MT10

Mathématiques pour la cryptographie

Partie 4

Factorisation : algorithme du crible quadratique[1]

Walter SCHÖN

1 : Source pour ce cours : Carl Pomerance « A Tale of Two Sieves »
Notices of the American Mathematical Society, December 1996

Introduction

- L'algorithme p-1 Pollard fonctionne dans les cas où le degré de superfriabilité du p-1 d'un des deux facteurs est suffisamment petit ce qui constitue une propriété particulière.
- A contrario connaissant l'attaque, on peut s'arranger pour qu'aucun des facteurs n'ait cette faiblesse.
- Il est donc bon d'avoir un algorithme qui ne dépende que de la taille des facteurs et non de propriétés particulières.
- L'algorithme du crible quadratique est à ce jour le meilleur pour factoriser des entiers jusqu'à un peu plus d'une centaine de digits.
- Pour des tailles plus grande il est devancé par l'algorithme du crible généralisé sur corps de nombres, très compliqué (et dont malgré tout les idées générales restent semblables à celles du crible quadratique).
- Ce cours contient une description détaillée du crible quadratique, avec exemples complets.

Introduction : méthode de Fermat

- Exemple : soit à factoriser N=8051
- Dans ce cas on peut remarquer que $8051=8100-49=90^2-7^2$
- Il s'ensuit que $8051=(90+7)(90-7)=97*83$
- Cet algorithme, qui fonctionne quand le nombre a deux facteurs voisins de sa racine carrée, est le suivant :
  - ✓ Pour les entiers x à partir du premier entier supérieur à la racine de N (ici 90)
  - ✓ Calculer les valeurs successives de x^2-N et espérer tomber sur un carré y^2 (ici dès le premier coup on tombe sur 49)
  - ✓ Dès que c'est le cas on a la factorisation $N=(x-y)(x+y)$
- Question : cet algorithme fonctionne-t-il dans tous les cas ?

Introduction : méthode de Fermat

- Réponse : Oui pour tout entier composite impair (seul cas d'intérêt pratique)
- En effet si N=a.b est un entier composite impair, a et b sont donc tous deux impairs.
- Par conséquent, l'identité $a.b = \left(\frac{1}{2}(a+b)\right)^2 - \left(\frac{1}{2}(a-b)\right)^2$

  montre que N peut bien être mis sous la forme de la différence des carrés de deux entiers.
- Mais dès lors que les facteurs a et b ne sont plus très proches de la racine de l'entier à factoriser, la méthode de Fermat est bien pire que la méthode d'essais de divisions en force brute qui nécessite de l'ordre de $\sqrt{N}$ divisions

Amélioration : méthode de Kraitchik (1920)

- L'idée consiste à rechercher non pas une différence de carrés égale à N, mais égale à un multiple de N.
- En effet si N divise x^2-y^2 pour deux entiers x et y
  - ✓ Soit N divise (x-y) ou (x+y) et nous sommes dans un cas « inintéressant » (il faut alors chercher une autre congruence du même type),
  - ✓ Soit N ne divise ni (x-y) ni (x+y) donc les facteurs de N se répartissent entre (x-y) et (x+y) et par conséquent pgcd(x-y,N) fournit un facteur non trivial de N (ainsi d'ailleurs que pgcd(x+y,N)).
- Or de telles congruences « intéressantes » existent, mais comment les trouver efficacement ?

Amélioration : méthode de Kraitchik (1920)

- Exemple : si on chercher à factoriser N=2041 par la méthode de Fermat.
- L'entier immédiatement supérieur à la racine de N est 46, et on obtient donc la suite :

x	x^2-N
46	75
47	168
48	263
49	360
50	459
51	560

Aucun carré identifié : la méthode de Fermat ne fonctionne pas…

Amélioration : méthode de Kraitchik (1920)

- Mais au lieu de rechercher un x pour lequel x^2-N est un carré, Kraitchik propose de rechercher un ensemble de x pour lesquels le produit des x^2-N est un carré Y^2.
- Pour cela il remarque que dans certains cas, x^2-N (beaucoup plus petit que N car x est voisin de la racine de N) se factorise facilement avec de petits facteurs premiers :

x	x^2-N	Factorisation
46	75	$3*5^2$
47	168	2^3*3*7
48	263	(263)
49	360	2^3*3^2*5
50	459	(3^3*17)
51	560	2^4*5*7

Amélioration : méthode de Kraitchik (1920)

- Si l'on tient un ensemble de x pour lesquels le produit des x^2-N est un carré Y^2 alors le produit des x^2 (noté par la suite X^2) est congru à Y^2 modulo N donc X^2-Y^2 est divisible par N. Si l'on est dans un cas « intéressant » pgcd(X-Y,N) fournit donc un facteur !
- Or dans notre exemple un « miracle » s'est produit : on a bien réussi à trouver un carré en assemblant quatre « morceaux ».

x	x^2-N	Factorisation
46	75	$3*5^2$
47	168	2^3*3*7
48	263	(263)
49	360	2^3*3^2*5
50	459	(3^3*17)
51	560	2^4*5*7

$(3*5^2)*(2^3*3*7)*$
$(2^3*3^2*5)*(2^4*5*7)=$
$2^{10}*3^4*5^4*7^2=(2^5*3^2*5^2*7)^2$

Par conséquent N=2041 divise
$(46*47*49*51)^2 - (2^5*3^2*5^2*7)^2$

Avec un peu de chance on est dans un cas « intéressant » et on a un diviseur !

