

Travaux Dirigés de MT10

Tests de primalité et factorisation

Ce TD a pour objectif de se familiariser avec certains algorithmes de tests de primalité et de factorisation. Les calculs qui y figurent sont conçus pour être effectués de tête (sans calculatrice).

Test de Rabin-Miller

Le test de Rabin est basé sur le seul petit théorème de Fermat, qui affirme que pour tout nombre p premier et tout nombre a non multiple de p alors :

$$a^{p-1} \equiv 1 \pmod{p}$$

Par conséquent étant donné un nombre candidat premier p on peut choisir un nombre test $a < p$ et calculer $a^{p-1} \pmod{p}$. Si le résultat ne vaut pas 1, le nombre candidat n'est certainement pas premier, s'il vaut 1, il l'est peut être (mais pas certainement). On peut recommencer le test avec un autre nombre a .

La seule difficulté est que le nombre p est grand et que le calcul de $a^{p-1} \pmod{p}$ ne peut être effectué en calculant a^{p-1} (qui provoquerait un débordement), mais en utilisant la méthode d'exponentiation rapide.

Nous allons simuler cela en prenant de petites valeurs de p , mais en s'imposant de faire les calculs de tête, il vous sera ensuite très facile d'écrire un programme implémentant le test de Rabin avec méthode d'exponentiation rapide :

Prenons comme candidat premier le nombre 15, même si le nombre test est 3, le calcul mental de 3^{14} est pénible.

- 1) Pour le nombre test 3 calculer successivement $3^2 \pmod{15}$, $3^4 \pmod{15}$, $3^8 \pmod{15}$, puis en remarquant que $3^{14} \pmod{15} = 3^{8+4+2} \pmod{15} = \{(3^8 \pmod{15}) * (3^4 \pmod{15}) \pmod{15}\} * \{3^2 \pmod{15}\} \pmod{15}$ (recaler modulo 15 à chaque fois que c'est possible, calculer $3^{14} \pmod{15}$. Conclusion ?
- 2) Refaire le test avec le nombre test 4. Conclusion ?
- 3) Le test de Miller Rabin permet de rendre les cas où le test est en échec moins fréquents en cumulant avec une autre propriété des nombres premiers : si p est premier $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc l'équation $x^2=1$ (soit donc $(x-1)*(x+1)=0$) n'a que deux racines $x=1$ et $x=-1$ (autre écriture de $p-1$ dans $\mathbb{Z}/p\mathbb{Z}$) : un corps est un anneau intègre donc sans diviseur de zéro. Si donc on trouve un nombre autre que $p-1$ ou 1 dont le carré vaut 1 (racines carrées de l'unité) dans $\mathbb{Z}/p\mathbb{Z}$, alors p n'est certainement pas premier.
 - Au lieu donc de calculer directement a^{p-1} , on cherche le nombre b de fois que 2 divise $p-1$ (la naïveté même en TD a ses limites, le nombre test n'est pas choisi pair !), puis le nombre m tel que $p-1=2^b*m$ (m est donc impair pourquoi ?)
 - On calcule ensuite $a^m \pmod{p}$, si ce nombre vaut 1 ou $p-1$ on s'arrête là et on conclut que le nombre est peut être premier (pourquoi ?)

- Sinon on calcule par élévations au carré successives (modulo p) les puissances 2^i de ce nombre :

Pour i variant de 1 à $b-1$

- ✓ Si on tombe sur $p-1$ on s'arrête là et on conclut que le nombre est peut être premier (pourquoi ?)
- ✓ Si on tombe sur 1 on s'arrête là et on conclut que le nombre n'est certainement pas premier (pourquoi ?)

Indice i suivant

Si l'on est arrivé jusque là sans trouver 1 ou $p-1$, il n'est pas utile de calculer le dernier terme : p n'est certainement pas premier (pourquoi ?)

4) Mise en pratique ! Le nombre test 4 ayant mis en échec le test de Rabin pour le candidat premier 15, essayez le test de Rabin-Miller !

5) A vos calculatrices !

Essayez Rabin-Miller avec le candidat 561 (non pris au hasard... c'est le premier nombre de Carmichael...) et le nombre test 50.

