Maths Expertes
Terminale

Nombres Premiers

CORRIGÉ DE L'EXERCICE

Modulo p premier

02

Correction

1. Montrons que *p* est de la forme $4n+1$ ou $4n+3$:

Par hypothèse, l'entier *a* est un « entier pair non nul ». Son carré est aussi un entier pair, et le nombre a^2+1 est un nombre impair.

Si *p* est un nombre premier qui divise a^2+1, ce nombre premier est impair (ce n'est pas 2).

Il existe donc un entier *u* strictement positif (car $p \geq 3$) tel que : $p = 2u+1$. Discutons suivant la parité de *u* :

- Si *u* est pair, il existe un entier $n > 0$ tel que $u = 2n$. Alors $p = 4n+1$.
- Si *u* est impair, il existe un entier $n \geq 0$ tel que $u = 2n+1$.
  Alors $p = 2(2n+1)+1 = 4n+3$.

Bilan : *p* est de la forme $4n+1$ (avec $n > 0$) ou de la forme $4n+3$ (avec $n \geq 0$).

2.a. Montrons que *p* ne divise pas *a* :

Cette propriété ne dépend pas de la forme de *p*. Peu importe que *p* soit de la forme $4n+1$ ou bien $4n+3$, seule intervient l'hypothèse « *p* divise le nombre a^2+1 ».

En effet, s'il en est ainsi, il existe un entier naturel *k* tel que : $a^2+1 = kp$.

Cette égalité peut s'écrire : $-a \times a + p \times k = 1$. Sous cette forme, il s'agit d'une relation de Bézout de la forme « $au+pv=1$ » avec $u = -a$; $v = k$, relation prouvant que *p* et *a* sont premiers entre eux.

Les entiers *p* (qui est ≥ 3) et *a* sont premiers entre eux donc *p* ne divise pas *a*.

2.b. Montrons que $(a^4)^n \times a^2 \equiv 1\ [p]$:

NB. L'entier *n* dont il est question est l'entier naturel vérifiant l'hypothèse $p = 4n + 3$.

En vertu des règles opératoires sur les puissances : $(a^4)^n \times a^2 = a^{4n+2}$

- *p* est un nombre premier.
- Le nombre entier naturel *a* n'est pas divisible par *p*.

Nous pouvons appliquer le petit théorème de Fermat avec, dans le contexte qui nous occupe,

$p - 1 = (4n + 3) - 1 = 4n + 2$.

D'après le petit théorème de Fermat : $a^{4n+2} \equiv 1\ [p]$

Autrement dit : $(a^4)^n \times a^2 \equiv 1\ [p]$.

2.c. Déduisons-en une contradiction :

D'une part, puisque *p* divise le nombre $a^2 + 1$, nous disposons de la congruence $a^2 + 1 \equiv 0\ [p]$ donc de la congruence $a^2 \equiv -1\ [p]$.

Par élévation au carré des deux membres de cette congruence, nous obtenons la congruence :

$a^4 \equiv (-1)^2\ [p]$, c'est-à-dire la congruence $a^4 \equiv 1\ [p]$.

Nous en déduisons, par élévation des deux membres à la puissance *k*, que pour tout entier naturel *k* :

$(a^4)^k \equiv 1\ [p]$. En particulier : $(a^4)^n \equiv 1\ [p]$.

D'autre part, sous l'hypothèse de la question précédente, $(a^4)^n \times a^2 \equiv 1\ [p]$.

Compte tenu de la congruence $(a^4)^n \equiv 1\ [p]$, nous obtenons $a^2 \equiv 1\ [p]$.

Ainsi, simultanément : $\begin{cases} a^2 \equiv 1\ [p]. \\ a^2 \equiv -1\ [p]. \end{cases}$. Mais puisque *p* est distinct de 2, ces deux congruences sont incompatibles. Il est impossible que le carré de *a* soit, en même temps, congru à 1 et à -1 modulo *p*.

3. Concluons :

L'hypothèse « Il existe un diviseur premier du nombre $a^2 + 1$ qui est de la forme $4n + 3$ » conduisant à une contradiction, cette hypothèse est à rejeter.

Nous devons tenir pour vraie la proposition contraire, soit :

« Aucun diviseur premier du nombre $a^2 + 1$ n'est de la forme $4n + 3$ ».

Autrement dit :

« Tous les diviseurs premiers du nombre $a^2 + 1$ sont de la forme $4n + 1$ ».

3. Concluons encore (suite et fin) :

L'injonction « Conclure » de l'énoncé est ouverte, l'énoncé ne nous impose pas à propos de quoi « conclure ». Il nous appartient d'en décider nous-mêmes. Nous avons proposé ci-dessus une conclusion honorable et, à notre sens, tout à fait satisfaisante. Cette conclusion peut clôturer la correction de cet exercice.

Rien ne nous empêche cependant de pousser le bouchon plus loin. Chose que nous nous proposons de faire ci-dessous.

Désignons par *E* l'ensemble des nombres premiers de la forme $4n + 1$.

Nous pouvons repérer facilement quelques éléments de *E*, par exemple :

$p_1 = 5$; $p_2 = 13$; $p_3 = 17$; $p_4 = 29$.

Supposons que nous ayons identifié un certain nombre *k* d'éléments de *E* : p_1 ; p_2 ; … ; p_k.

Posons $a_k = 2 \times p_1 \times p_2 \times \ldots \times p_k$ (deux fois le produit de ces nombres premiers) et $b_k = {a_k}^2 + 1$.

D'après les questions précédentes :

- a_k est un nombre pair non nul.
- Tous les facteurs premiers de b_k appartiennent à *E*.
- b_k est premier avec a_k donc avec chacun des nombres p_1 ; p_2 ; … ; p_k

Donc, ces facteurs premiers de b_k (il y en a au moins un) sont de nouveaux éléments de *E* qui n'ont pas encore été identifiés. Quel que soit le nombre *k* d'éléments déjà identifiés de *E*, il y en a au moins un autre.

Il en résulte que *E* n'a pas un nombre fini d'éléments.

Par exemple, à l'aide de $a_4 = 2 \times 5 \times 13 \times 17 \times 29$, nous obtenons trois nouveaux éléments de *E* :

37, 173 et 641701.

Define $a4=2\cdot 5\cdot 13\cdot 17\cdot 29$	*Terminé*
$a4$	64090
Define $b4=a4^2+1$	*Terminé*
$b4$	4107528101
factor$(b4)$	$37\cdot 173\cdot 641701$

Concluons :

Il y a une infinité de nombres premiers de la forme $4n + 1$.