Amélioration : méthode de Kraitchik (1920)

- En effet notant X=46*47*49*51 et Y=2^5*3^2*5^2*7
- X mod 2041=311 et Y mod 2041 =1416 donc
  X-Y mod 2041=311-1416=-1105=936 et X+Y mod 2041=1727
- Par conséquent ni X-Y ni X+Y n'est divisible par N donc on est bien dans un cas intéressant !
- Effectivement pgcd(X-Y,N)=pgcd(936,2041) ou
  pgcd(Y-X,N)=pgcd(1105;2041) donne le facteur 13
- On peut maintenant diviser N par 13 ou calculer
  pgcd(X+Y,N)=pgcd(1727,2041) qui vaut 157
- Finalement 2041=13*157 (dans cet exemple les essais de divisions auraient été plus rapides, mais cela donne les idées générales…)
- Dès lors : existe-t-il une méthode pour trouver un carré autrement que par « miracle » ?

Méthode systématique de recherche de carrés

- C'est à M. A. Morrison and J. Brillhart en 1975 que l'on doit une méthode systématique, qui (bizarrement) n'utilise que de l'algèbre linéaire tout à fait élémentaire !
- En effet tout entier positif peut s'exprimer sous la forme d'un « vecteur d'exposants » donnant les puissances de sa décomposition (unique d'après le théorème fondamental de l'arithmétique) sur les différents nombres premiers.
- Ainsi les nombres d'un degré de friabilité (« smooth ») inférieur ou égal à B peuvent s'exprimer dans une « base de facteurs » constituée des nombres premiers inférieurs ou égaux à B.
- Dans notre exemple, les 4 nombres 7-smooth sont représentés par :

$75=3*5^2$: (0,1,2,0) $168=2^3*3*7$: (3,1,0,1)

$360=2^3*3^2*5$: (3,2,1,0) $560=2^4*5*7$: (4,0,1,1)

Méthode systématique de recherche de carrés

- Maintenant comme le vecteur d'exposants d'un produit de nombres est la somme des vecteurs d'exposants de ces nombres, trouver un carré revient à trouver une somme de vecteurs dont toutes les composantes sont paires !
- En d'autres termes il suffit de conserver les modulo 2 des composantes des vecteurs d'exposants et à chercher un ensemble de vecteurs de somme (modulo 2) nulle !
- Dans notre exemple :
  $75=3*5^2$: (0,1,0,0) $168=2^3*3*7$: (1,1,0,1)
  $360=2^3*3^2*5$: (1,0,1,0) $560=2^4*5*7$: (0,0,1,1)
- Et l'on voit bien que (addition dans Z/2Z) :
  (0,1,0,0)+(1,1,0,1)+(1,0,1,0)+(0,0,1,1)=(0,0,0,0)

Méthode systématique de recherche de carrés

- Plus formellement, nous avons ici 4 vecteurs de $(Z/2Z)^4$ et nous cherchons s'il existe 4 coefficients x_i de Z/2Z non tous nuls tels que :
- $x_1.(0,1,0,0)+x_2.(1,1,0,1)+x_3.(1,0,1,0)+x_4.(0,0,1,1)=(0,0,0,0)$
- En d'autres termes les vecteurs doivent être liés ce qui ici n'est pas garanti (4 vecteurs en dimension 4 peuvent être indépendants).
- Cette relation peut être mise sous forme matricielle (noter la transposition) :

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Méthode systématique de recherche de carrés

- Pour résoudre ce genre de système on cherche à mettre la matrice sous forme triangulaire (méthode de Gauss) en utilisant :
  - Permutation des lignes (=permutation d'équations)
  - Combinaison linéaire (ici somme) de deux lignes (somme d'équations)

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \xrightarrow{L1<->L2} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \xrightarrow{L4=L4+L2} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

$$\xrightarrow{L4=L4+L3} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

La matrice est donc de rang 3 (4ème équation triviale) et les solutions sont tous les vecteurs tels que $x_1=x_2$ et $x_2=x_3$ et $x_3=x_4$ soit (0,0,0,0) solution triviale et (1,1,1,1)

Méthode systématique de recherche de carrés

- Pour systématiser la procédure, il suffit de :
  - ✓ Se fixer un seuil de friabilité (revient à limiter la base aux K premiers nombres premiers pour un certain K),
  - ✓ Explorer les x^2-N à partir de l'entier immédiatement supérieur à $\sqrt{N}$ à la recherche d'entiers factorisables sur cette base (étape très coûteuse qui sera l'objet du « crible » cf. plus loin)
  - ✓ Dès qu'on en a trouvé K+1 on a par conséquent K+1 vecteurs de l'espace vectoriel $(Z/2Z)^K$ (de dimension K), et qui sont donc linéairement dépendants,
  - ✓ Il existe donc au moins une combinaison linéaire nulle, et (les scalaires étant réduits à 0 et 1) donc une somme de vecteurs nulle.
  - ✓ Reste à vérifier si l'on est dans un cas « intéressant » ou non

Noter que dans l'exemple nous avons eu un peu de chance : pour être sûr d'avoir une combinaison (en dimension 4) il fallait 5 vecteurs, 4 ont suffi.

