PREMIERS PAS VERS UNE THÉORIE PARABOLIQUE DES NOMBRES

Yves PIRAT

Peut-on être mathématicien amateur? En astronomie, en botanique, en zoologie ... la contribution des amateurs est fort appréciée des professionnels. Mais les outils nécessaires à la résolution de problèmes mathématiques sont tellement sophistiqués qu'on ne voit pas comment pourrait exister un mathématicien amateur. Quelques rares domaines se prêtent mieux à l'amateurisme : on connaît LINDGREN, spécialiste des puzzles géométriques et employé des postes australiennes.

Mais n'est-il pas plaisant de redécouvrir des résultats peu connus. L'article qui suit retrouve *par une autre voie* une méthode de factorisation inventée par FERMAT. L'auteur, Monsieur Y. PIRAT, s'il a un bac mathélem depuis 1945 a eu une activité professionnelle qui l'a bien éloigné des mathématiques.

Peut-être est-ce ça l'amateurisme en mathématiques? Pouvoir enthousiasmer son entourage sur des sujets classiques mais peu répandus. Faute de participer directement au progrès de notre discipline c'est un moyen sûr d'encourager son développement.(N.D.L.R.)

Plusieurs passages de l'ouvrage de WARUSFEL, "*Les Nombres et leurs Mystères* ", m'avaient particulièrement intrigué, et celui-ci entre autres : "*Nous savons bien quelle est la règle qui permet de passer d'un carré n^2 au carré suivant $(n+1)^2$: les écarts entre deux carrés successifs sont en progression arithmétique. S'il y avait quelque chose de tel pour la recherche qui nous occupe (= les nombres premiers), nous serions très avancés dans cette théorie* ". Je dois avouer que je ne m'étais jamais penché sur les *mystères* que l'on rencontre à chaque pas lorsque l'on s'engage sur le chemin de cette recherche. D'ailleurs, j'ignorais même que les nombres premiers suscitaient encore tant de problèmes délicats. Et mon étonnement fut encore plus vif lorsque je lus que certains spécialistes semblaient admettre que le hasard avait présidé à la répartition des nombres premiers dans le champ des entiers!

Curieux de nature, je décidai de m'aventurer un moment dans ce domaine qui n'est pas le mien, et ce malgré la mise en garde de WARUSFEL, laquelle aurait dû refroidir mon enthousiasme : "*Les armes nécessaires pour apprendre quelque chose sur les nombres premiers sont de taille formidable* ". Certes, mais qui peut affirmer que toutes les ressources offertes par les armes modestes ont bien été épuisées?...

La première figure que je dessinai — un peu pour m'amuser d'ailleurs! — fut la bonne, mais ...je l'ignorais !...J'eus en effet l'idée de reporter les 150 premiers nombres impairs dans un système d'axes selon le procédé suivant :

