Auteur :

Sandou 1 Daffé

Affiliation :

Professeur de MERISE et Accès à l'université de Labé.

Titre: les noyaux des nombres entiers composés impairs.

Introduction :

Les nombres composés impairs sont tous les nombres impairs qui ne sont pas premiers ; Les nombres composés impairs comprennent 9, 15, 21, 25, 27 etc.

Soit f et p deux fonctions distinctes à valeur dans N ;

$\forall$ *n, i, k* $\in N$;

$\exists$ $k_1, K_2, K_3, \ldots, k_{n-1}, k_n \in N$ /

1- $p= 2k_1+1$; *est un nombre impair ;*

Exemple : p=3 est impair et non composé;

$3=2x1+1 \Rightarrow k_1=1;$

2- $f= (2k_1+1)(2k_2+1)(2k_3+1)\ldots\ldots (2k_{n-1}+1)(2k_n+1)$ *est un nombre impair composé;*

Exemple :

$f=9 \Rightarrow f=3x3$ *est donc composé impair;*

$9= (2x1+1)(2x1+1) \Rightarrow k_1=k_2=1$;

$f=27 \Rightarrow f=3x3x3$ *est donc composé impair;*

$27= (2x1+1)(2x1+1)(2x1+1) \Rightarrow k_1=k_2= k_3=1$;

Pour décomposer un nombre entier composé impair f en produit de facteurs premiers, cela reviens à trouver ses noyaux ;

Cette nouvelle méthode est composé d'un concept et d'un système d'équation dénommé système d'équation Sandou I Daffé (le SESID) dont la première équation est :

$f= (2k_1+1) (2k_2+1) (2k_3+1)\ldots\ldots (2k_{n-1}+1) (2k_n+1)$ (E_1) *qui est l'équation principale ;*

Tout revient donc à trouver les variables k_n *comme illustrer manuellement dans ces exemples :*

f=9;

$9= (2k_1+1) (2k_2+1)$ (E_1)

$2=k_1+k_2$ (E_2) $\Rightarrow k_1=k_2=1$ (E_2)

f=15;

$15= (2k_1+1) (2k_2+1)$ (E_1)

$3=k_1+k_2$ $\Rightarrow k_1=1, k_2=2$ (E_2)

f=27;

$27= (2k_1+1) (2k_2+1) (2k_3+1)$ (E_1)

$2=k_1+k_2$ (E_2)

$3=k_1+k_2+k_3$ $\Rightarrow k_1=1, k_2=1, k_3=1$ (E_3)

Concept :

1-Noyaux des nombres entiers composé impairs:

Le noyau d'un nombre entier impair f est la valeur entière qui correspond à la somme des $k_1, k_2, k_3, \ldots, k_{n-1}$ *et* k_n *d'une équation secondaire ; chaque nombre entier composé impair a au moins un noyau noté noy;*

Un nombre premier $p=2k_1+1$ *a un seul noyau* $noy =K_1$ *avec* $k_2 =0$ *; et un nombre composé impair a un nombre de noyaux égale au nombre d'équations secondaires ;*

2-Le SESID:

$\forall$ *noy,* $j \in N$ *;*

$\exists\ noy_1,\ noy_2,\ noy_3, \ldots\ldots\ldots, noy_{j-1}, noy_j \in N /$

$f= (2k_1+1)(2k_2+1)(2k_3+1)\ldots\ldots (2k_{n-1}+1)(2k_n+1)\ (E_1)$

$noy_1=k_1+k_2\ (E_2)$

$noy_2=k_1+k_2+k_3\ (E_3)$

-

-

$noy_{j-1}=k_1+k_2+k_3+\ldots\ldots\ldots\ldots\ldots+k_{n-1}\ (E_{n-1})$

$noy_j=k_1+k_2+k_3+\ldots\ldots\ldots\ldots\ldots+k_{n-1}+k_n\ (E_n)$

-Si un seul noyau existe alors le SESID reviens à :

$f= (2k_1+1)(2k_2+1)\ (E_1)$

$noy_1=k_1+k_2 \Rightarrow k_1 = noy_1 - k_2\ (E_2)$

$f= 4k_1k_2+2k_1+2k_2+1\ (E_1)$

$f= 4k_2(noy_1 - k_2)+2(noy_1 - k_2)+2k_2+1\ (E_1)$

$f= 4x\ noy_1\ k_2- 4k^2_2+2x\ noy_1+1\ (E_1)$ *équation Sandou I Daffé (ESID) est une équation de second dégrée;*

Si l'on connaît le noyau :

$f=(2k_1+1)(2k_2+1)\ E1$

$noy1= k_1+ k_2\ E2$

Exemple d'un pseudo composé

$9=(2k_1+1)(2k_2+1)\ E1$

$2= k_1+ k_2\ \ E2 \Rightarrow k_1=2- k_2$

$9=[2(2- k_2)+1](2k_2+1) \Rightarrow 9=(5-2k_2)(2k_2+1) \Rightarrow 9=10k_2 +5-4k^2_2-2k_2$