Extension aux nombres négatifs

- On peut aussi inclure les nombres négatifs en explorant les x^2-N inférieurs à $\sqrt{N}$
- Pour cela il suffit de rajouter le nombre -1 dans la base de facteurs (qui doit donc aussi être à une puissance paire pour avoir un carré)

x	x^2-N	Factorisation
45	-16	$(-1)*2^4$
44	-105	$(-1)*3*5*7$
43	-192	$(-1)*2^6*3$
42	-277	$(-1)*277$
41	-360	$(-1)*(2^3*3^2*5)$
40	-441	$(-1)*3^2*7^2$

Certes cela augmente de 1 la dimension de l'espace vectoriel mais cela peut être rentable en fournissant beaucoup d'autres nombres

Exemple de résolution complète

- Cela donne finalement 9 relations dans un espace de dimension 5 (base : -1, 2, 3, 5, 7) :

x	x^2-N	Factorisation	Vecteur
51	560	2^4*5*7	(0,0,0,1,1)
49	360	2^3*3^2*5	(0,1,0,1,0)
47	168	2^3*3*7	(0,1,1,0,1)
46	75	$3*5^2$	(0,0,1,0,0)
45	-16	$(-1)*2^4$	(1,0,0,0,0)
44	-105	(-1)*3*5*7	(1,0,1,1,1)
43	-192	$(-1)*2^6*3$	(1,0,1,0,0)
41	-360	$(-1)*(2^3*3^2*5)$	(1,1,0,1,0)
40	-441	$(-1)*3^2*7^2$	(1,0,0,1,0)

Exemple de résolution complète

- Cet ensemble de vecteurs nous donne donc une fois transposé la matrice suivante :

Vecteur
(0,0,0,1,1)
(0,1,0,1,0)
(0,1,1,0,1)
(0,0,1,0,0)
(1,0,0,0,0)
(1,0,1,1,1)
(1,0,1,0,0)
(1,1,0,1,0)
(1,0,0,1,0)

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Exemple de résolution complète

- L'échelonnement de la matrice en utilisant les deux opérations ci-dessous produit le résultat suivant :

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

L1<->L4

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

L5:=L5+L1+L2

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Exemple de résolution complète

Le système à résoudre est donc :

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Ce qui conduit à :

$x_9=0$ $\quad x_5=x_6+x_7+x_8$

$x_3=x_4+x_6+x_7$ $\quad x_2=x_4+x_6+x_7+x_8$

$x_1=x_4+x_7$

Où : x_4, x_6, x_7, x_8 peuvent prendre toutes les valeurs possibles soit 0 ou 1 (16 solutions)

Exemple de résolution complète

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
0	0	0	0	0	0	0	0
0	1	0	0	1	0	0	1
1	1	1	0	1	0	1	0
1	0	1	0	0	0	1	1
0	1	1	0	1	1	0	0
0	0	1	0	0	1	0	1
1	0	0	0	0	1	1	0
1	1	0	0	1	1	1	1
1	1	1	1	0	0	0	0
1	0	1	1	1	0	0	1
0	0	0	1	1	0	1	0
0	1	0	1	0	0	1	1
1	0	0	1	1	1	0	0
1	1	0	1	0	1	0	1
0	1	1	1	0	1	1	0
0	0	1	1	1	1	1	1

Liste des 16 jeux de valeurs possibles (en rouge : valeurs libres (table de vérité de toutes les valeurs possibles) en bleu : valeurs liées calculées par les équations obtenus grâce à la résolution précédente :

$$x_1 = x_4 + x_7$$

$$x_2 = x_4 + x_6 + x_7 + x_8$$

$$x_3 = x_4 + x_6 + x_7$$

$$x_5 = x_6 + x_7 + x_8$$

$$x_9 = 0$$

Exemple de résolution complète

On vérifie que l'on obtient bien des carrés et on reporte les valeurs de X et Y :

	x	x^2-N
1	51	2^4*5*7
2	49	2^3*3^2*5
3	47	2^3*3*7
4	46	$3*5^2$
5	45	$(-1)*2^4$
6	44	$(-1)*3*5*7$
7	43	$(-1)*2^6*3$
8	41	$(-1)*(2^3*3^2*5)$
9	40	$(-1)*3^2*7^2$

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	X	Y
0	0	0	0	0	0	0	0	0	0
0	1	0	0	1	0	0	1	49*45*41	2^5*3^2*5
1	1	1	0	1	0	1	0	51*49*47*45*43	$2^{10}*3^2*5*7$
1	0	1	0	0	0	1	1	51*47*43*41	2^8*3^2*5*7
0	1	1	0	1	1	0	0	49*47*45*44	2^5*3^2*5*7
0	0	1	0	0	1	0	1	47*44*41	2^3*3^2*5*7
1	0	0	0	0	1	1	0	51*44*43	$2^5*3*5*7$
1	1	0	0	1	1	1	1	51*49*45*44*43*41	$2^{10}*3^3*5^2*7$
1	1	1	1	0	0	0	0	51*49*47*46	$2^5*3^2*5^2*7$
1	0	1	1	1	0	0	1	51*47*46*45*41	$2^7*3^2*5^2*7$
0	0	0	1	1	0	1	0	46*45*43	2^5*3*5
0	1	0	1	0	0	1	1	49*46*43*41	$2^6*3^3*5^2$
1	0	0	1	1	1	0	0	51*46*45*44	2^4*3*5^2*7
1	1	0	1	0	1	0	1	51*49*46*44*41	$2^5*3^3*5^3*7$
0	1	1	1	0	1	1	0	49*47*46*44*43	$2^6*3^3*5^2*7$
0	0	1	1	1	1	1	1	47*46*45*44*43*41	$2^8*3^3*5^2*7$

