Théorie Algorithmique des Nombres

Pollard rho

David Kohel

02/11/2020

Pollard rho

02/11/2020 (1)

Algorithme de Floyd (lièvre et tortue)

Idée : construire une suite (a_i, a_{2i}) pour identifier une collision $a_i = a_{2i}$.

Dernière fois : l'algo pour le log discret.

Aujourd'hui : Pollard rho pour la factorisation. La même principe, on cherche une collision mod p dans la suite $a_0, a_1, \dots, a_i, \dots \in \mathbb{Z}/N\mathbb{Z}$, en supposant que $p \mid N$ (inconnu).

On suppose $N = pm$, où p est la plus petit diviseur de N.

On choisit une fonction $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$, par exemple $f(x) = x^2 + 1$ (ou $x^2 + c$).

Comme f est polynomiale on a un diagramme commutatif

$$\begin{array}{ccc} \mathbb{Z}/N\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/N\mathbb{Z} \\ \downarrow & \circlearrowright & \downarrow \\ \mathbb{Z}/p\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/p\mathbb{Z} \end{array}$$

Par le paradoxe des anniversaires, si une suite (a_i) se comporte comme une suite aléatoire, sa réduction mod p doit avoir une collision après $O(\sqrt{p})$ étapes (question de probabilité).

Algorithme

Initialisation

- $(a_0, a_0) = (2,2)$ et $d = 1$.

Itération : pour $i = 1, 2, \ldots$

- $(a_i, a_{2i}) = (f(a_{i-1}), f(f(a_{2i-2})))$
- $d = pgcd(a_{2i} - a_i, N)$.

Si $d \neq 1$, on retourne d (diviseur de N).

Remarque : Si $d = N$, le résultat est ECHEC. Sinon, on a trouvé une factorisation de N.

Idée : On ne connaît pas p, mais on peut détecter la congruence $a_{2i} \equiv a_i \bmod p$ par le $pgcd(a_{2i} - a_i, N)$.

On a construit une suite (a_i) par $a_{i+1} = f(a_i)$, en esperant que cette suite se comporte comme suite aléatoire. Par conséquent, la première congruence doit être après $O(\sqrt{p})$ étapes.

Quel est la probabilité d'ECHEC?

Supposant que q est autre diviseur de N ($p \neq q$), les congruences mod p et mod q sont indépendentes par le théorème chinois :

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \longrightarrow \mathbb{Z}/pq\mathbb{Z} \quad (\mathbb{Z}/N\mathbb{Z})$$

$$\text{dist}_{\text{unif}} \times \text{dist}_{\text{unif}} \Longleftrightarrow \text{dist}_{\text{unif}}$$

Une congruence $a_{2i} \equiv a_i \bmod p$ est indépendente d'une congruence éventuelle $a_{2j} \equiv a_j \bmod q$.

Alors si i est le premier indice tel que $a_{2i} \equiv a_i \bmod p$, alors la proba

d'une collision mod q pour cette indice est $O(1/\sqrt{q})$, où $q > p$. Alors la probabilité d'ECHEC est très faible.

Remarque. En cas d'ECHEC, on peut repéter la construction avec une nouvelle valeur initiale: (a_0, a_0), ou avec une fonction différente: $f(x) = x^2 + c$ pour $c \neq 1$.

Remarque. On observe que l'image $S_1 = f(\mathbb{F}_p)$ est de cardinal proche à $\frac{p}{2}$, car l'application $x \longmapsto x^2+1$ est généruquement 2 à 1. $(\pm x \longmapsto x^2+1)$. $(x \neq 0)$

On peut poser la question des cardinaux des ensembles

$$S_n = f(S_{n-1}),$$

$$S_0 = \mathbb{F}_p \supseteq S_1 \supseteq S_2 \supseteq \cdots$$

$$p \qquad \sim p/2 \qquad \sim 3p/8$$

Voir des exercices pour plus de détailles.

Exemple Supposer $N = 194291$.

On obtient la suite : (pour $f(x) = x^2+1$)

i	a_i	a_{2i}	d
0	2	2	1
1	5	26	1
2	26	69748	1
3	677	155974	$97 = p$

En effet, on a trouvé $N = 97 \cdot 2003$ après trois itérations.

Noter que $f(x) = x^2+1$ donne :

$$0 \to 1 \to \textcircled{2} \to 5 \to 26 \to 677 \to \text{etc.}$$

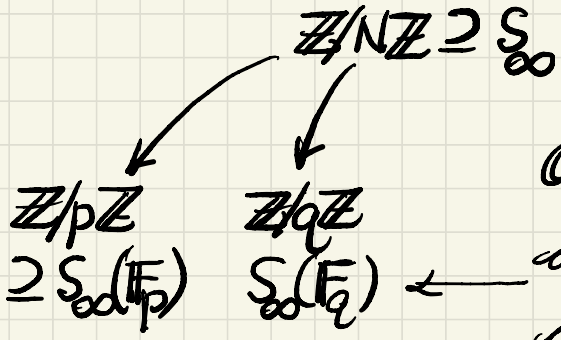
Alors 2 est déjà dans $S_2 = f(f(\mathbb{F}_p))$, où $S_0 = \mathbb{F}_p \supseteq S_1 \supseteq S_2 \supseteq \cdots$

Remarques

1/ Il suffit de connaître N, a_{2i}, a_i pour calculer $\text{pgcd}(a_{2i} - a_i, N)$, et alors pour découvrir d (= p avec haute proba si $d \neq 1$).

2/ $a_{2i} \equiv a_i \bmod p$ ssi $p \mid \text{pgcd}(a_{2i} - a_i, N)$ ssi $a_{2i} - a_i \equiv 0 \bmod p$.

3/ Si la suite (a_i) est restreint à un ensemble $S_\infty = \bigcap_{i \geq 0} S_i$, alors le paradoxe des anniversaires s'appliquent à l'ensemble S_∞ de taille plus petit.

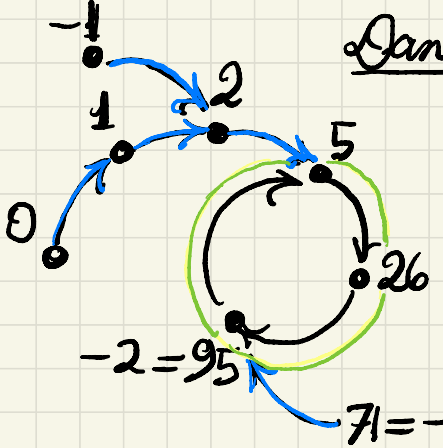


On détecter des collisions dans ces ensembles de taille plus petit.

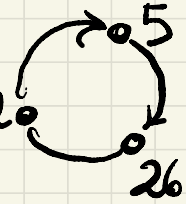
Rappel l'exemple

i	a_i	a_{2i}	$\bar{a}_i$	$\bar{a}_{2i}$	$\bar{a}_i$	
0	2	2	2	2	2	
1	5	26	5	26	5	26
2	26	69748	26	5	26	1646
3	677	155974	95	95	677	1743
			⋮		⋮	

mod 97 mod 2003



Dans $\mathbb{F}_{97}$: On voit la structure du ρ de Pollard, avec cycle :



Question :

Combien de cycles est-ce qu'il y a ?

Combien d'éléments de $\mathbb{F}_{97}$ sont dans un cycle de f ?

Combien d'éléments font partie d'une queue (pas dans un cycle) ?