$4k^2_2 - 8k_2+4=0/4$

$k^2_2 - 2k_2+1=0$

Posons $k_2 = x$

$X^2-2x+1=0$

$\Delta=(-2)^2 - 4(1)(1) \Rightarrow \Delta=0$

$x1=x2= -(-2)/2(1) \Rightarrow x1=x2=1 \Rightarrow k_1= k_2 =1$

$9= [2(1)+1] [2(1)+1] \Rightarrow 9=3*3$

Exemple avec 15

$15=(2 k_1+1)(2 k_2 +1)$ E1

$3= k_1+ k_2$ E2 $\Rightarrow k_1=3- k_2$

$15=[2(3- k_2)+1](2 k_2 +1) \Rightarrow 15=(7-2 k_2)(2 k_2 +1) \Rightarrow 15=14 k_2 +7-4 k^2_2-2 k_2$

$4 k^2_2 - 12 k_2 +8=0/4$

$k^2_2 - 3 k_2 +2=0$

Posons $k_2 =x$

$X^2-3x+2=0$

$\Delta=(-3)^2 - 4(1)(2) \Rightarrow \Delta=1$

$x1= (3-1)/2 \Rightarrow x1=1$

$x2= (3+1)/2 \Rightarrow x2=2 \Rightarrow k_1=1; k_2 =2$

$15= [2(1)+1] [2(2)+1] \Rightarrow 15=3*5$

Si l'on ne connaît pas le noyau :

Le travail consistera de chercher le noyau comme illustrer dans cet exemple :

$9=2x4+1$

$9=2x3+3$

$9=2x2+5$ $\Rightarrow T=2$ *(valeur à chercher) correspondant au noyau de 9.*

$9=2x1+7$

-Si l'on note $T_j=noy_j$ on aura le SESID suivant :

$$\frac{f}{(2k3+1).....(2kn-1+1)(2kn+1)} = (2k_1+1)(2k_2+1)\ (E_1)$$

$f=2T_1+n_1 \quad (E_2)$

$f=2T_2+n_2 \quad (E_3)$

-

-

$f=2T_{j-1}+n_{j-1} \quad (E_{n-1})$

$f=2T_j+n_j \quad (E_n)$

Comme la résolution est séquentielle alors on commence par (E_1) et (E_2) :

$f= (2k_1+1)(2k_2+1)\ (E_1)$

$f=2T_1+n_1\ ;\ 2T_1=f-n_1 \Rightarrow 2(k_1+k_2)= f-n_1 \Rightarrow k_1= \frac{f-n1-2k2}{2} \quad (E_2)$

$f= 4k_1k_2+2k_1+2k_2+1;$

$f= 4k_2(\frac{f-n1-2k2}{2}) +2(\frac{f-n1-2k2}{2}) +2k_2+1\ (E_1)$

$4k^2_2 -2(f-n_1)\ k_2 + (n_1-1) =0\ (E_1)$ ou ESID ;

$a= 4;$

$b= -2(f-n_1);$

$c= (n_1-1);$

$\Delta=b^2-4ac$

Tout le problème revient à la recherche de n_j en parcourant dans l'ordre décroissant pour trouver cette valeur d'après ma remarque ;
De toute façon le mauvais sens de parcours de n nous ferra aboutir à $\Delta<0$;
Ces conditions sont donc nécessaires pour toutes solutions de (E_1) :

- $n_j \in [n_1\ 2]$;
- $\Delta \geq 0$;
- $K_1, k_2, k_3,..,k_n$, Racine(Δ) $\in N$

-D'après ma remarque, n_j correspondant à la première valeur de la Racine(Δ) $\in \mathbf{N}$ est une solution de (E_1) ssi K_1 et k_2 forme deux nombres premiers tels que $div_1(2k_1+1)=1$ et $div_1(2k_2+1)=1$;

Ensuite, $2k_1+1$ et $2k_2+1$ divise chacun f ;

-Par contre, il est une partie de solution de (E_1) ssi l'un des k forme un nombre premier $(2k_1+1)$ et l'autre un nombre composé $(2k_2+1)$ et de même chacun divise f ;

-Formule de recherche du noyau :

$f=2T_1+n_1 \Rightarrow T_1=\frac{f - n1}{2}$

$noy_1=T_1$;

-Recherche de n_1 :

-Méthode :

T=Troncature (Racine-carré(f))

Si les variables k des noyaux de f sont proches alors cette valeur est toujours exacte avec des conditions suivantes :

f=2q+1 ;

Si {q est pair} $\Rightarrow$ {T doit être aussi pair et soit T, T+2 ou T-2 correspond à n_j recherché} ; si T est impair $\Rightarrow$ T-1, T+1, T-3 sont les trois valeurs qui sont à vérifier ;

