la suite $(x_t)_{t \geq 0}$ a une prépériode de taille $O(\sqrt{M})$.

Application à la factorisation

Soit $N \in \mathbb{Z}$ à factoriser, et p son plus petit facteur premier, inconnu.

Idée : On prend $E = \mathbb{Z}/N\mathbb{Z}$, et on choisit $x_0 \in \mathbb{Z}/NZ$ aléatoire et $f \in \mathbb{Z}/N\mathbb{Z}[X]$ au comportement itéré aléatoire (heuristique). Alors,

- la suite $(x_t \mod p)_{t \geq 0}$ a une prépériode de taille $O(\sqrt{p})$,
- sans connaître p, on peut détecter une collision pour la suite $(x_t \mod p)$ en calculant $\mathrm{pgcd}(x_j - x_i, N)$.

Application à la factorisation

Soit $N \in \mathbb{Z}$ à factoriser, et p son plus petit facteur premier, inconnu.

Idée : On prend $E = \mathbb{Z}/N\mathbb{Z}$, et on choisit $x_0 \in \mathbb{Z}/NZ$ aléatoire et $f \in \mathbb{Z}/N\mathbb{Z}[X]$ au comportement itéré aléatoire (heuristique). Alors,

- la suite $(x_t \mod p)_{t\geq 0}$ a une prépériode de taille $O(\sqrt{p})$,
- sans connaître p, on peut détecter une collision pour la suite $(x_t \mod p)$ en calculant $\mathrm{pgcd}(x_j - x_i, N)$.

En **pratique**, des fonctions du type $f(z) = z^2 + a$, avec $a \neq 0$ (ex : $a = 1$), ont un comportement suffisamment aléatoire pour que l'analyse probabiliste tienne.

Avantage : très efficace à calculer.

Application à la factorisation

Soit $N \in \mathbb{Z}$ à factoriser, et p son plus petit facteur premier, inconnu.

Idée : On prend $E = \mathbb{Z}/N\mathbb{Z}$, et on choisit $x_0 \in \mathbb{Z}/NZ$ aléatoire et $f \in \mathbb{Z}/N\mathbb{Z}[X]$ au comportement itéré aléatoire (heuristique). Alors,

- la suite $(x_t \mod p)_{t\geq 0}$ a une prépériode de taille $O(\sqrt{p})$,
- sans connaître p, on peut détecter une collision pour la suite $(x_t \mod p)$ en calculant $\mathrm{pgcd}(x_j - x_i, N)$.

En **pratique**, des fonctions du type $f(z) = z^2 + a$, avec $a \neq 0$ (ex : $a = 1$), ont un comportement suffisamment aléatoire pour que l'analyse probabiliste tienne.

Avantage : très efficace à calculer.

Question. Comment détecter la collision $\mathrm{pgcd}(x_j - x_i, N)$?

Application à la factorisation

Soit $N \in \mathbb{Z}$ à factoriser, et p son plus petit facteur premier, inconnu.

Idée : On prend $E = \mathbb{Z}/N\mathbb{Z}$, et on choisit $x_0 \in \mathbb{Z}/NZ$ aléatoire et $f \in \mathbb{Z}/N\mathbb{Z}[X]$ au comportement itéré aléatoire (heuristique). Alors,

- la suite $(x_t \mod p)_{t \geq 0}$ a une prépériode de taille $O(\sqrt{p})$,
- sans connaître p, on peut détecter une collision pour la suite $(x_t \mod p)$ en calculant $\mathrm{pgcd}(x_j - x_i, N)$.

En **pratique**, des fonctions du type $f(z) = z^2 + a$, avec $a \neq 0$ (ex : $a = 1$), ont un comportement suffisamment aléatoire pour que l'analyse probabiliste tienne.

Avantage : très efficace à calculer.

Question. Comment détecter la collision $\mathrm{pgcd}(x_j - x_i, N)$?

Méthode naïve :

- pour chaque nouvel x_j calculé, on teste la collision potentielle avec les x_i calculés antérieurement ;
- complexité **quadratique** en j en temps, et linéaire en espace.

Application à la factorisation

Soit $N \in \mathbb{Z}$ à factoriser, et p son plus petit facteur premier, inconnu.