Exemple de résolution complète

Il ne reste plus qu'à parcourir les solutions, à la recherche d'un cas « intéressant » (en testant la divisibilité de X+Y et X-Y par N), ici 8 cas sur 15 (d'une manière générale environ la moitié des cas sont « intéressants »

X mod N	Y mod N	X-Y mod N	X+Y mod N	pgcd(X-Y,N)	pgcd(X+Y,N)
601	1440	1202	0		
82	82	0	164		
1041	1041	0	41		
346	1916	471	221	157	13
1107	479	628	1586	157	13
565	1319	1287	1884	13	157
759	1230	1570	1989	157	13
311	1416	936	1727	13	157
797	1582	1256	338	157	13
1247	480	767	1727	13	157
2016	339	1677	314	13	157
1805	236	1569	0		
1211	830	381	0		
332	332	0	664		
713	1328	1426	0		

Restriction de la base de facteurs

- Certains facteurs premiers peuvent être exclus car ne peuvent pas diviser x^2-N
- En effet si p divise x^2-N, on a $x^2=N+k.p$ (k entier), donc N est un carré (on dit aussi résidu quadratique) modulo p
- Or certains nombres ne sont pas des carrés modulo p, donc si N est dans ce cas, on peut exclure p de la base des facteurs.
- Exemples :
  - ✓ Dans Z/2Z : tous les éléments (0 et 1) sont des carrés
  - ✓ Dans Z/3Z : 0 et 1 sont des carrés mais 2 ne l'est pas (2*2=1)
  - ✓ Dans Z/5Z : les carrés sont 0, 1, 4 mais 2 et 3 ne le sont pas
  - ✓ Dans Z/7Z : les carrés sont 0, 1, 2, 4 mais 3, 5 et 6 ne le sont pas
  - ✓ Dans Z/11Z : les carrés sont 0, 1, 3, 4, 5, 9 mais 2, 6, 7, 8, 10 ne le sont pas
- ✓ Dans Z/pZ pour p>2 (donc impair) outre 0 (qui est un carré) il y a (p-1)/2 carrés non nuls et (p-1)/2 non carrés (voir ci-après)

Résidus quadratiques et symbole de Legendre

- En effet, pour p premier différent de 2 :
  - ✓ (p-1)/2 est donc entier
  - ✓ Z/pZ est un corps son sous groupe multiplicatif est d'ordre p-1 (donc pour tout a du groupe $a^{p-1}=1$: théorème de Fermat)
  - ✓ Par conséquent $a^{(p-1)/2} = \pm 1$
  - ✓ Ce sous-groupe est cyclique on peut en trouver au moins un générateur, soit g l'un quelconque d'entre eux,
  - ✓ Tout élément a non nul de Z/pZ peut donc se mettre sous la forme $a=g^k$ où k ($0 \leq k \leq p-2$) est appelé logarithme à base g de x (nombre modulo p-1 car $g^{p-1}=1$ comme pour tout élément)
  - ✓ Si a est le carré d'un élément b de logarithme j, alors $a=(g^j)^2=g^{2j}$ le logarithme de a qui vaut 2j modulo p-1 est donc pair car p-1 est pair

Résidus quadratiques et symbole de Legendre

- Réciproquement si le logarithme k de a est pair (soit k=2t) alors $a=g^{2t}=(g^t)^2$ et est donc bien un carré
- Un élément non nul de Z/pZ est donc un carré si et seulement si son logarithme (a base n'importe quel générateur de $(Z/pZ)^*$) est pair.
- La moitié des p-1 logarithmes possibles entre 0 et p-2 est pair
- Les carrés non nuls de Z/pZ sont donc exactement les (p-1)/2 éléments g^k pour k valant 0, 2… p-3
- Les p-1 autres éléments sont donc des non carrés
- Remarque : les générateurs sont donc forcément des non carrés. La réciproque et fausse.
  - Exemple dans Z/7Z : 6 est un non carré (les carrés sont 1, 2 (3^2) et 4) et son groupe cyclique est : 6->1 (ordre 2 qui divise 6), donc c'est un non carré non générateur (seul exemple dans ce cas car 3 et 5 sont générateurs)

Résidus quadratiques et symbole de Legendre

- Maintenant si un élément a est un carré donc de logarithme k=2t $a^{(p-1)/2}=(g^{2t})^{(p-1)/2}=g^{p-1}=1$
- Réciproquement si un élément a de logarithme k est tel que $a^{(p-1)/2}=1$ alors $(g^k)^{(p-1)/2}=g^{k(p-1)/2}=1$ donc k(p-1)/2 est congru à 0 modulo p-1 donc k est pair donc a est un carré
- Un élément non nul de Z/pZ est donc un carré si et seulement si $a^{(p-1)/2}=1$
- Il en résulte que pour les non carrés $a^{(p-1)/2}=-1$ (seule autre valeur possible).