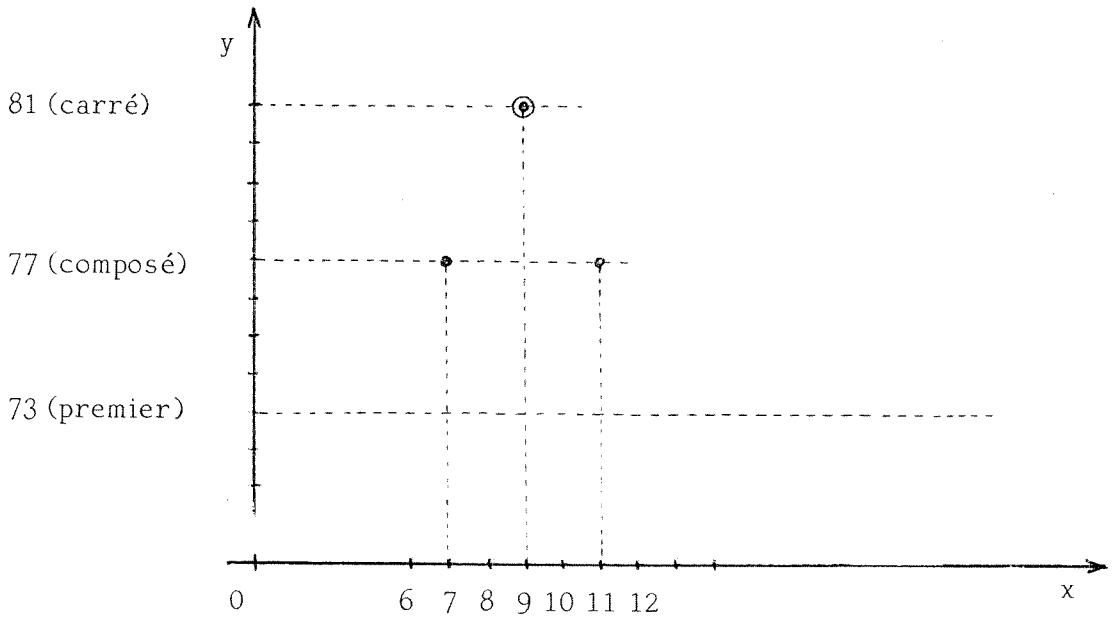


Figure 1

Immédiatement, j'eus l'impression qu'une famille nombreuse de paraboles s'emboîtait comme des poupées gigognes, chaque parabole ayant pour sommet un point matérialisant un carré. Quelques coups de crayon rouge confirmèrent l'exactitude de mon impression : il s'agissait bel et bien de paraboles, toutes identiques (voir *figure 2*).

Il ne fallut pas longtemps pour formuler leur équation, $Y = -X^2 + 2bX$, ou bien $Y = X(2b - X)$. Chaque sommet a pour coordonnées (b, b^2). En outre, si l'on respecte la condition $b \geq X$ (impair) ≥ 3, qui élimine les nombres pairs et les racines $X_1 = 1$ et $X_2 = N$, Y représente exclusivement *TOUS* les nombres entiers impairs *NON PREMIERS*.

