Maths Expertes
Terminale

Nombres Premiers

CORRIGÉ DE L'EXERCICE

Modulo p premier

01

Correction

Nous rappelons l'énoncé du théorème de Gauss, que nous aurons l'occasion d'utiliser.
« Soit *a, b, c* des entiers relatifs. Si *a* divise le produit $b \times c$ et s'il est premier avec *b*, alors il divise *c* ».

Intéressons-nous également aux hypothèses « *a* non congru à 0 modulo *p* » (**question 1**) et « *a* premier avec *p* » (**question 2**).
D'après l'énoncé, *p* est un nombre premier, il n'a que deux diviseurs. Par conséquent, étant donné un entier relatif *a*, le PGCD de *p* et de *a* ne peut prendre que deux valeurs, ou bien *p* ou bien 1. De deux choses l'une : ou bien *p* divise *a* ou bien *p* et *a* sont premiers entre eux. Les hypothèses des questions 1 et 2 sont donc équivalentes ; nous lisons deux formulations différentes pour exprimer une même chose. Il est certain qu'il s'agit d'une volonté délibérée de l'auteur du sujet.

1. Montrons que, si $a \not\equiv 0 \ [p]$, $ax \equiv ay \ [p] \ \Rightarrow \ x \equiv y \ [p]$:

NB. Comme nous l'avons indiqué en préambule, *p* étant un nombre premier, l'hypothèse « $a \not\equiv 0 \ [p]$ » est équivalente à l'hypothèse « *a* et *p* sont premiers entre eux ».

Soit *x* et *y* deux entiers relatifs. Supposons qu'ils vérifient la congruence : $ax \equiv ay \ [p]$.
Par définition d'une congruence modulo *p*, cette congruence est vérifiée si et seulement si *p* divise la différence $ax - ay$, c'est-à-dire si et seulement si *p* divise $a \times (x - y)$.

Or, *p* et *a* sont premiers entre eux. Nous pouvons appliquer le théorème de Gauss : l'entier *p* divise le produit $a \times (x - y)$ et il est premier avec *a*, donc il divise $(x - y)$.
Par définition d'une congruence modulo *p*, dire que *p* divise $(x - y)$ équivaut à dire que $x \equiv y \ [p]$.
Concluons :

Sous l'hypothèse $a \not\equiv 0 \ [p]$, si *x* et *y* vérifient $ax \equiv ay \ [p]$, alors $x \equiv y \ [p]$.

2. Montrons que si *a* est premier avec *p* et si *n* est multiple de $p-1$, alors $a^n \equiv 1 \ [p]$:

Dans cette question, *n* est un entier naturel. Dire que « *n* est multiple de $p-1$ » revient à dire qu'il existe un entier naturel *k* tel que $n = k(p-1)$. C'est là l'entier *k* que nous allons utiliser ci-dessous.

Commençons par démontrer la congruence stratégique : $a^{p-1} \equiv 1 \ [p]$.

- *p* est un nombre premier.
- Le nombre entier *a* n'est pas divisible par *p* (car par hypothèse *p* et *a* sont premiers entre eux).

Nous pouvons appliquer le petit théorème de Fermat.

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

Nous pouvons dès lors élever à la puissance *k* (entier naturel comme nous l'avons noté) les deux membres de cette congruence.

Nous obtenons une nouvelle congruence modulo *p* : $(a^{p-1})^k \equiv 1^k \ [p]$.

En tenant compte d'une part que $(a^{p-1})^k = a^{k(p-1)} = a^n$ et d'autre part que 1 est invariant par élévation à une puissance, cette congruence s'écrit aussi bien : $a^n = a^{k(p-1)} \equiv 1 \ [p]$.

En conclusion, si *n* est un multiple de $p-1$: $a^n \equiv 1 \ [p]$.

3. Si *a* est premier avec *p*, montrons l'existence d'un entier *b* tel que $ab \equiv 1 \ [p]$:

NB. L'entier *p* étant un nombre premier, il est supérieur ou égal à 2. Dans a^{p-2}, qui intervient dans la résolution de cette question, l'exposant $p-2$ est toujours un entier naturel, le nombre a^{p-2} est toujours un nombre entier non nul.