Idée : On prend $E = \mathbb{Z}/N\mathbb{Z}$, et on choisit $x_0 \in \mathbb{Z}/NZ$ aléatoire et $f \in \mathbb{Z}/N\mathbb{Z}[X]$ au comportement itéré aléatoire (heuristique). Alors,

- la suite $(x_t \mod p)_{t \geq 0}$ a une prépériode de taille $O(\sqrt{p})$,
- sans connaître p, on peut détecter une collision pour la suite $(x_t \mod p)$ en calculant $\mathrm{pgcd}(x_j - x_i, N)$.

En **pratique**, des fonctions du type $f(z) = z^2 + a$, avec $a \neq 0$ (ex : $a = 1$), ont un comportement suffisamment aléatoire pour que l'analyse probabiliste tienne.

Avantage : très efficace à calculer.

Question. Comment détecter la collision $\mathrm{pgcd}(x_j - x_i, N)$?

Méthode naïve :

- pour chaque nouvel x_j calculé, on teste la collision potentielle avec les x_i calculés antérieurement ;
- complexité **quadratique** en j en temps, et linéaire en espace.

Remarque : si $\mathrm{pgcd}(x_j - x_i, N) = N$ sans avoir obtenu de facteur propre auparavant, il faut changer x_0.

Algorithme de Floyd (années 1960)

Lemme. Soit $(x_t)_{t\geq 0}$ une suite de prépériode T et de période τ. Alors, il existe $i \leq T-1$ tel que $x_{2i} = x_i$.

Preuve.

Algorithme de Floyd (années 1960)

Lemme. Soit $(x_t)_{t\geq 0}$ une suite de prépériode T et de période τ. Alors, il existe $i \leq T-1$ tel que $x_{2i} = x_i$.

Preuve. La différence entre les indices $2i$ et i vaut i. Au moins l'un des $i \leq T-1$ est divisible par la période τ, ce qui assure que $x_{2i} = x_i$.

Algorithme de Floyd (années 1960)

Lemme. Soit $(x_t)_{t\geq 0}$ une suite de prépériode T et de période τ. Alors, il existe $i \leq T-1$ tel que $x_{2i} = x_i$.

Preuve. La différence entre les indices $2i$ et i vaut i. Au moins l'un des $i \leq T-1$ est divisible par la période τ, ce qui assure que $x_{2i} = x_i$.

Exemple. $N = 11 \times 13 = 143$, donc $\sqrt{N} \lesssim 12$ et $\sqrt{p} = \sqrt{11} \lesssim 4$.

Algorithme de Floyd (années 1960)

Lemme. Soit $(x_t)_{t\geq 0}$ une suite de prépériode T et de période τ. Alors, il existe $i \leq T-1$ tel que $x_{2i} = x_i$.

Preuve. La différence entre les indices $2i$ et i vaut i. Au moins l'un des $i \leq T-1$ est divisible par la période τ, ce qui assure que $x_{2i} = x_i$.

Exemple. $N = 11 \times 13 = 143$, donc $\sqrt{N} \lesssim 12$ et $\sqrt{p} = \sqrt{11} \lesssim 4$.

avec $x_0 = 133$

i	x_i	$y_i = x_{2i}$
0	133	133
1	101	49
2	49	127
3	114	127
4	127	127
5	114	127
6	127	127
7	114	127
8	127	127

période = 2
prépériode = 4

avec $x_0 = 34$

i	x_i	$y_i = x_{2i}$
0	34	34
1	13	27
2	27	83
3	15	105
4	83	83
5	26	105
6	105	83
7	15	105
8	83	83

période = 4
prépériode = 4

Algorithme ρ de Pollard

ALGORITHME ρ DE POLLARD POUR LA FACTORISATION (1975)

Entrée : un entier N composé (non-carré)
Sortie : un facteur d de N
Donnée externe : une fonction $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$, typiquement $f(z) = z^2 + 1 \mod N$

1. Tirer a uniformément dans $\{1, \ldots, N-1\}$
2. Initialiser $x \leftarrow f(a)$ et $y \leftarrow f(f(a))$
3. Calculer $d = \mathrm{pgcd}(y - x, N)$
4. **Tant que** $d = 1$:
   - Calculer $x \leftarrow f(x)$
   - Calculer $y \leftarrow f(f(y))$
   - Calculer $d = \mathrm{pgcd}(y - x, N)$
5. **Si** $d = N$, revenir à l'étape 1. **Sinon, retourner** d.