Résidus quadratiques et symbole de Legendre

- Conclusion : soit p un nombre premier impair, et a un entier :
- Notant $\left(\frac{a}{p}\right)$ (symbole de Legendre) la quantité $a^{(p-1)/2} \bmod p$

(signifiant : « a est il un carré modulo p ?», le contexte permet d'éviter de le confondre avec une simple fraction).

- $\left(\frac{a}{p}\right)$ vaut :

  - 1 si a est un carré non nul modulo p
  - -1 si a n'est pas un carré modulo p
  - 0 si a est multiple de p (donc 0 modulo p)

Pour p=2 tout nombre pair est 0^2 modulo p et tout nombre impair 1^2 modulo p

Restriction de la base des facteurs : conclusion

- Pour déterminer la base des facteurs, par conséquent :
  - ✓ On se fixe un seuil de friabilité
  - ✓ Pour tous les nombres premiers p impairs inférieurs à ce seuil, on calcule le symbole de Legendre $N^{(p-1)/2}$ mod p (calculé comme : $(N \bmod p)^{(p-1)/2}$ mod p avec l'exponentiation rapide).
  - ✓ S'il vaut 1 retenir le facteur, s'il vaut -1 l'écarter car N n'est pas un carré modulo p donc aucun x^2-N ne peut être divisible par p (s'il vaut 0 on a trouvé un facteur !).
  - ✓ Dans notre exemple : 2041 mod 3=1, 2041 mod 5=1, 2041 mod 7=4 et 4^3 mod 7 =1 donc 3, 5, 7 (ainsi que 2) peuvent être des facteurs. Par contre 2041 mod 11=6 et 6^5 mod 11 =-1, par conséquent 11 devrait être écarté de la base des facteurs si on avait pris un seuil de friabilité >7. Quant à 13…

Identification des nombres friables par criblage

- C'est à Carl Pomerance en 1981 que l'on doit une amélioration décisive simplifiant la coûteuse phase d'identification des nombres friables.
- L'idée repose sur une généralisation du crible d'Erathostène pour l'identification des x^2-N friables sur la base des facteurs.
- Les x^2-N étant scannés pour x autour de la racine du nombre N à factoriser, comment trouver ceux qui sont factorisables sur la base des facteurs (et dans ce cas la factorisation associées) sans procéder à des essais de division par les facteurs ?

x	40	41	42	43	44	45	46	47	48	49	50	51
x^2-N	-441	-360	-277	-192	-105	-16	75	168	263	360	459	560

Identification des nombres friables par criblage

- Etant donné un facteur p de la base, si x^2-N est divisible par p, alors x est congru modulo p à une racine de N dans Z/pZ (dont on sait qu'elle existe car sinon p ne serait pas dans la base).
- Or il existe des algorithmes efficaces de calculs de racines carrées (Shanks-Tonelli, mais ceci est un autre sujet) : soit r et -r les deux racines carrées de N modulo p (distinctes sauf si p=2)
- Les x^2-N divisibles par p sont ceux dont les x sont des représentants de la classe d'équivalence de ces deux racines dans la congruence modulo p, qu'il est facile de « cribler » dans tout le tableau.

x	40	41	42	43	44	45	46	47	48	49	50	51
x^2-N	-441	-360	-277	-192	-105	-16	75	168	263	360	459	560

Identification des nombres friables par criblage

- Pour notre exemple (N=2041) : pour p=2, N modulo p vaut 1 l'unique racine est donc 1 et les x^2-N divisibles par 2 sont ceux qui correspondent à des x impairs.
- Pour p=3, N modulo p vaut 1 donc les racines sont 1 et -1 et les x^2-N divisibles par 3 sont ceux qui correspondent à des x non divisibles par 3.
- Pour p=5, N modulo p vaut 1 donc les racines sont 1 et -1 et les x^2-N divisibles par 5 sont ceux qui correspondent à des x congrus à 1 ou 4 modulo 5.
- Pour p=7, N modulo p vaut 4 dont les racines sont 2 et -2 les x^2-N divisibles par 7 sont ceux qui correspondent à des x congrus à 2 ou 5 modulo 7
- (Le facteur -1 de x^2-N qui a son importance est également identifié)

x	40	41	42	43	44	45	46	47	48	49	50	51
x^2-N	-441	-360	-277	-192	-105	-16	75	168	263	360	459	560
Facteur -1	X	X	X	X	X	X						
Facteur 2		X		X		X		X		X		X
Facteur 3	X	X		X	X		X	X		X	X	
Facteur 5		X			X		X			X		X
Facteur 7	X				X			X				X

