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 :

$a^{p-1}[p]=1$

Par conséquent étant donné un nombre candidat premier p on peut choisir un nombre test a<p et calculer $a^{p-1}[p]$. 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 $a^{p-1}[p]$ 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 $3^2[15]$, $3^4[15]$, $3^8[15]$, puis en remarquant que $3^{14}[15]= 3^{8+4+2}[15]= \{(3^8[15]* 3^4[15])\ [15]\}*\{3^2[15]\}[15]$ (recaler modulo 15 à chaque fois que c'est possible, calculer 3^{14} [15]. Conclusion ?

   Solution : présenter un tableau où après avoir écrit en binaire l'exposant 14 : 1110 :

i	**8**	**4**	**2**	**1**	**12**	**14**
Bits de p-1	1	1	1	0		
$3^i[15]$	6	6	9	3	6	9

   Le test conclut donc ici que 15 n'est certainement pas premier

2) Refaire le test avec le nombre test 4. Conclusion ?

   Solution : présenter un tableau où après avoir écrit en binaire l'exposant 14 : 1110 :

i	**8**	**4**	**2**	**1**	**12**	**14**
Bits de p-1	1	1	1	0		
$4^i[15]$	1	1	1	4	1	1

   Par conséquent le test est ici un échec : conclut que 15 est peut être premier.

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 Z/pZ 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 Z/pZ) : 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 Z/pZ, 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 ?) : réponse, sinon on pourrait diviser une fois de plus par 2.
    - On calcule ensuite $a^m[p]$, si ce nombre vaut 1 ou p-1 on s'arrête là et on conclut que le nombre est peut être premier (pourquoi ?) : Réponse : le carré suivant vaut 1, donc le dernier terme 2^b*m aussi, donc ni le théorème de Fermat, ni le fait que les seules racines carrées de 1 sont 1 et -1 n'est violé
    - 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 ?) : Réponse : Idem question précédente
        - ✓ Si on tombe sur 1 on s'arrête là et on conclut que le nombre n'est certainement pas premier (pourquoi ?) : Réponse : comme le premier terme ne valait pas 1 ou -1 et que l'on n'est pas tombé jusque là sur -1, on vient de trouver une racine carrée de 1 différente de 1 ou -1

      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 ?) : Réponse : soit ce dernier terme est différent de 1 et le théorème de Fermat est violé, soit il vaut 1 et on a trouvé une racine carrée de 1 différente de 1 ou -1
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 !

Solution : p-1 vaut 14 = 2*7 donc b=1 et m=7 :

i	**8**	**4**	**2**	**1**	**7**	**14**
Bits de m	0	1	1	0		
$4^i[15]$	1	1	1	4	4	1

Le test montre que $4^2=1$ dans Z/15Z, donc 15 n'est certainement pas premier

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. Conclusion ? Réponse : le test conclut : peut être premier alors que 561=3*11*17

6) Développements possibles en TP : écrire un programme permettant de trouver tous les cas d'échec de Rabin-Miller pour ce nombre
   Ecrire un véritable Rabin Miller compatible avec le format long int
   Ecrire une librairie permettant de manipuler des grands nombres (en utilisant des tableaux d'entiers) : développer l'addition, la soustraction, la multiplication et la division Euclidienne (attention à gérer les exceptions comme le débordement et la division par zéro)
   Utiliser cette librairie (où une librairie du domaine public) pour faire un vrai Rabin Miller sur des grands nombres.
   Utiliser ce Rabin Miller pour faire un générateur de grand nombre probablement premier de taille fixée (pourra être utilisé pour générer des clés RSA).

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 ?) : réponse c'est p si p est premier, c'est le plus grand facteur premier si p ne l'est pas

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 fausse

1) pourquoi ? contre-exemples ? Pour vérifier que vous avez compris : l'entier 12 est combien smooth et combien supersmooth
   (réponses : 3 smooth et 4 supersmooth).
2) Faire la liste des nombres B-supersmooth pour B=2, 3 et 4
   Réponse
   B=2 : 2
   B=3 : le précédent plus 3, 6
   B=4 : les précédents plus 4 et 12

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 ppcm(1,2,…B) est multiple de q, selon les ouvrages on trouve la description de l'algorithme avec B! ou ppcm(1,2…B)

Moralité : si p est un facteur premier de N, tel que p-1 soit B supersmooth, étant donné un nombre test a (non multiple de p, ce qui a peu de chances de se produire) :

$a^{p-1}=1[p]$ (Fermat) et ppcm(1,2..B)=k(p-1) pour un entier k d'après ce qui précède

- Donc $a^{ppcm(1,2…B)}[p] = a^{k(p-1)}[p]= 1[p]$
- Donc $a^{ppcm(1,2…B)}-1$ est divisible par p et il en est donc de même de $a^{ppcm(1,2…B)}-1[N]$ (car N est aussi divisible par p par hypothèse).
- Donc $a^{ppcm(1,2…B)}-1[N]$ et N sont tous deux divisibles par p (que pour l'instant on ne connaît pas mais si on calcule pgcd($a^{ppcm(1,2…B)}-1[N]$,N) on peut espérer le trouver. Noter que le calcul de $a^{ppcm(1,2…B)}$ 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 ?) : Réponse grâce à la liste des 4-supersmooth établie plus haut. Essayons tout de même avec a=2 comme nombre test. Calculer ppcm(1,2,3,4) (réponse : 12 alors que 4 !=24) et calculer $a^{ppcm(1,2,3,4)}$ [7991] par l'algorithme d'exponentiation rapide (calculette juste pour la fin…)

   Réponse

i	**8**	**4**	**2**	**1**	**12**
Bits de 12	1	1	0	0	
2^i[7991]	256	16	4	2	4096

4) Calculer (Euclide, calculette ou tableur) pgcd($a^{ppcm(1,2,3,4)}$ [7991]-1, 7991)

   Réponse : 7991=1*4095+3896, 4095=1*3896+199, 3896=19*199+115, 199=1*115+84, 115=1*84+31, 84=2*31+22 31=1*22+9, 22=2*9+4, 9=4*2+1 : le pgcd vaut 1, on n'a pas trouvé de facteur.

5) Recommencer avec B=5 en gardant a=2 (calculette indispensable ce coup-ci…) et expliquer le résultat obtenu

Réponses : ppcm(1,2,3,4,5)=60

Réponse

i	**32**	**16**	**8**	**4**	**2**	**1**	**48**	**56**	**60**
Bits de 60	1	1	1	1	0	0			
2^i[7991]	4571	1608	256	16	4	2	6439	2238	3844

7991=2*3843+305, 3843=12*305+183, 305=183+122, 183=122+61, 122=2*61 : victoire ! N est bien divisible par 61 : 7991=61*131

Explication 60=3*4*5 est bien 5 supersmooth par contre 130=2*5*13 est 13 supersmooth…

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 ?

Correction

90	109
91	290
92	473
93	658
94	845
95	1034
96	1225

$1225=35^2$

Donc $96^2-7991=35^2$

Donc 7991=(96-35)(96+35)=61*131… Mais encore faut il le voir…