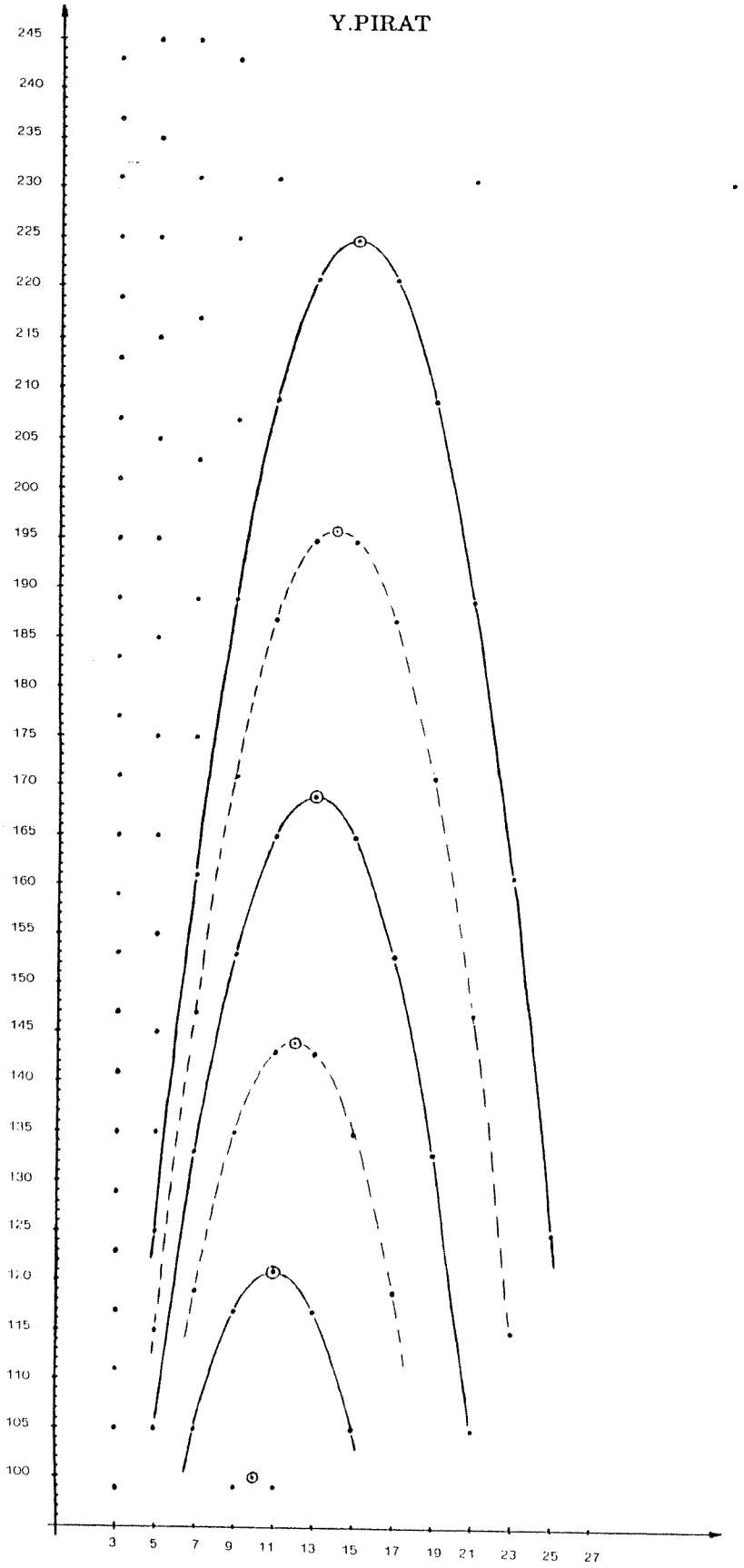
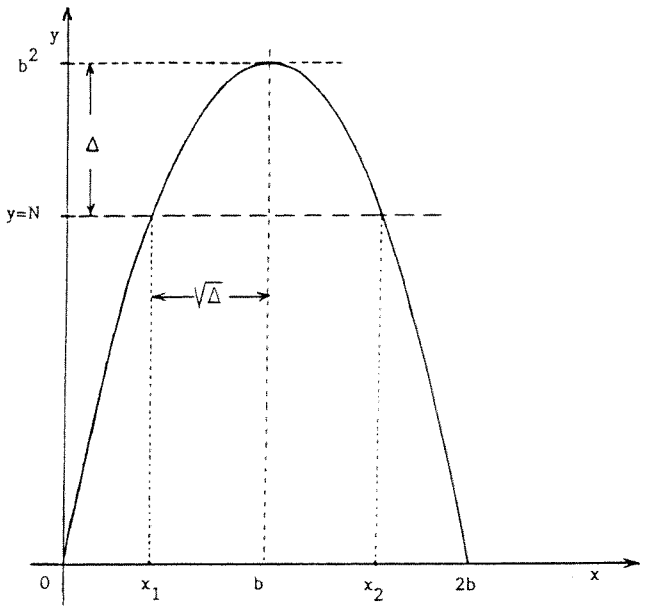

245
240
235
230
225
220
215
210
205
200
195
190
185
180
175
170
165
160
155
150
145
140
135
130
125
120
115
110
105
100
3
5
7
9
11
13
15
17
19
21
23
25
27

Figure 2

La *figure 3* montre l'agencement théorique de chaque parabole.



$$y(=N) = -x^2 + 2bx$$
$$N = b^2 - \Delta$$

Figure 3

Il est dès lors possible de classer, en fonction de la valeur de $\Delta(= b^2 - N)$, les trois catégories de nombres entiers impairs :

Si Δ est un carré, nous avons deux racines distinctes ($N = X_1 \times X_2 =$ nombre composé) ;

Si Δ est nul, nous avons une racine double ($X_1 = X_2$; N est donc un carré, sommet d'une parabole) ;

Si Δ n'est ni un carré, ni nul, pour toutes les valeurs possibles de b, il n'existe aucune racine entière, et N est premier.