Si {q est impair} $\Rightarrow$ {T doit être aussi impair et soit T, T+2 ou T-2 correspond à n_j recherché} ; si T est pair $\Rightarrow$ T+1, T-1, T+3 sont les trois valeurs qui sont à vérifier ;

A noter que c'est la méthode la plus efficace d'après mes remarques et j'espère que l'expérience continue avec tous les lecteurs pour la recherche d'une méthode plus efficace sur cette question ;

Dans le cas ou les variables k des noyaux de f ne sont pas proches on doit donc procéder par décrémentation ou par décroissance pour des grandes valeurs dont le noyau serrait au dessus de n_1 ;

En fin de compte, on doit trouver n_1 en fonction de T d'où : $n_1=f-2T$

Exemple1 : f=9

-recherche de n:

T=Troncature (Racine-carré(9))

T=3 est impair

$9=2x4+1 \Rightarrow q=4$ est pair

$T=T-1 \Rightarrow T=3-1 \Rightarrow T=2$

$f=2T+n_1 \Rightarrow n_1=f-2T \Rightarrow n_1=9-2x2$

$n_1=5$

$9=(2k_1+1)(2k_2+1)\ (E_1)$

$f=(2k_1+1)(2k_2+1)\ (E_1)$

$f=2T_1+n_1$; $2T_1=f-n_1 \Rightarrow 2(k_1+k_2)=f-n_1 \Rightarrow k_1=\frac{f-n1-2k2}{2}$ (E_2)

$f=4k_1k_2+2k_1+2k_2+1$;

$f=4k_2(\frac{f-n1-2k2}{2})+2(\frac{f-n1-2k2}{2})+2k_2+1\ (E_1)$

$4k_2^2-2(f-n_1)k_2+(n_1-1)=0\ (E_1)$;

$a=4$;

$b=-2(f-n_1)$;

$c=(n_1-1)$;

$\Delta=b^2-4ac$;

$n_1=5$;

$b=-2(9-5) \Rightarrow b=-8$

$c=5-1 \Rightarrow c=4$

$\Delta=-8^2-4\ x\ 4\ x\ 4 \Rightarrow \Delta=64-64 \Rightarrow \Delta=0$

$$K'_2=K''_2=\frac{-b}{2a}$$

$$K'_2=K''_2=\frac{8}{8} \qquad K'_2=K''_2=1;$$

$k_1=\frac{f - n1 - 2k2}{2} \Rightarrow k_1=\frac{9 - 5 - 2(1)}{2}$

$k_1=k_1'=1 \Rightarrow f=(2x1+1)(2x1+1) \Rightarrow f=3x3$

-Si $(2k_1+1)$ et $(2k_2+1)$ sont tous composés càd $div_1(2k_1+1)\neq 1$ ou en algorithme le tes-Miller-Rabin$(2k_1+1)$=faux et $div_1(2k_2+1)\neq 1$ ou en algorithme le tes-Miller-Rabin$(2k_2+1)$=faux alors $\exists f_1, f_2, /$ $f_1=(2k_1+1)(2k_2+1)(E_{1.1})$ et $f_2=(2k_3+1)(2k_4+1)(E_{1.1})$;

Il y a donc plus de deux noyaux et il faut recommencer le calcul par le même cheminement que le précédant avec $\frac{f}{f2}=f_1$ *et avec* $\frac{f}{f1}=f_2$;

-Si un seul f_j est composé càd f_1 est composé alors le k de f_1 n'est pas une solution du SESID et seul $\frac{f}{f2}=f1$ *est résolue ; ainsi le k de f_2 déjà trouvé est aussi l'une des solutions du SESID ou f_2 est composé alors le k de f_2 n'est pas une solution du SESID et seul* $\frac{f}{f1}=f_2$ *est résolue ; ainsi le k de f_1 déjà trouvé est aussi l'une des solutions du SESID ;*

-Si $f_1=f_2$ alors seul une seule équation des deux est nécessaire à résoudre et $k_1=k_3$, et $k_2=k_4$;

Concept de div_i :

div_1: premier diviseur ; ex: div (12)={1, 2, 3, 4, 6, 12} $div_1(12)=\{2\}$ car 12 n'est pas un nombre premier et en plus 1 est l'élément neutre pour la multiplication et la division ; $div_2(12)=\{3\}$; $div_3(12)=\{4\}$;

Un autre exemple, cette foi-ci relative d'un nombre premier ;

div (5)= {1, 5} ; $div_1(5)=\{1\}$ et $div_2(5)=\{5\}$ car nous n'avons que ces deux valeurs ;

nbdiv : nombre de diviseur et permet de calculer le nombre de diviseur d'un nombre ;

Conclusion :

La solution proposée ici est une aubaine pour l'informatique, pour son évolution notamment dans les échanges de données ; elle reste tout de même ouverte aux autres solutions qui en combinant par exemple avec le test-MillerRabbin peut aller très loin dans la cryptographie.