CORRECTION DU DEVOIR MAISON N° 3	
Congruences et nombres premiers	***Pour le 6 novembre 2007***

Exercice donné en juin 2005 dans les Centres Étrangers

Partie A

1) $N = a^2 - b^2 = (a+b)(a-b)$.
Supposons que a et b soient deux entiers naturels pairs, alors $a+b$ et $a-b$ sont pairs, et par suite, N est pair ; ce qui est contraire à l'hypothèse.
Supposons que a et b soient deux entiers naturels impairs, alors $a+b$ et $a-b$ sont pairs, et par suite, N est pair ; ce qui est contraire à l'hypothèse.
Par conséquent, **a et b n'ont pas la même parité**.

2) $N = a^2 - b^2 = (a+b)(a-b)$. Comme a et b sont des entiers naturels, alors $a+b$ et $a-b$ sont des entiers.
D'où, **N peut s'écrire comme produit de deux entiers naturels p et q**.

3) Comme le produit de p et de q est impair, alors **p et q doivent être impairs**.
En effet, si p et q sont impairs, alors $p = 2m+1$ et $q = 2m'+1$ avec m et m' deux entiers naturels.
Alors $N = 4mm' + 2m + 2m' + 1 = 2(2mm' + m + m') + 1$ avec $2mm' + m + m'$ kk' un entier naturel, ce qui signifierait que N serait un entier impair.

Partie B

1) a)

X	0	1	2	3	4	5	6	7	8
X^2	0	1	4	0	$-2 = 7$	$-2 = 7$	0	4	1

b) Comme $a^2 - 250\,507 = b^2$ et que, d'après la question 1) a), b^2 a pour restes possibles modulo 9 : 0 ; 1 ; 4 et 7, alors **les restes possibles modulo 9 de $a^2 - 250\,507$ sont 0 ; 1 ; 4 et 7**.

Or $250\,507 = 27\,834 \times 9 + 1$, c'est-à-dire $250\,507 \equiv 1 \pmod 9$; et comme $a^2 = b^2 + 250\,507$ alors $a^2 \equiv b^2 + 1 \pmod 9$. Donc, les restes possibles de a^2 modulo 9 sont ceux de $b^2 + 1$.
Par conséquent, les restes possibles de a^2 modulo 9 sont 1 ; 2 ; 5 et 8.
Or d'après la question 1) a), les restes de a^2 modulo 9 sont 0 ; 1 ; 4 et 7.
On en conclut que **le reste de a^2 modulo 9 est 1**.

c) D'après les questions 1) a) et 1) b), on en déduit que **les restes possibles de a modulo 9 sont 1 et 8**.

2) a) Si le couple $(a\,;\,b)$ vérifie la relation (E), alors $a^2 - 250\,507 = b^2$, c'est-à-dire $a^2 = b^2 + 250\,507$.
Comme $b^2 \geq 0$, alors $b^2 + 250\,507 \geq 250\,507$, ou encore $a^2 \geq 250\,507$.

C. Lainé

Or la fonction racine carrée est strictement croissante sur $[0\ ;\ +\infty[$, alors $a \geq \sqrt{250\,507}$, c'est-à-dire $a \geq 501$.
Par conséquent, **si le couple $(a\,;b)$ vérifie la relation (E), alors $a \geq 501$**.

b) $(501\,;b)$ est solution de (E) équivaut à $501^2 - 250\,507 = b^2$, c'est-à-dire à $b^2 = 494$.
Or l'équation $b^2 = 494$ n'a pas de solution dans **N**.
Par conséquent, **il n'existe pas de solution du type $(501\,;\ b)$**.

3) a) $503 \equiv 8 \pmod 9$ car $503 = 55 \times 9 + 8$, et $505 \equiv 1 \pmod 9$ car $505 = 56 \times 9 + 1$.
Comme 503 et 505 sont supérieurs à 501, et que a est égal à 1 ou à 8 modulo 9 (d'après la question 1) c) de la partie B, alors ***a* est congru à 503 ou à 505 modulo 9**.

b) $(505 + 9k\ ;\ b)$ est solution de (E) équivaut à $(505 + 9k)^2 - 250\,507 = b^2$, c'est-à-dire à $b^2 = 81k^2 + 9090k + 4518$.
Faisons un tableau :

k	b^2	Est-ce que $\sqrt{b^2}$ est un entier ?
0	4518	non
1	13689	oui
2	23022	non
3	32517	non
4	42174	non
5	51993	non
6	61974	non
7	72117	non
8	82422	non
9	92889	non
10	103518	non

Par conséquent, **1 est le plus petit entier naturel k tel que le couple $(505 + 9k\ ;\ b)$ soit solution de (E) ; ce couple solution est $(514\ ;\ 117)$**.

Partie C

1) D'après la partie B, le couple $(514\ ;\ 117)$ est une solution de (E), alors
$\mathbf{250\,507} = (514 + 117) \times (514 - 117) = \mathbf{631 \times 397}$.

2) Utilisons l'algorithme d'Euclide :

Étapes	a	b	Restes	
1	631	397	112	631 = 1 × 397 + 234
2	397	234	98	397 = 1 × 234 + 163
3	234	163	14	234 = 1 × 163 + 71
4	163	71	21	163 = 2 × 71 + 21
5	71	21	8	71 = 3 × 21 + 8
6	21	8	5	21 = 2 × 8 + 5
7	8	5	3	8 = 1 × 5 + 3
8	5	3	2	5 = 1 × 3 + 2

9	3	2	**1**		$3 = 1 \times 2 + 1$
10	2	1	0		$2 = 1 \times 2 + 0$

Le PGCD de 631 et de 397 est 1 ; par conséquent, **631 et 397 sont premiers entre eux**.

3) D'après la question précédente, la seule écriture primaire de 250 507 est 631×397. Il n'existe pas d'autre écriture si ce n'est l'écriture $1 \times 250\ 507$. De plus, les nombres 631 et 397 sont premiers.
L'écriture précédente est donc unique.