Stage Factorisation des entiers > channel events — 17 JUIN 2024

Notification Bot 17:12

Publique channel created by F-X. Dehon. **Description:**

> *Aucune description.*

Stage Factorisation des entiers > Sujet

F-X. Dehon MODIFIÉ 17:47

1. **Factorisation des entiers :** algorithmes plus ou moins naïfs, historique notamment nbres de Fermat, algorithme rho de Pollard, expérimentation sur machine
   Sujets connexes : Nombres premiers, Cryptographie RSA
2. **Développement décimal d'un nombre rationnel :** suite récurrente des restes de la division euclidienne, phénomènes de périodicité
3. **One hundred prisonners :** stratégie bien meilleure qu'espéré
4. **Suite récurrente $u_{n+1}=f(u_n)$ où la fonction f ne prends qu'un nombre fini de valeurs :** périodicité à partir d'un certain rang, statistiques sur la longueur de la période lorqu'on choisi f au hasard.

MODIFIÉ 17:51

A propos de (1) :

Codage d'algorithmes naïfs :

- Ce premier algorithme écrit en Basic pour Commodore 64, qu'on peut exécuter en ligne (https://stigc.dk/c64/basic/?s=2NYxJCoAwEATveUXjyeVgEhXUGEFwmznEIPH_X3FAvFZXtdEgb_t-MGO8KSRk5DNHTlkZQnx-oBoN9la1gnfwRFjCCpolyanmomSkcwvicGXG40oXWq06je-VnUgv)

```
10 I=28891:PRINT "I=";I;
20 INPUT "I=";I
30 J=2
40 IF J<I AND I>INT(I/J)*J THEN J=J+1:GOTO 40
50 PRINT J;I/J
```

Le même algorithme en Python, qu'on peut exécuter sur SagemathCell (https://sagecell.sagemath.org/?z=eJzLtDWysLA05OXKsjXi5SrPyMxJVciyyVRIzEtRyFTNUrQ1sMqyzdIGKigoyswr0cjSydTXz9IEAJUADv4=&lang=sage&interacts=eJyLjgUAARUAuQ==) (i%j est le reste de la division entière de i par j):

```
i=28891
j=2
while j<i and i%j!=0:j=j+1
print(j,i//j)
```

- D'autres codages sur le site Rosetta Code (https://rosettacode.org/wiki/Prime_decomposition)

Stage Factorisation des entiers > Programme

F-X. Dehon MODIFIÉ 18:05

Je propose pour demain :

- **Une réflexion sur l'amélioration de l'algorithme naïf de factorisation des entiers :** Comment éviter de tester la divisibilité par les multiples de 2 et 3 une fois la divisibilité par 2 et 3 testée ? Combien de tests éviterait on ainsi si on applique l'algorithme au nombre 101 ? Même chose avec 2,3,5,7.
  Expérimentation Python en ligne sur SagemathCell (https://sagecell.sagemath.org/) par exemple (sélectionner Python au bon endroit).
  Screenshot-from-2024-06-17-17-59-15.png

  Sur SagemathCell on peut copier le lien avec encodé le script qu'on exécute en cliquant sur Share.
  Screenshot-from-2024-06-17-18-03-47.png

  Exemple avec ce lien (https://sagecell.sagemath.org/?z=eJxLtLUwtU6yNTTh5Sooyswr0UjUT9LL00jJTM8sKbY1NdDU5OXi5aqwTVRN4uVKyy9SyFTIzFMoSsxLT9VI0rTi5VIAAojOCk0Ir8JWw9BAq0JTNQkApOUYXA==&lang=sage&interacts=eJyLjgUAARUAuQ==).

- **Une recherche documentaire sur les nombres de Fermat :** pourquoi Fermat s'est il interessé à eux ?

Stage Factorisation des entiers > channel events — 18 JUIN 2024

Notification Bot 15:53

Louna Brémaud a marqué ce sujet comme résolu.