Identification des nombres friables par criblage

- Maintenant au lieu de bêtement se borner à cribler, Pomerance propose :
  - ✓ Pour tout p de la base
    - Pour tout élément dont le x^2-N identifié comme divisible par p
    - Diviser x^2-N par la plus grande puissance de p possible
    - garder cette puissance dans la coordonnée correspondante d'un vecteur associé à l'élément
  - ✓ Next p

x	40	41	42	43	44	45	46	47	48	49	50	51
x^2-N	-441	-360	-277	-192	-105	-16	75	168	263	360	459	560
x^2-N divis.	441	360	277	192	105	16	75	168	263	360	459	560
Facteur -1	1	1	1	1	1	1						

Identification des nombres friables par criblage

- Maintenant au lieu de bêtement se borner à cribler, Pomerance propose :
  - ✓ Pour tout p de la base
    - Pour tout élément dont le x^2-N identifié comme divisible par p
    - Diviser x^2-N par la plus grande puissance de p possible
    - Garder cette puissance dans la coordonnée correspondante d'un vecteur associé à l'élément
  - ✓ Next p

x	40	41	42	43	44	45	46	47	48	49	50	51
x^2-N	-441	-360	-277	-192	-105	-16	75	168	263	360	459	560
x^2-N divis.	441	45	277	3	105	1	75	21	263	45	459	35
Facteur -1	1	1	1	1	1	1						
Facteur 2		3		6		4		3		3		4

Identification des nombres friables par criblage

- Maintenant au lieu de bêtement se borner à cribler, Pomerance propose :
  - ✓ Pour tout p de la base
    - Pour tout élément dont le x^2-N identifié comme divisible par p
    - Diviser x^2-N par la plus grande puissance de p possible
    - garder cette puissance dans la coordonnée correspondante d'un vecteur associé à l'élément
  - ✓ Next p

x	40	41	42	43	44	45	46	47	48	49	50	51
x^2-N	-441	-360	-277	-192	-105	-16	75	168	263	360	459	560
x^2-N divis.	49	5	277	1	35	1	25	7	263	5	17	35
Facteur -1	1	1	1	1	1	1						
Facteur 2		3		6		4		3		3		4
Facteur 3	2	2		1	1		1	1		2	3	

Identification des nombres friables par criblage

- Maintenant au lieu de bêtement se borner à cribler, Pomerance propose :
  - ✓ Pour tout p de la base
    - Pour tout élément dont le x^2-N identifié comme divisible par p
    - Diviser x^2-N par la plus grande puissance de p possible
    - garder cette puissance dans la coordonnée correspondante d'un vecteur associé à l'élément
  - ✓ Next p

x	40	41	42	43	44	45	46	47	48	49	50	51
x^2-N	-441	-360	-277	-192	-105	-16	75	168	263	360	459	560
x^2-N divis.	49	1	277	1	7	1	1	7	263	1	17	7
Facteur -1	1	1	1	1	1	1						
Facteur 2		3		6		4		3		3		4
Facteur 3	2	2		1	1		1	1		2	3	
Facteur 5		1			1		2			1		1

Identification des nombres friables par criblage

- Maintenant au lieu de bêtement se borner à cribler, Pomerance propose :
  - ✓ Pour tout p de la base
    - Pour tout élément dont le x^2-N identifié comme divisible par p
    - Diviser x^2-N par la plus grande puissance de p possible
    - garder cette puissance dans la coordonnée correspondante d'un vecteur associé à l'élément
  - ✓ Next p

x	40	41	42	43	44	45	46	47	48	49	50	51
x^2-N	-441	-360	-277	-192	-105	-16	75	168	263	360	459	560
x^2-N divis.	1	1	277	1	1	1	1	1	263	1	17	1
Facteur -1	1	1	1	1	1	1						
Facteur 2		3		6		4		3		3		4
Facteur 3	2	2		1	1		1	1		2	3	
Facteur 5		1			1		2			1		1
Facteur 7	2				1			1				1

Identification des nombres friables par criblage

- Finalement tous les éléments pour lequel les x^2-N sont devenus 1 (9 dans l'exemple), ont été complètement factorisés sur la base des facteurs et la factorisation se lit directement dans le vecteur, dont il suffit de prendre le modulo 1 pour s'engager dans la phase d'algèbre linéaire décrite plus haut…

x	40	41	42	43	44	45	46	47	48	49	50	51
x^2-N	-441	-360	-277	-192	-105	-16	75	168	263	360	459	560
x^2-N divis.	1	1	277	1	1	1	1	1	263	1	17	1
Facteur -1	1	1	1	1	1	1						
Facteur 2		3		6		4		3		3		4
Facteur 3	2	2		1	1		1	1		2	3	
Facteur 5		1			1		2			1		1
Facteur 7	2				1			1				1

Récapitulatif : première étape

- Reprenons les différentes étapes en illustrant par un exemple plus conséquent : N=87463
- On commence par chercher la base des facteurs en calculant pour les premiers nombres premiers (>2)
  $(N \bmod p)^{(p-1)/2} \bmod p$ (symbole de Legendre). Pour l'exemple prenons les nombres premiers jusqu'à 29 :

p	3	5	7	11	13	17	19	23	29
N mod p	1	3	5	2	12	15	6	17	28
(p-1)/2	1	2	3	5	6	8	9	11	14
(N mod p)^(p-1)/2	1	9	125	32	2985984	2562890625	10077696	3,42719E+13	1,82059E+20
(N mod p)^(p-1)/2 mod p	1	4	6	10	1	1	1	#NOMBRE!	#NOMBRE!

