Arithmétique

Durée : 2 h

L'usage des documents, des calculatrices, des ordinateurs, des téléphones portables et de tout dispositif électronique est interdit. Les téléphones portables doivent être rangés dans les sacs. Les résultats indiqués dans l'énoncé peuvent êtres utilisés pour la suite du problème. Il ne faut pas hésiter à traiter les questions dans l'ordre de son choix.

On considère l'exercice suivant que l'on ne demande pas de résoudre en totalité. Les questions auxquelles vous devez répondre sont indiquées plus bas dans *Les questions pour le candidat.*

L'exercice tiré du manuel Sesamaths.

130 Le théorème de Wilson Démo

Soit un nombre premier $p > 3$ et l'ensemble des naturels $A = [2\,;p-2]$.

1. Montrer que pour tout $x \in A$, p ne divise pas $x^2 - 1$.

2. a) Soit $x \in A$, montrer qu'il existe $u \in \mathbb{Z}$ tel que : $xu \equiv 1\ (p)$.

b) En déduire l'existence d'un unique entier $r \in A$ distinct de x tel que $xr \equiv 1\ (p)$.

c) Établir que : $2 \times 3 \times \ldots \times (p-2) \equiv 1\ (p)$ puis que $(p-1)! \equiv -1\ (p)$.

3. Ce résultat est-il encore vrai pour $p = 2$ et $p = 3$?

4. Réciproquement, soit p un entier ($p \geqslant 2$) tel que : $(p-1) \equiv -1\ (p)$.

En raisonnant par l'absurde, montrer que p est premier.

5. En déduire le théorème de Wilson : « Un entier naturel n est premier si, et seulement si, $(n-1)! + 1$ est divisible par n ».

6. Application : montrer que 13 est premier à l'aide du théorème de Wilson.

Ce théorème est-il judicieux comme test de primalité ?

Réponse de l'élève (1) à la question 1.

x est dans A donc $x \leq p-2$. . Si p divise x^2-1 alors p divise $(x-1)(x+1)$ (identité remarquable). Mais si un entier n divise ab, on sait que n divise a ou n divise b, donc si $n = p$ si p divise x^2-1 alors p divise $x-1$ ou p divise $x+1$. Maintenant on fait deux cas :
- si p divise $x-1$ alors p divise un élément de $[1, p-3]$ et ce n'est pas possible.
- si p divise $x+1$ alors p divise un élément de $[3, p-1]$ et ce n'est pas possible non plus.

Réponse de l'élève (2) à la question 4.

Je veux montrer que si n n'est pas premier alors $(n-1)!$ est différent de (-1) modulo n. Si n n'est pas premier alors $n = d_1 d_2$ avec d_1 et d_2 des entiers tels que $1 \leq d_1 < d_2 \leq n-1$.
Dans le produit qui donne $(n-1)!$ les nombres d_1 et d_2 apparaissent
car $(n-1)! = 1 \times 2 \times \ldots \times d_1 \times \ldots \times d_2 \times \ldots \times (n-1)$ donc $d_1 d_2 | (n-1)!$ et alors $(n-1)! \equiv 0\ (n)$.

Réponse de l'élève (3) à la question 4.

On suppose que $(p-1)! \equiv (-1)\ (p)$. Soit $k \in \mathbb{Z}$. On a par définition de la congruence que $(p-1)! - (-1) = kp$. Donc $(p-1)! + 1 = kp$. Après je suis bloqué.

Les questions pour le candidat.

A. Analyser la réponse de l'élève (1) en en mettant en évidence acquis et faiblesses. On essaiera de hiérarchiser et d'être synthétique. Quand c'est possible, proposer une remédiation pour les faiblesse significatives relevées.

B. Proposer une correction de la question **1** destinée à une classe de Terminale.

C. Quel théorème du cours est clairement l'outil clé pour répondre à la question **2.a** ? Enoncer et démontrer ce théorème. (Si votre démonstration de ce théorème repose essentiellement sur un autre théorème du cours, on le démontrera également.)

D. Proposer une correction de la question **2.c** destinée à une classe de Terminale.

E. Il manque des cas à étudier dans la réponse de l'élève (2). Identifier ces cas manquants et résoudre la question **4** pour ces cas en suivant la démarche de l'élève.

F. A partir de la réponse de l'élève (3), et en améliorant, proposer une autre réponse à la question **4**.

G. On suppose que l'exercice est terminé et que l'on a démontré le théorème de Wilson. Montrer que si p est un nombre premier et si n est un entier tel que $1 \leq n \leq p$ alors on a $(n-1)!(p-n)! \equiv (-1)^n \pmod{p}$.

Question indépendante.

Un élève demande :

Est-ce que le nombre $6,21515151...$ où je répète le 51 à l'infini c'est une fraction ?

H.1 Reformuler la question de l'élève en utilisant le vocabulaire à bon escient.
H.2 Proposer une réponse, au niveau de votre choix

[Pour H.2, on n'utilisera pas un théorème donnant directement la réponse,
mais <u>on démontrera ce que l'on annonce</u> dans ce cas particulier.]