DOMAINE : Arithmétique
NIVEAU : Débutants
CONTENU : Exercices

AUTEUR : Vincent JUGÉ
STAGE : Montpellier 2012

Congruences

- Énoncé des exercices vus en cours -

Exercice 1 Trouver les entiers a tels que 5 divise $a^3 + 3a + 1$.

Exercice 2 Trouver les entiers a, b et c tels que $a^2 + b^2 + 1 = 4c$.

Exercice 3 Trouver un entier x tel que $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 4$ et $x \equiv 1 \pmod 5$.

Exercice 4 Existe-t-il un entier x tel que $x \equiv 1 \pmod 6$, $x \equiv 9 \pmod{14}$ et $x \equiv 7 \pmod{15}$?

Exercice 5 Le nombre $\underbrace{20122012\ldots2012}_{\text{2012 fois ″2012″}}$ est-il divisible par 19 ?

Exercice 6 Soit a un entier. Montrer que $a^{561} \equiv a \pmod{561}$.

Exercice 7 Soit p et q deux nombres premiers distincts, d et e deux entiers tels que $de \equiv 1 \pmod{(p-1)(q-1)}$ et a un entier quelconque. Montrer que $\left(a^d\right)^e \equiv a \pmod{pq}$.

- Solutions -

Solution de l'exercice 1 La condition se réécrit $a^3 + 3a + 1 \equiv 0 \pmod 5$. En essayant les 5 résidus, on constate que les seules solutions sont les entiers congrus à 1 et 2 modulo 5.

Solution de l'exercice 2 Le problème revient à rechercher les entiers a et b tels que $a^2 + b^2 + 1 \equiv 0 \pmod 4$. Les seuls carrés modulo 4 sont 0 et 1, et on constate donc que l'équation $a^2 + b^2 + 1 \equiv 0 \pmod 4$ n'admet aucune solution. Il s'ensuit que nul triplet d'entiers (a, b, c) ne vérifie $a^2 + b^2 + 1 = 4c$.

Solution de l'exercice 3 Tout d'abord, le théorème chinois indique qu'un tel x existe bien, car 3, 4 et 5 sont premiers entre eux deux à deux. En outre, il indique également qu'il existe un unique entier naturel $a < 3 \times 4 \times 5 = 60$ tel que $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 4$ et $x \equiv 1 \pmod 5$ si et seulement si $x \equiv a \pmod{60}$.

Cherchons alors un tel entier a. On sait que $a \equiv 2 \pmod 3$ et que $a \equiv 3 \pmod 4$. On peut donc écrire $a = 3k + 2$. Il faut alors que k satisfasse l'égalité $3k + 2 \equiv 3 \pmod 4$, ou encore $3k \equiv 1 \pmod 4$.

Puisque 3 est inversible modulo 4 et que son inverse est 3 , cela signifie que $k \equiv 3 \pmod 4$. On peut ainsi écrire $k = 4l + 3$, et donc $a = 12l + 11$.

On veut alors que l satisfasse l'égalité $12l + 11 \equiv 1 \pmod 5$, ou encore $12l \equiv 0 \pmod 5$. Puisque 12 est inversible modulo 12, il s'ensuit que $l \equiv 0 \pmod 5$. On peut donc écrire $l = 5m$ et $a = 60m + 11$.

On a donc montré que $a = 11$. En particulier, il s'ensuit que $x = 11$ satisfait simultanément les trois égalités $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 4$ et $x \equiv 1 \pmod 5$.

Solution de l'exercice 4 On souhaiterait appliquer directement le théorème chinois, mais on ne le peut pas, parce que 6 et 14 ne sont pas premiers entre eux (et que 6 et 15 ne sont pas premiers entre eux non plus).