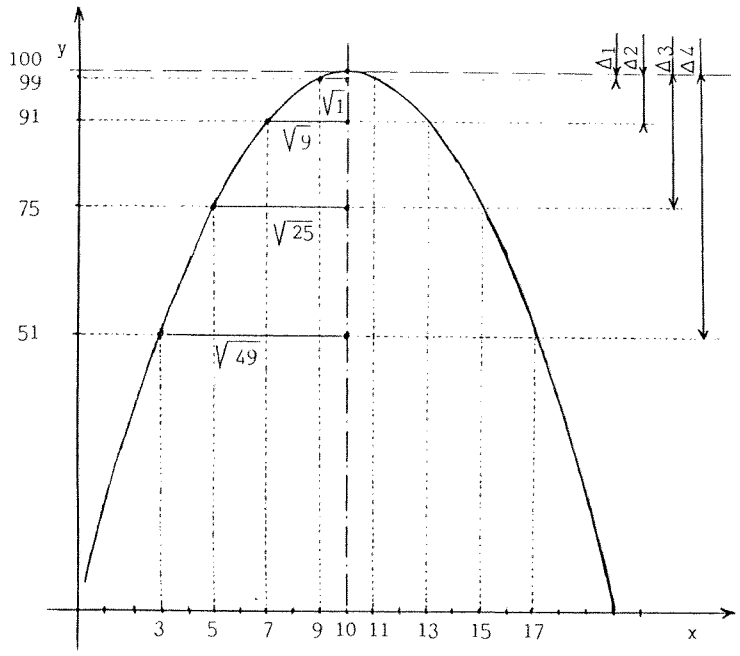
La *figure 1* donne un exemple pour chaque cas.

Comme on l'a facilement compris, chaque nombre non premier appartient à une ou plusieurs paraboles, et la différence entre le sommet et le nombre est égale à Δ, donc à un carré (naturellement, les N carrés sont exclus puisqu'ils sont sommets). Ainsi se trouve matérialisée la fameuse *différence de carrés* : $N = (A - B)(A + B) = A^2 - B^2$ (*Figure 4*).

Voyons brièvement l'exemple du nombre 105, choisi en raison du fait qu'il est susceptible de plusieurs factorisations (3×35, 5×21 et 7×15) et qu'il appartient conséquemment à 3 paraboles différentes dont les sommets sont respectivement

