121 – Nombres premiers. Applications.

Question.

Combien d'opérations nécessite le test de tous les témoins dans le test de Solovay-Strassen ?

Réponse.

Si n désigne la taille de N (le nombre à tester), alors chaque test de Solovay-Strassen a une complexité en $O(n^3)$, on obtient donc une complexité de $O(2^n n^3)$, ce qui est moins bon que l'algorithme naïf, de complexité $O(e^{\frac{n}{2}})$ (l'intérêt de Solovay-Strassen étant qu'on n'a pas besoin de tester tous les témoins).

Question.

Dans le théorème d'Erdös-Ginzburg-Ziv, est-ce que $2n-1$ est optimal ?

Réponse.

Oui, car si on prend $n-1$ fois 0 et $n-1$ fois 1, alors on n'a pas de sous-ensemble $I \subset \{1, \dots, 2n-2\}$ tel que $\sum_{i \in I} a_i \equiv 0[n]$.

Question.

Donner un exemple d'anneau non factoriel.

Réponse.

Un anneau non intègre, ou $\mathbb{Z}[X, Y, Z, T]/(XY - ZT)$.

Question.

Là on a mis en défaut l'unicité, une idée pour prouver l'existence en général ?

Réponse.

Quand on a un anneau noetherien, c'est bon.

Question.

Une idée pour la démonstration du théorème de Dirichlet ?

Réponse.

Pour la version faible on utilise des polynômes cyclotomiques. Pour la version forte on utilise de l'anneau complexe, en particulier des fonctions L, du type $s \mapsto \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s}$.

Question.

Qu'est-ce qu'un nombre de Mersenne ? Que peut-on en dire ?

Réponse.

Un nombre de la forme $M_p := 2^p - 1$. Certains de ces nombres sont premiers, en tout cas si p n'est pas premier alors M_p ne l'est pas non plus. En effet, $2^{ab} - 1 = (2^b)^a - 1^a$ qui est divisible par $2^b - 1$.

Question.

On définit la suite $u_0 = 3, u_1 = 0, u_2 = 2$ et $u_n = u_{n-2} + u_{n-3}$. Montrer que pour p premier, $u_p \equiv 0[p]$.

Réponse.

On écrit la suite sous forme matricielle :

$$\begin{pmatrix} u_{n+3} \\ u_{n+2} \\ u_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} u_{n+2} \\ u_{n+1} \\ u_n \end{pmatrix}.$$

On calcule le polynôme caractéristique de la matrice A ci-dessus : $\chi_A = -(X^3 - X - 1)$ et note α, β, γ les racines (pas forcément distinctes) de χ_A.
Par ailleurs, on montre par récurrence que $u_n = \alpha^n + \beta^n + \gamma^n$. En effet, c'est vrai pour les trois premiers termes, et ensuite $\alpha^{n-2} + \alpha^{n-3} = \alpha^{n-3}(\alpha + 1) = \alpha^n$ par définition de α, et on a la même relation pour β et γ.
Finalement, si on regarde u_n dans $\mathbb{F}_p$, on a $u_p = \alpha^p + \beta^p + \gamma^p = (\alpha + \beta + \gamma)^p = \mathrm{tr}(\chi_A) = 0$.

Question.

Soit $n \in \mathbb{N}, a \in \mathbb{N}$ tels que $a \wedge n = 1$. Quelles conditions pour que a soit un carré modulo n ?

Réponse.

On écrit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, alors $a \equiv b^2[n] \iff a \equiv b^2[p_i^{\alpha_i}]$ pour tout i.
Or a est un carré modulo p^α ssi a est un carré modulo p pour $p \neq 2$. Ceci se fait par méthode de Newton.