Algorithme ρ de Pollard

ALGORITHME ρ DE POLLARD POUR LA FACTORISATION (1975)

Entrée : un entier N composé (non-carré)
Sortie : un facteur d de N
Donnée externe : une fonction $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$, typiquement $f(z) = z^2 + 1 \mod N$

1. Tirer a uniformément dans $\{1, \dots, N-1\}$
2. Initialiser $x \leftarrow f(a)$ et $y \leftarrow f(f(a))$
3. Calculer $d = \mathrm{pgcd}(y - x, N)$
4. **Tant que** $d = 1$:
   - Calculer $x \leftarrow f(x)$
   - Calculer $y \leftarrow f(f(y))$
   - Calculer $d = \mathrm{pgcd}(y - x, N)$
5. **Si** $d = N$, revenir à l'étape 1. **Sinon, retourner** d.

Complexité.

- Le nombre d'itérations de la boucle 4. est $O(\sqrt{p})$ avec grande probabilité, où p est le plus petit facteur premier de N.
- On a $\mathrm{pgcd}(y - x, N) = N$ avec faible probabilité : cela correspond à avoir une collision dans $\mathbb{Z}/N\mathbb{Z}$ avant d'en avoir dans des $\mathbb{Z}/p_i\mathbb{Z}$.

$\Longrightarrow$ complexité en $O(\sqrt{p} \log^2 N)$ opérations dans $\mathbb{Z}/N\mathbb{Z}$.

Algorithme ρ de Pollard

ALGORITHME ρ DE POLLARD POUR LA FACTORISATION (1975)

Entrée : un entier N composé (non-carré)
Sortie : un facteur d de N
Donnée externe : une fonction $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$, typiquement $f(z) = z^2 + 1 \mod N$

1. Tirer a uniformément dans $\{1, \dots, N-1\}$
2. Initialiser $x \leftarrow f(a)$ et $y \leftarrow f(f(a))$
3. Calculer $d = \mathrm{pgcd}(y - x, N)$
4. **Tant que** $d = 1$:
   - Calculer $x \leftarrow f(x)$
   - Calculer $y \leftarrow f(f(y))$
   - Calculer $d = \mathrm{pgcd}(y - x, N)$
5. **Si** $d = N$, revenir à l'étape 1. **Sinon, retourner** d.

Complexité.

- Le nombre d'itérations de la boucle 4. est $O(\sqrt{p})$ avec grande probabilité, où p est le plus petit facteur premier de N.
- On a $\mathrm{pgcd}(y - x, N) = N$ avec faible probabilité : cela correspond à avoir une collision dans $\mathbb{Z}/N\mathbb{Z}$ avant d'en avoir dans des $\mathbb{Z}/p_i\mathbb{Z}$.

$\Longrightarrow$ complexité en $O(\sqrt{p} \log^2 N)$ opérations dans $\mathbb{Z}/N\mathbb{Z}$.

Pollard ρ : exemple

Exemple. Pollard ρ avec $N = 4307$

avec $x_0 = 2747$

x_i	$y_i = x_{2i}$	$\mathrm{pgcd}(x_i - y_i, N)$
146	4089	1
4089	370	1
148	3451	1
370	2027	1
3384	370	1
3451	3451	4307

Pas de chance...

avec $x_0 = 2748$

x_i	$y_i = x_{2i}$	$\mathrm{pgcd}(x_i - y_i, N)$
1334	766	1
766	2188	1
1005	1267	1
2188	620	1
2268	3502	1
1267	2435	73

C'est bon : $N = 73 \times 59$

Pollard ρ : exemple

Exemple. Pollard ρ avec $N = 4307$

avec $x_0 = 2747$

x_i	$y_i = x_{2i}$	$\mathrm{pgcd}(x_i - y_i, N)$
146	4089	1
4089	370	1
148	3451	1
370	2027	1
3384	370	1
3451	3451	4307

Pas de chance...

avec $x_0 = 2748$

x_i	$y_i = x_{2i}$	$\mathrm{pgcd}(x_i - y_i, N)$
1334	766	1
766	2188	1
1005	1267	1
2188	620	1
2268	3502	1
1267	2435	73

C'est bon : $N = 73 \times 59$

Pour $N = 4307$, il y a 516 « mauvais » x_0 : proportion $\simeq 0.12$.

Fait. La proportion de « mauvais » x_0 diminue heuristiquement :

- Pour $N = 253$, il y a 98 « mauvais » x_0 : proportion $\simeq 0.38$.
- Pour $N = 1511057$, il y a 4378 « mauvais » x_0 : proportion $\simeq 0.0029$...

Fin du cours

Questions ?