Louna Brémaud a marqué ce sujet comme non résolu. 15:53

Stage Factorisation des entiers > One hundred prisoners

F-X. Dehon MODIFIÉ 17:22

Séance de mardi 18 juin

2n prisonniers, 2n urnes, n=1,2,... avant n=50

- **Disposition :** Les prisonniers comme les urnes sont numérotés de 1 à 2n.
- **Etat (aléatoire) des urnes :** l'urne 1 contient le nombre i_1, etc. k ↦ i_k est une permutation de {1,...,2n} : une fonction bijective de l'ensemble {1,...,2n} dans lui même. Il y a (2n)!=(2n)×(2n-1)×⋯×1 états pour l'ensemble des urnes.
- **Stratégies des prisonniers :** chaque prisonnier choisit comment il va choisir les n=(2n)/2 urnes qu'il a le droit d'ouvrir. Il peut tenir compte du numéro qu'il porte, de la numérotation convenue des urnes et des résultats qu'il obtient progressivement lorsqu'il ouvre les urnes. Combien de stratégies a t-il ainsi pour 2n=4 ? Ce n'est pas très facile à expliciter.
- **Stratégie naïve :** chaque prisonniers choisit d'avance n urnes au hasard ; le succès collectif a alors une probablité de (1/2)^(2n).
- **1/2 :** Il n'y a pas de stratégie donnant au premier prisonnier une probabilité de succès individuel supérieure à 1/2. Pourquoi ?
- **Stratégie spectaculaire :** le prisonnier no k ouvre d'abord l'urne no k, lit le nombre i_k, et, si i_k ≠ k, va à l'urne no i_k, etc.
  Affirmation : cette stratégie donne un succès collectif si et seulement si la permutation (k ↦ i_k, k=1,...,2n) n'a pas de cycle de longueur >n. Cette affirmation est elle vraie ?
  Peut on calculer un majorant <1 de la probabilité qu'une permutation de {1,...,2n} prise au hasard ait un cycle de longueur >50 ? Qu'est ce que cela dit de la probabilité de succès collectif de la stratégie ?
- **Le géolier découvre la stratégie spectaculaire** mise en oeuvre par les prisonniers ; que peut il faire pour la contrer ?
- **Les prisonniers découvrent que le géolier connait et contre leur stratégie spectaculaire** ; que peuvent ils faire pour rétablir le succès (certes pas absolu) de leur stratégie ?

Stage Factorisation des entiers › **Programme** — 24 JUIN 2024

F-X. Dehon — 17:56

Séance de jeudi 20 juin

Recherche documentaire sur le pourquoi de l'intérêt de Fermat pour les nombres dits de Fermat et leur factorisation. La réponse obtenue d'une I.A. "Fermat aimait les mathématiques," est elle satisfaisante ? Comparer avec le pourquoi du style de peinture de Picasso.

MODIFIÉ — 18:10

Séance de lundi 24 juin

Présentation de l'algorithme rho de Pollard de factorisation des entiers. Débriefing demain mardi. Trois éléments de l'exposé :

- Suite $(u_0, u_1, ...)$ définie par récurrence $u_{n+1} = f(u_n)$, à valeur dans $0, ..., n-1$ ⇝ il existe $0 \leq i < j \leq n$ tels que $u_i = u_j$ et alors la suite est périodique à partir du rang i de période de longueur $j - i$.
- Mesure centrale et dispersion de la période lorsqu'on choisit l'application f et le terme initial u_0 au hasard.
- A quoi s'attend t'on lorsqu'on remplace le test d'égalité $u_i = u_j$ par $u_i - u_j$ et n ont un facteur commun > 1 ? On peut efficacement déterminer si $u_i - u_j$ et n ont un facteur commun sans connaître la factorisation de n en calculant le pgcd de $u_i - u_j$ et n (algorithme d'Euclide).

Document pour un TP sur ordinateur en Licence : TP-factorisation-des-entiers.pdf

25 JUIN 2024

F-X. Dehon MODIFIÉ — 16:38

Séance du mardi 25 juin

- Test à la main de l'algorithme rho de Pollard (https://fr.wikipedia.org/wiki/Algorithme_rho_de_Pollard) pour $f(x) = (x^2+1)\%n, n = 10$ puis $n = 11 * 13 = 143, u_0 = 0$ et d'autres valeurs. Nombre et longueurs des cycles pour l'égalité $u_i = u_j$ et l'égalité modifiée $\text{pgcd}(u_i - u_j, n) > 1$ ce qui équivaut à $u_i\%p = u_j\%p$ pour au moins un diviseur premier p de n.
  A faire : test sur SageMathCell, cf la feuille TP-factorisation-des-entiers
- Théorème des restes chinois (https://fr.wikipedia.org/wiki/Th%C3%A9or%C3%A8me_des_restes_chinois) : pour x,y∈ℕ on a x%143 = y%143 si et seulement si x%11 = y%11 et x%13 = y%13.
  x-y et 143 ont un facteur commun >1 si et seulement si x%11 = y%11 **ou** x%13 = y%13.
- A lire (pas facile) Histoire des nombres de Fermat (https://fr.wikipedia.org/wiki/Nombre_de_Fermat) et de leurs factorisations (http://www.prothsearch.com/fermat.html).

Une image

Le graphe d'arrêtes i→f(i) pour n=143. On observe 4 cycles. Selon la valeur de u_0 choisie, la suite (u_n) va vers l'un de ces cycles.
K3.png
K3.svg

28 JUIN 2024

F-X. Dehon — 11:55

Vendredi 28 juin

L'analyse de l'algorithme rho de Pollard dans une feuille de calcul Sagemath (https://math.univ-cotedazur.fr/~dehon/Ens/Sagemath/p%C3%A9riodes.html)

Stage Factorisation des entiers › **Présentation sur la factorisation des entiers** — 1 JUIL. 2024

Gaetan Gil — 11:39

Bonjour, ci-joint notre présentation sur la factorisation des entiers en pdf, bonne journée :
La-factorisation-des-entiers.pdf

F-X. Dehon — 13:19

Gaetan Gil said:

> Bonjour, ci-joint notre présentation sur la factorisation des entiers en pdf, bonne journée :
> La-factorisation-des-entiers.pdf

Merci ! et bon été.