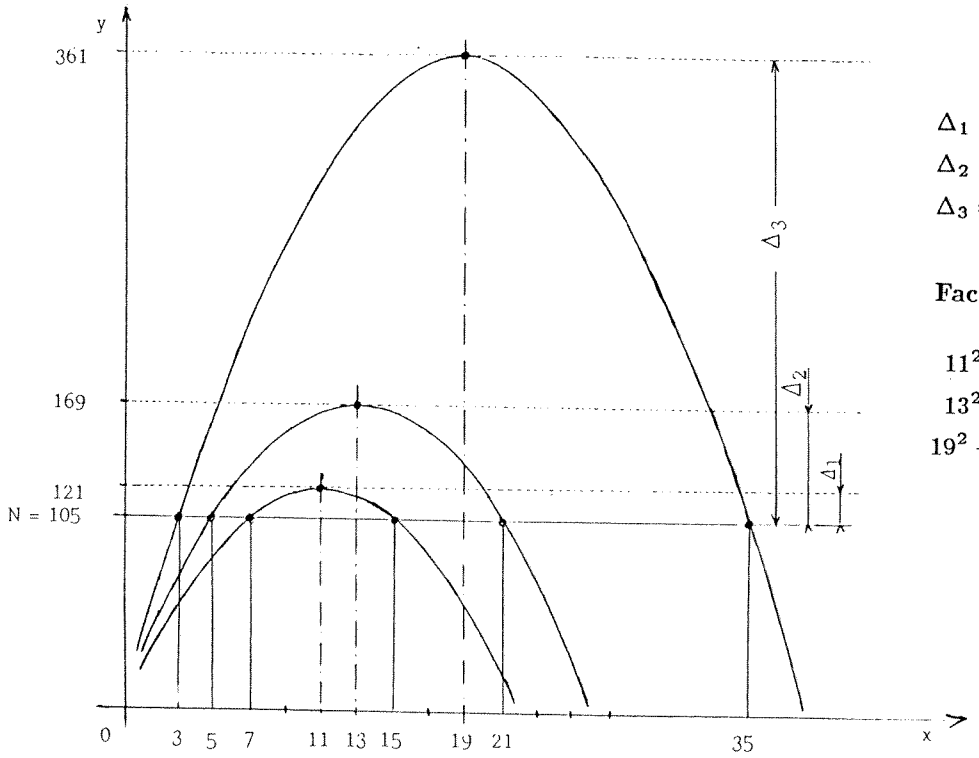
$$\frac{3+35}{2} = 19\,, \quad \frac{5+21}{2} = 13 \quad \text{et} \quad \frac{7+15}{2} = 11 \qquad (\textit{figure5}).$$

Jusqu'à présent, et à ma connaissance, personne n'a jamais réussi à *sortir* de la définition primaire du nombre premier, à savoir qu'il n'est divisible que par 1 et par lui-même.



$\Delta_1 = 1^2 = 1$
$\Delta_2 = 3^2 = 9$
$\Delta_3 = 5^2 = 25$
$\Delta_4 = 7^2 = 49$

Figure 4



$\Delta_1 = 121 - 105 = 16 \rightarrow 4^2$
$\Delta_2 = 169 - 105 = 64 \rightarrow 8^2$
$\Delta_3 = 361 - 105 = 256 \rightarrow 16^2$

Factorisation :

$11^2 - 4^2 = (11 + 4)(11 - 4) = 15 \times 7$
$13^2 - 8^2 = (13 + 8)(13 - 8) = 21 \times 5$
$19^2 - 16^2 = (19 + 16)(19 - 16) = 35 \times 3$

Figure 5

Puis-je me permettre de proposer de considérer désormais comme nombre premier tout nombre pour lequel l'équation $Y = -X^2 + 2bX$ n'admet aucune solution entière? Mon *tout petit niveau mathématique* me conduit peut-être à ne proposer qu'une ineptie, mais j'ai l'impression que cette façon de voir les nombres premiers fait plus sérieux que la *divisibilité* enseignée aux potaches!

Le problème qui se pose maintenant peut s'énoncer en ces termes : *Sachant que la différence entre le sommet d'une parabole P et un nombre composé NC, dont les facteurs sont des racines de P, est toujours un carré (= Δ), il suffit de rechercher si un nombre donné appartient ou non à une parabole pour en déduire son caractère, respectivement non-premier ou premier.*

Pour l'instant, précisons simplement que si l'on ajoute à N soit des carrés successifs (à partir de 1^2), soit les termes de la progression 1,3,5,7,..., et que l'on obtienne un carré à un moment donné, N n'est pas premier. Exemple :

$65527 + 1^2$ (pas carré), $65527 + 2^2$ (pas carré), $65527 + 3^2 = 65536$, carré de 256; donc 65527 n'est pas premier et ses facteurs sont $256 + 3$ et $256 - 3$; sa parabole a pour sommet la moitié de la somme de ses facteurs, soit 256 (confirmation); Δ égale $256^2 - 65527 = 3^2$.

65527+1 (pas carré), $65528 + 3$ (pas carré), $65531 + 5 = 65536$ (carré de 256).