Algorithme p-1 de Pollard

L'algorithme p-1 de Pollard permet dans certains cas de trouver efficacement un des facteurs noté p d'un entier composé. Pour cet algorithme, il faut que l'entier p-1 soit suffisamment « friable » ou « lisse » (traductions approximatives de l'Anglais « smooth »). Voici brièvement ce dont il s'agit :

Un entier p est dit B smooth si tous ses facteurs premiers sont inférieurs ou égaux à B . Tout entier est p est donc p smooth (pourquoi ? dans quel cas c'est exactement p ?)

Un entier est dit B supersmooth si toutes les puissances de nombres premiers qui le divisent sont inférieures ou égales à B . Un entier B supersmooth est donc B -smooth mais la réciproque est évidemment fautive

1) pourquoi ? contre-exemples ? Pour vérifier que vous avez compris : l'entier 12 est combien smooth et combien supersmooth ?

2) Faire la liste des nombres B -supersmooth pour $B=2, 3$ et 4

L'algorithme p-1 de Pollard va fonctionner si l'un des facteurs p du nombre N a factoriser est tel que p-1 est B -supersmooth avec une valeur de B suffisamment petite (très petite devant N sinon la méthode n'a aucun intérêt). Il va donc faire cette hypothèse et la tester avec une valeur de B choisie pas trop grande... en espérant que cela marche (le résultat n'est pas garanti...).

Si un entier q est B supersmooth, alors le produit $B!$ de tous les entiers inférieurs ou égaux à B contient toutes les puissances de nombres premiers qui divisent q , donc $B!$ est multiple de q (réfléchissez... c'est le nœud du raisonnement). Mieux, on peut pour les mêmes raisons dire

que $\text{ppcm}(1,2,\dots,B)$ est multiple de q , selon les ouvrages on trouve la description de l'algorithme avec $B!$ ou $\text{ppcm}(1,2,\dots,B)$

Moralité : si p est un facteur premier de N , B supersmooth, étant donné un nombre test a (non multiple de p , ce qui a peu de chances de se produire, sinon d'ailleurs il serait non premier avec N et on aurait donc aussi trouvé un diviseur commun) :

$a^{p-1} \equiv 1 \pmod{p}$ (Fermat) et $\text{ppcm}(1,2,\dots,B) = k(p-1)$ pour un entier k d'après ce qui précède

- Donc $a^{\text{ppcm}(1,2,\dots,B)} \pmod{p} = a^{k(p-1)} \pmod{p} = 1 \pmod{p}$
 - Donc $a^{\text{ppcm}(1,2,\dots,B)} - 1$ est divisible par p et il en est donc de même de $a^{\text{ppcm}(1,2,\dots,B)} - 1 \pmod{N}$ (car N est aussi divisible par p par hypothèse).
 - Donc $a^{\text{ppcm}(1,2,\dots,B)} - 1 \pmod{N}$ et N sont tous deux divisibles par p (que pour l'instant on ne connaît pas mais si on calcule $\text{pgcd}(a^{\text{ppcm}(1,2,\dots,B)} - 1 \pmod{N}, N)$ on peut espérer le trouver. Noter que le calcul de $a^{\text{ppcm}(1,2,\dots,B)}$ est effectué modulo N et ne nécessite pas de manipuler de nombres beaucoup plus grands que N (exponentiation rapide...).
- 3) Mise en œuvre : supposons que l'on sache que le nombre 7991 n'est pas premier quels sont ses facteurs ? Supposons un de ses facteurs p tel que $p-1$ soit 4-supersmooth ($B=4$) : c'est clairement trop gourmand car cela signifie que N est divisible par 3, 5, 7 ou 13 (pourquoi ?). Essayons tout de même avec $a=2$ comme nombre test. Calculer $\text{ppcm}(1,2,3,4)$ et calculer $a^{\text{ppcm}(1,2,3,4)} \pmod{7991}$ par l'algorithme d'exponentiation rapide (calculatrice juste pour la fin...)
 - 4) Calculer (Euclide, calculatrice ou tableur) $\text{pgcd}(a^{\text{ppcm}(1,2,3,4)} \pmod{7991} - 1, 7991)$
 - 5) Recommencer avec $B=5$ en gardant $a=2$ (calculatrice indispensable ce coup-ci...) et expliquer le résultat obtenu
 - 6) Méthode de Fermat : calculer le nombre immédiatement supérieur à la racine de 7991 et pour les premiers entiers K à partir de ce nombre, calculer les valeurs successives de $K^2 - 7991$. Conclusion ?