- Même dans cet exemple simple, l'exponentiation rapide s'avère indispensable…

Récapitulatif : première étape

- Pour N=87463 , calculs de $(N \bmod p)^{(p-1)/2} \bmod p$ (symbole de Legendre) par l'exponentiation rapide pour les nombres premiers de 3 à 29 :

p	3	5	7	11	13	17	19	23	29
(p-1)/2	1	2	3	5	6	8	9	11	14
1 : N mod p	1	3	5	2	12	15	6	17	28
2 : (N mod p)^2 mod p	1	4	4	4	1	4	17	13	1
4 : ((N mod p)^2 mod p)^2 mod p	1	1	2	5	1	16	4	8	1
8 : (((N mod p)^2 mod p)^2 mod p)^2 mod p	1	1	4	3	1	1	16	18	1
(N mod p)^(p-1)/2	1	4	6	10	1	1	1	22	1
Ecriture binaire de (p-1)/2 :			(20 mod 7)				(96 mod 19)	(221 mod 23 =14) (252 mod 23=22)	

- Les nombres manipulés ne sont jamais beaucoup plus grands que p, et on trouve finalement la table des symboles de Legendre :

p	3	5	7	11	13	17	19	23	29
$N^{(p-1)/2} \bmod p$	1	-1	-1	-1	1	1	1	-1	1

- Comme -1 et 2 peuvent toujours être retenus comme facteurs (rappel : tout entier est un carré modulo 2), la base de facteurs retenue est donc : -1, 2, 3, 13, 17, 19, 29

Récapitulatif : deuxième étape

- N=87453, base de facteurs -1, 2, 3, 13, 17, 19, 29
- Deuxième étape : On cherche les racines de N modulo ces facteurs (sauf -1 évidemment), il y en a deux opposées (sauf si p=2 auquel cas elles sont égales).
- En pratique on cherche la racine de N modulo p (rappel : p est petit) problème pas facile mais il existe des algorithmes efficaces (Shanks-Tonelli). Dans l'exemple, la force brute suffit (et peut suffire dans des cas plus grands : les p sont petits et en nombre limité).

p	2	3	13	17	19	29
N modulo p	1	1	12	15	6	28
Racines de N modulo p	1	±1	±5 (25-13)	±7 (49-34)	±5 (25-19)	±12 (144-116)

Récapitulatif : troisième étape

p	2	3	13	17	19	29
Racines de N modulo p	1	±1	±5	±7	±5	±12

- Cribler en utilisant ces racines, sur un intervalle autour de l'entier immédiatement inférieur la racine de n (ici 295) : phase coûteuse nécessite une division par le facteur p pour trouver un représentant d'une racine de N modulo p dans l'intervalle (les autres se déduisent par simples « décalages »), puis pour chaque x^2-N identifié comme divisible autant de divisions que possible par p.

x	261	262	263	264	265	266	267	268	269	270	271	272	273	274
x^2-N	-19342	-18819	-18294	-17767	-17238	-16707	-16174	-15639	-15102	-14563	-14022	-13479	-12934	-12387
x^2-N divis.	-509	-41	-3049	-17767	-1	-5569	-8087	-401	-839	-14563	-41	-4493	-223	-4129
2	1		1		1		1		1		1		1	
3		3	1		1	1		1	2		2	1		1
13					2			1						
17		1			1									
19	1										1			
29													1	

x	275	276	277	278	279	280	281	282	283	284	285	286	287	288
x^2-N	-11838	-11287	-10734	-10179	-9622	-9063	-8502	-7939	-7374	-6807	-6238	-5667	-5094	-4519
x^2-N divis.	-1973	-11287	-1789	-1	-283	-53	-109	-467	-1229	-2269	-3119	-1889	-283	-4519
2	1		1		1		1		1		1		1	
3	1		1	3		2	1		1	1		1	2	
13				1			1							
17					1			1						
19						1								
29				1										

Récapitulatif : troisième étape

p					2	3	13	17	19	29				
Racines de N modulo p					1	±1	±5	±7	±5	±12				
x	289	290	291	292	293	294	295	296	297	298	299	300	301	302
x^2-N	-3942	-3363	-2782	-2199	-1614	-1027	-438	153	746	1341	1938	2537	3138	3741
x^2-N divis.	-73	-59	-107	-733	-269	-79	-73	1	373	149	1	2537	523	43
2	1		1		1		1		1		1		1	
3	3	1		1	1		1	2		2	1		1	1
13			1			1								
17								1			1			
19		1									1			
29														1