Il faut alors ruser dans l'utilisation du théorème chinois : en factorisant $6 = 2 \times 3$, $14 = 2 \times 7$ et $15 = 3 \times 5$, on remarque que

– $x \equiv 1 \pmod 6$ si et seulement si $x \equiv 1 \pmod 2$ et $x \equiv 1 \pmod 3$;

– $x \equiv 9 \pmod{14}$ si et seulement si $x \equiv 9 \equiv 1 \pmod 2$ et $x \equiv 9 \equiv 2 \pmod 7$;

– $x \equiv 7 \pmod{15}$ si et seulement si $x \equiv 7 \equiv 1 \pmod 3$ et $x \equiv 7 \equiv 2 \pmod 5$.

On a donc montré que $x \equiv 1 \pmod 6$, $x \equiv 9 \pmod{14}$ et $x \equiv 7 \pmod{15}$ si et seulement si $x \equiv 1 \pmod 2$, $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$ et $x \equiv 2 \pmod 7$. Le théorème chinois indique alors qu'il existe bien un tel entier x, et même, après un peu de travail, que ces entiers sont les entiers congrus à 37 (mod 210).

Solution de l'exercice 5 Dans la suite, on note N le nombre $\underbrace{20122012\ldots2012}_{\text{2012 fois "2012"}}$, pour plus de simplicité dans les notations. Remarquons que $N = 2012 \sum_{k=0}^{2011} 10^{4k} = 2012 \dfrac{10^{8048} - 1}{10^4 - 1}$.

L'idée est alors de regarder les puissances de 10 modulo 7 : $10 \equiv 10 \pmod{19}$, $10^2 \equiv 5 \pmod{19}$, $10^3 \equiv 12 \pmod{19}$, … En outre, le petit théorème de

Fermat indique que $10^{18} \equiv 1 \pmod{19}$. Ceci montre que $2012 \equiv 2 \times 10^3 + 10 + 2 \equiv 2 \times 12 + 12 \equiv 17 \pmod{19}$.

De surcroit, puisque $8048 \equiv 2 \pmod{9}$ et $8048 \equiv 0 \pmod{2}$, alors $8048 \equiv 2 \pmod{18}$: on peut écrire 8048 sous la forme $8048 = 18k + 2$. Il s'ensuit que $10^{8048} \equiv \left(10^{18}\right)^k \times 10^2 \equiv 5 \pmod{19}$.

On a ainsi prouvé que 19 ne divise ni 2012 ni $10^{8048} - 1$. En particulier, cela montre que 19 ne divise pas $2012\left(10^{8048} - 1\right)$, et donc ne divise pas N non plus.

Solution de l'exercice 6 On commence par factoriser 561 en produit de facteurs premiers : $561 = 3 \times 11 \times 17$. D'après le théorème chinois, il suffit alors de montrer que $a^{561} \equiv a \pmod{3}$, $a^{561} \equiv a \pmod{11}$ et $a^{561} \equiv a \pmod{17}$.

En particulier, on note que $561 = 2 \times 280 + 1 = 10 \times 56 + 1 = 16 \times 35 + 1$, donc que $a^{561} \equiv \left(a^2\right)^{280} \times a \equiv a \pmod{3}$, $a^{561} \equiv \left(a^{10}\right)^{56} \times a \equiv a \pmod{11}$ et $a^{561} \equiv \left(a^{16}\right)^{35} \times a \equiv a \pmod{17}$.

Cela signifie que $a^{561} - a$ est divisible à la fois par 3, par 11 et par 17, c'est-à-dire que $a^{561} \equiv a \pmod{561}$.

Solution de l'exercice 7 Soit k un entier tel que $de = k(p-1)(q-1) + 1$. Si p divise a, alors $a^{de} \equiv 0 \equiv a \pmod{p}$. Sinon, alors $a^{de} \equiv \left(a^{p-1}\right)^{k(q-1)} \times a \equiv a \pmod{p}$. Dans tous les cas, cela signifie que $a^{de} \equiv a \pmod{p}$.

De même, on montre que $a^{de} \equiv a \pmod{p}$. Le théorème chinois indique alors que $a^{de} \equiv a \pmod{pq}$.