Dans les deux cas le coût est strictement le même. En outre, il peut être très élevé si le carré le plus fort (sommet de la parabole) est très éloigné de N (cf. l'algorithme de FERMAT).

Deux questions se posent alors : Comment améliorer ce coût? Quelles sont les limites de la recherche?

LIMITES : Ajouter des carrés ou des termes de progression, c'est bien joli, mais, comme en toute chose, il faut savoir s'arrêter à temps! Les lecteurs — beaucoup plus compétents que moi! — n'ignorent pas qu'en matière de différence de carrés la limite est :

$$\left(\frac{N+1}{2}\right)^2 - \left(\frac{N-1}{2}\right)^2 = N$$

au-delà de laquelle nous obtenons des résultats plus grands que N.

Or, mes paraboles permettent de fixer une limite autrement plus intéressante que la précédente, et si cela ne constitue que leur seul intérêt ma recherche n'aura pas été inutile.

En effet, si nous traçons la parabole P_s à laquelle appartient le multiple de 3 immédiatement inférieur à N, nous pouvons affirmer que la parabole-limite supérieure de N a $(s-1)$ pour sommet (voir *fig. 6*). Quant à la parabole-limite inférieure, P_i, elle a pour sommet le carré immédiatement supérieur à N ([1])

([1]) Pour trouver la limite avec le multiple de 3, j'utilise un *truc* personnel empirique : j'ajoute 9 à N et je divise la somme par 6. J'ignore si ce procédé est connu des spécialistes!

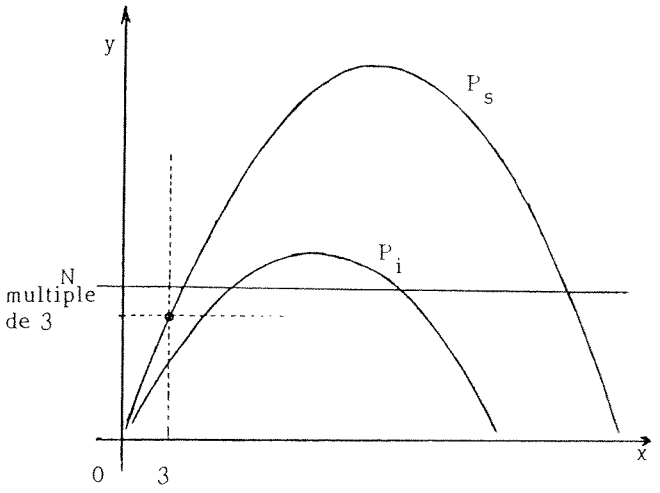


Figure 6

Si N n'est pas premier, sa parabole est impérativement située entre P_s et P_{i-1}. Si, parvenu au stade P_{s-1}, on n'a pas rencontré de carré, N est premier et il est inutile de poursuivre au-delà.

Il est très facile d'abaisser la limite supérieure (P_s), et de manière appréciable de surcroît, en éliminant par méthode naïve les petits facteurs (7, 11 et 13 par exemple), et de calculer le sommet de la parabole à laquelle appartient le multiple de 17 (par exemple) immédiatement inférieur à N.