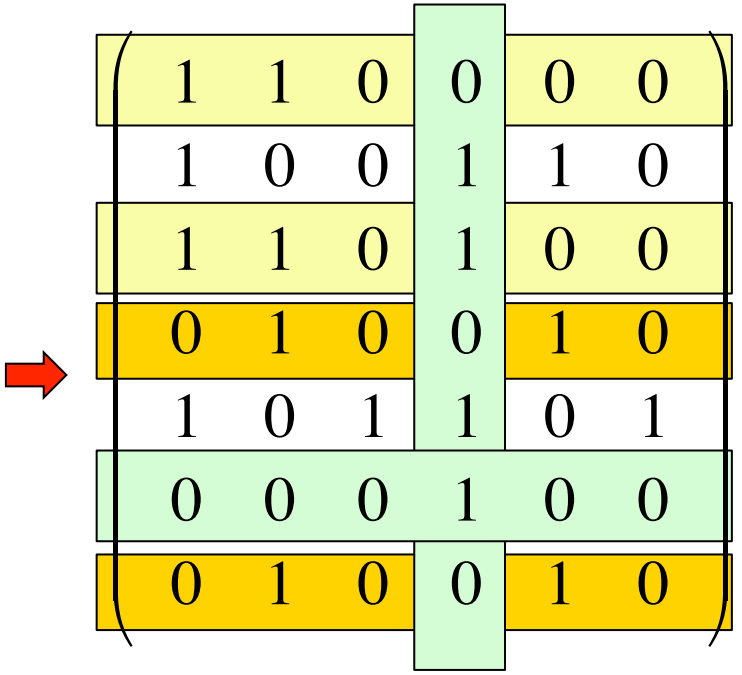
x	303	304	305	306	307	308	309	310	311	312	313	314	315	316
x^2-N	4346	4953	5562	6173	6786	7401	8018	8637	9258	9881	10506	11133	11762	12393
x^2-N divis.	2173	127	103	6173	1	2467	211	2879	1543	9881	103	1237	5881	1
2	1		1		1		1		1		1		1	
3		1	3		2	1		1	1		1	2		6
13		1			1									
17											1			1
19							1							
29					1									

x	317	318	319	320	321	322	323	324	325	326	327	328	329	330
x^2-N	13026	13661	14298	14937	15578	16221	16866	17513	18162	18813	19466	20121	20778	21437
x^2-N divis.	2171	719	2383	4979	7789	5407	937	17513	1009	6271	9733	353	3463	1261
2	1		1		1		1		1		1		1	
3	1		1	1		1	2		2	1		1	1	
13														
17														1
19		1										1		
29														

Récapitulatif : quatrième étape

- Bilan : 6 Nombres se factorisent complètement sur la base des facteurs choisie. Phase d'algèbre linéaire : espace vectoriel de dimension 7 avec 6 vecteurs, trouver une combinaison linéaire nulle avec coefficients non tous nuls n'est pas garanti, cela va dépendre du rang de la matrice…

x	265	278	296	299	307	316
x^2-N	-17238	-10179	153	1938	6786	12393
-1	1	1	0	0	0	0
2	1	0	0	1	1	0
3	1	3	2	1	2	6
13	2	1	0	0	1	0
17	1	0	1	1	0	1
19	0	0	0	1	0	0
29	0	1	0	0	1	0



De plus la 6ème équation imposant $x_4=0$, cette dimension (correspondant à x=299) peut être supprimée du problème, ainsi que la sixième équation (correspondant au facteur de base 19). On note alors que les équations 1 et 3 sont identiques et qu'on peut donc en supprimer une, idem pour la 4ème et la 7ème

Récapitulatif : quatrième étape

Finalement en supprimant une variable et 3 équations reste :

$$\left(\begin{array}{cccccc} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{array}\right) \Rightarrow \left(\begin{array}{ccccc} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{array}\right) \quad \left(\begin{array}{ccccc} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{array}\right)$$

La somme des trois premières étant triviale on peut en supprimer une : ⇨

Enfin remplaçant la troisième par la somme des trois :

$$\left(\begin{array}{ccccc} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{array}\right)$$

Ce qui donne la matrice échelonnée recherchée.

Récapitulatif : quatrième étape

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Pour rappel, le nombre x=299 ainsi que le facteur 19 n'ont plus lieu d'être donc la base est la suivante :

x	265	278	296	307	316
x^2-N	-17238	-10179	153	6786	12393
-1	1	1	0	0	0
2	1	0	0	1	0
3	1	3	2	2	6
13	2	1	0	1	0
17	1	0	1	0	1
29	0	1	0	1	0

Les solutions sont donc tous les quintuplets vérifiant $x_3=x_4+x_5$ et $x_1=x_2=x_4$ soit 4 possibilités seulement dont une triviale.

x_1	x_2	x_3	x_4	x_5	X	Y
0	0	0	0	0	0	0
0	0	1	0	1	296*316	3^4*17
1	1	1	1	0	265*278*296*307	2*3^4*13^2*17*29
1	1	0	1	1	265*278*307*316	2*3^6*13^2*17*29

Récapitulatif : dernière étape

N=87463

Il ne reste plus qu'à rechercher les cas « intéressants » ce qui nécessite le calcul de X-Y mod N et X+Y mod N, si aucun ne vaut 0, les pgcd donnent des facteurs non triviaux. Ici 2 cas sur 3 sont intéressants.

X mod N	Y mod N	X-Y mod N	X+Y mod N	pgcd(X-Y,N)	pgcd(X+Y,N)
6073	1377	4696	7450	587	149
34757	28052	6705	62809	149	587
9921	77542	19842	0		

87463=149*587

Deux facteurs premiers très loin d'être évidents

De plus le degré de superfriabilité le plus faible de p-1 est pour 148 avec un degré 37 (attaque par p-1 Pollard pas très aisée mais réalisable).