Sujet TD : Arithmétique

Dominique Michelucci, Université de Dijon

1 PGCD et Fibonacci dans la même galère

1. Combien y a t-il d'appels récursifs, ou d'étapes lors du calcul du PGCD de F_{n-1} et F_n, où F_n est la suite de Fibonacci : $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ pour $n \geq 2$.

2. Soit ϕ et ϕ' les 2 racines de $X^2 = X + 1$, ϕ est la plus grande. Calculer ϕ et ϕ'. ϕ est appelé le nombre d'or. Prouvez que $F_n = a\phi^n + b\phi'^n$ pour 2 constantes a, b que vous calculerez (par exemple en considérant F_0 et F_1) ; ensuite procédez par récurrence.

3. Montrez que $F_n \in O(\phi^n)$.

4. Vous admettrez que le PGCD de 2 nombres successifs dans la suite de Fibonacci est le pire des cas. Quelle est la complexité du nombre d'étapes du calcul du PGCD de $a, b \leq N$. Vous devez trouver qu'il y a $O(\log_\phi N) = O(\log_2 N) = O(\log_e N)$, car tous ces log sont proportionnels.

2 2 méthodes pour calculer l'inverse de t mod P

Soit t un entier donné modulo P. On veut trouver x tel que $tx = 1 \bmod P$. On dit que x est l'inverse de t, et on le note parfois t^{-1} ou $1/t$ (modulo P).

Si P est premier, alors d'après le petit théorème de Fermat, pour tout t non nul, $t^{P-1} = 1 \bmod P$, donc $t \times t^{P-2} = t^{P-1} = 1$, donc t^{P-2} est l'inverse de t

Une autre méthode utilise l'algoritme étendu d'Euclide sur t et P : il donne u, v tel que $tu + Pv = g$ où g est le PGCD de t et P. Si P est premier, et t réduit modulo P, alors u est l'inverse de t : il suffit de considérer $tu + Pv = 1$ modulo P, ce qui donne : $tu + 0 = 1$.

Note : Ceci est cohérent avec le fait que si (u, v, g) est une solution d'Euclide(a, b), (ie $au + bv = g = gcd(a, b)$), alors $(u + b, v - a, g)$ est aussi solution, et donc $u + \lambda b, v - \lambda a, g)$ aussi pour $\lambda \in \mathbb{Z}$.

Si g est différent de 1, cela signifie que P n'est pas premier.

3 Racine carrée mod un nombre premier $P > 2$

3.1 Critère d'Euler

Critère d'Euler : a est un carré modulo P (on dit : un résidu quadratique) ssi $a^{\frac{P-1}{2}} = 1$ modulo P.

Remarquez que, comme x et $-x = P - x$ ont même carré, la moitié des nombres $1, 2, \ldots P - 1$ sont des carrés, et l'autre moitié des non carrés.

Preuve du critère d'Euler : par le petit théorème de Fermat, $x^{p-1} - 1 = (x^{\frac{P-1}{2}} - 1)(x^{\frac{P-1}{2}} + 1)$ considéré modulo P a $p-1$ racines : $1, 2, \ldots p-1$. Les carrés modulo P sont forcément racines de la partie $(x^{\frac{P-1}{2}} - 1)$ puisque

$$(x^2)^{\frac{P-1}{2}} - 1 = x^{P-1} - 1$$

est égal à 0, par le thm de Fermat.

3.2 $P = 3$ modulo 4

Si $P = 3$ modulo 4 (et premier), et si a est un carré (ce qu'on peut décider par le critère d'Euler...), alors une des deux racines carrées de a est

$$x = a^{\frac{P+1}{4}} \text{ car : } x^2 = a^{\frac{P+1}{2}} = a^{\frac{P-1}{2}} a^{\frac{2}{2}} = 1 \times a = a$$

3.3 $P = 1$ mod 4. Méthode de Zassenhauss-Cantor

Si $P = 1$ modulo 4, il n'y a pas de formule, mais l'algorithme probabiliste suivant (qui fonctionne aussi pour $P = 3$ modulo 4 : yapasde raison...). Soit a un résidu quadratique dont on cherche la racine carrée. Soit x cette racine carrée, inconnue. On considère une valeur aléatoire t dans $1, 2, \ldots P-1$, et on calcule $(x+t)^{\frac{P-1}{2}}$; ça vaut ± 1 d'après le petit théorème de Fermat (ou, en utilisant le critère d'Euler, +1 pour un résidu quadratique, -1 pour un non résidu quadratique). Pour calculer $(x+t)^{\frac{P-1}{2}}$, on réduit en remplaçant x^2 par a (puisque par définition $x^2 = a$), et les calculs sont bien sûr réduits modulo P. On trouve donc u, v tels que $(x+t)^{\frac{P-1}{2}} = u + vx$. Si v est différent de 0, on résout : $u + vx = \pm 1$, et on trouve $x = (1-u)v^{-1}$. Attention, $(x+t)^{\frac{P-1}{2}} = \pm 1$ ... sauf quand $t = -x$, voir plus bas. Il faut donc toujours vérifier que $x^2 = a \mod P$, pour détecter cette erreur !

Exemple : $P = 13, a = 10$.

Avec $t = 5$, on trouve $(x+5)^{\frac{P-1}{2}} = 0 + 2x$. Résoudre $2x = 1 \mod 13$ donne $x = 1/2 = 7$, ce qui est correct : $7^2 = 10$. Résoudre $2x = -1 = 12 \mod 13$ donne $x = 6$, qui est bien l'autre racine carrée de 10. Remarquer que 6+7=0 mod 13.

Avec $t = 6$, on obtient $(x+6)^{\frac{P-1}{2}} = 7 + 12x$, qui vaut ± 1. Pour $+1$: $7 + 12x = 1 \Rightarrow x = (1-7)/12 = 6 \mod 13$ et en effet $6^2 = a = 10$. Pour -1 : $7 + 12x = -1 = 12 \Rightarrow x = (12-7)/12 = 8$ mais $8^2 = 12 \neq a$. Problème ! C'est dû au fait que cette valeur de t est l'opposé de la racine carrée 6 de 10 ; donc on a calculé $(t+x)^{\frac{P-1}{2}} = 0^{\frac{P-1}{2}} = 0$, et pas 1. Mais ce cas ne se produit que dans 2 cas sur P. Et il donne malgré tout une racine correcte ; l'autre racine est l'opposée de la racine correcte.

L'essai avec $t = 1$ échoue car $(1+x)^{\frac{P-1}{2}} = 12 + 0x$, qui ne nous apprend rien.

Etudiez le cas $P = 13$. Calculer la table des $x \in 1, 2 \ldots 12$, et les $x^2 \mod 13$. Calculez la racine carrée de 10 avec d'autres valeurs de t.

Bien sûr, il faut utiliser la méthode rapide pour calculer la puissance $(x+t)^{\frac{P-1}{2}}$.

4 Test probabiliste de primalité

Si P est premier, alors pour tout a non nul modulo P, $a^{\frac{P-1}{2}} = \pm 1$. Tester des valeurs aléatoires de a donne un test probabiliste de primalité de P.