Soit *a* un entier relatif premier avec *p*. Appliquons le résultat de la **question 1** avec $n = p-1$ (voir la « congruence stratégique » de cette question) : $a^{p-1} \equiv 1 \ [p]$.

Nous pouvons écrire cette congruence ainsi : $a \times a^{p-2} \equiv 1 \ [p]$.

Nous obtenons le résultat recherché en considérant l'entier relatif $b = a^{p-2}$.

Pour tout entier *a* premier avec *p*, le nombre a^{p-2} est un inverse modulo *p* de *a*.

4. Déduisons-en que tout entier *a* tel que $0 < a < p$ admet un inverse modulo *p* strictement compris entre 0 et *p* :

L'entier *p* étant un nombre premier, il est premier avec tout entier *a* strictement positif qui est strictement plus petit que lui (c'est-à-dire avec tout entier *a* de l'ensemble $\{1, \ 2, \ldots, \ p-1\}$).

D'après la question précédente, tout élément *a* de cet ensemble a pour inverse modulo *p*, l'entier $b = a^{p-2}$.

Soit alors *r* le reste de la division euclidienne de $b = a^{p-2}$ par *p*.

- D'une part $0 \leq r < p$, mais *r* n'est pas nul (car *a* et *p* étant premiers entre eux, a^{p-2} et *p* sont aussi premiers entre eux : *p* ne divise pas a^{p-2}).
- D'autre part $r \equiv b\ [p]$ donc $ar \equiv ab\ [p]$ et, par transitivité, $ar \equiv 1\ [p]$

Le reste *r* de la division euclidienne de a^{p-2} par *p* est un inverse modulo *p* de *a* qui vérifie la double inégalité $0 < r < p$.

Complément offert par Freemaths, calcul automatisé à l'aide de Python de « l'inverse modulo *p* compris strictement entre 0 et *p* » :

L'algorithme « invmodulo » a pour argument un nombre premier *p*. Pour tout entier *a* de l'ensemble $\{2,\ 3, \ldots,\ p-1\}$, l'algorithme calcule $b = a^{p-2}$ puis le reste *r* de la division euclidienne de $b = a^{p-2}$ par *p* et affiche les nombres *b* et *r*. L'algorithme procède ensuite à une vérification (facultative …), il vérifie que l'entier *r* est bien l'inverse modulo *p* compris entre 0 et *p* de l'entier *a*.
(Nous avons négligé volontairement le cas trivial de l'entier 1 qui a pour inverse modulo *p* lui-même).

Pour l'exemple, cet algorithme a été testé avec $p = 7$. Il va de soi que les deux inverses proposés ne sont pas les seuls. Tous les entiers congrus modulo 7 aux deux nombres cités sont eux aussi des « inverses modulo 7 ».

```
>>> def invmodulo(p):
        for a in range(2,p):
                b=a**(p-2)
                r=b%p
                v=(r*a)%p
                print(a,"a pour inverses modulo",p,"les entiers",b,"et",r)
                print(" Vérifions : Le produit",r,"x",a,"est congru à",v,"modulo",p)


>>> invmodulo(7)
2 a pour inverses modulo 7 les entiers 32 et 4
        Vérifions : Le produit 4 x 2 est congru à 1 modulo 7
3 a pour inverses modulo 7 les entiers 243 et 5
        Vérifions : Le produit 5 x 3 est congru à 1 modulo 7
4 a pour inverses modulo 7 les entiers 1024 et 2
        Vérifions : Le produit 2 x 4 est congru à 1 modulo 7
5 a pour inverses modulo 7 les entiers 3125 et 3
        Vérifions : Le produit 3 x 5 est congru à 1 modulo 7
6 a pour inverses modulo 7 les entiers 7776 et 6
        Vérifions : Le produit 6 x 6 est congru à 1 modulo 7
```