DIMINUTION DU COÛT

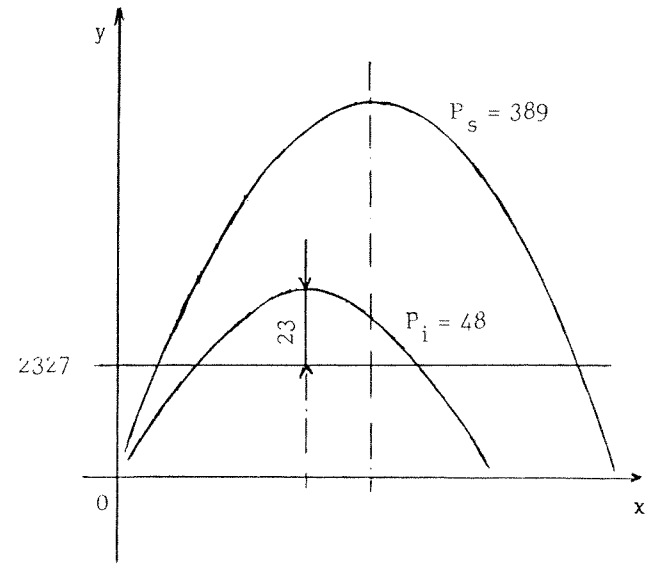


Figure 7

Tous les lecteurs comprendront sans autres explications que l'on peut atteindre le sommet de la parabole de N (si celui-ci n'est pas premier) en parcourant successivement tous les sommets situés entre N et cette parabole. Prenons l'exemple de $2327 (= 13 \times 179)$ (*fig. 7*).

Les additions successives des carrés ou des termes de la progression 1,3,5,7,..., nécessitent 83 opérations qui nous mènent à $2327 + 83^2 = 9216$, carré de 96, sommet de la parabole du nombre donné. Les additions successives des sommets permettent de gagner déjà un temps appréciable puisque 48 opérations seront nécessaires pour parvenir à 6889, carré de 83 ($= \Delta$) :

$$23 + (48 + 49) + (49 + 50) + \cdots (94 + 95) + (95 + 96) = 6889.$$

Le dernier sommet ajouté, 96, est celui de la parabole à laquelle appartient 2327; preuve : $96^2 - 83^2 = 2327$.

Mais on peut également procéder par soustraction en partant du premier sommet (parabole 48), et nous allons voir que c'est la méthode la plus rapide. Pour l'instant, donnons cet exemple :

$$48^2 - 2327(= \text{pas carré})$$
$$49^2 - 23287(= \text{pas carré}) \ldots$$
$$96^2 - 2327 = 6889(= 83^2 = \Delta).$$

Dans les deux derniers procédés, le coût est identique.

En jouant sur les chiffres finals, il est possible de réduire très sensiblement le nombre des opérations. En effet, nous savons que les nombres non premiers terminés par 7 sont les produits de $\ldots 7 \times \ldots 1$ ou de $\ldots 9 \times \ldots 3$, d'où l'on tire : — pour N terminés par 07, 27, 47, 67 et 87, les sommets des paraboles sont des nombres terminés par 4 ou 6 (et b^2 par 6 et Δ par 9) ; — pour N terminés par 17, 37, 57, 77 et 97, les sommets des paraboles sont des nombres terminés par 1 ou 9 (et b^2 par 1 et Δ par 4).

Dans le cas de 2327, nous savons donc que sa parabole (s'il n'est pas premier) a pour sommet un nombre terminé par 4 ou 6, ce qui limite les recherches à :

$$54^2 - 2327, 56^2 - 2327, 64^2 - 2327, \ldots, 94^2 - 2327, 96^2 - 2327,$$

soit 10 opérations, à raison de 2 par dizaine.

Vous pouvez ainsi vérifier que la factorisation de 956506017 réclame 640 soustractions par le procédé précédent ($b^2 - \Delta = 34129^2 - 14432^2$), au lieu de 3000 et quelques opérations.

Mes connaissances en mathématiques sont beaucoup trop restreintes pour explorer davantage ce champ parabolique. D'ailleurs, j'ignore si son sol est fertile ou stérile! Je laisse le soin à ceux qui savent cultiver la mathématique de haut niveau de semer et de récolter.

Quoi qu'il en soit, je me suis bien diverti ...entre deux records du monde de mots croisés (où je suis beaucoup plus à l'aise). Mais, entre nous, il n'y a pas d'abîme insondable entre l'étude que je viens de vous soumettre et les grilles que je soumets à mes lecteurs : une définition de mots croisés n'est-elle pas, elle aussi, une parabole? ...