# Arithmétique A

16 Janvier

On commencera par corriger les exercices $1, 3, 4, 8, 9, 11, 12, 13, 17$ et d'autres s'il reste du temps, concentrez-vous donc sur ceux-là.

## Exercices

*Exercice 1.* Est-ce qu'on a $100 \equiv 1 \pmod{3}$ ? $\pmod{9}$ ? $\pmod{11}$ ?
Est-ce qu'on a $15 \equiv 37 \pmod{5}$ ? $\pmod{11}$ ?

*Exercice 2.* On suppose que $n$ est un multiple de $3$, quelles sont les valeurs possibles de $n$ modulo $9$ ?

*Exercice 3.* Quelles sont les valeurs possibles de $x^3$ modulo $9$ ?
Est-il possible d'avoir $x^3 + y^3 = z^3 + 4$ ?

*Exercice 4.* Quelles sont les valeurs possibles de $x^2$ modulo $4$ ?
En déduire les parités possibles de $x, y, z$ si on a $x^2 + y^2 = z^2$.

*Exercice 5.* Résoudre l'équation diophantienne $x^2 + y^2 = 206$.

*Exercice 6.* Montrer que si $p$ et $p^2 + 2$ sont premiers, alors $p^3 + 2$ est premier.

*Exercice 7.* Pour quelles valeurs de $n \geqslant 2$ le nombre $n^{n-1} + 2n - 3$ est-il premier ?

*Exercice 8.* (Critères de divisibilité)
Soit $n$ un entier. Montrer que $n$ est divisible par...
$1)$ $3$ ou $9$ si et seulement si la somme de ses chiffres l'est.
$2)$ $2$ ou $5$ si et seulement si son dernier chiffre l'est.
$3)$ $4$ si et seulement si ses deux derniers chiffres le sont.
$4)$ En s'inspirant de $1)$, énoncer un critère de divisibilité par $11$ et le démontrer.
123456784 est-il divisible par $11$ ?

*Exercice 9.* Pour chaque question qui suit, indiquer si ce nombre possède un inverse pour ce modulo, et le trouver s'il existe.
$a)$ $1$ modulo $15$
$b)$ $47$ modulo $24$
$c)$ $14$ modulo $35$

d) $12$ modulo $17$
e) $19$ modulo $43$

*Exercice 10.* Soit $p > 3$ un nombre premier, montrer que $p^2 \equiv 1 \pmod{24}$.

*Exercice 11.* Alice collectionne les billes. Elle sait qu'elle en a moins de $100$, et quand elle les ordonne en rangées de $4$, il lui en reste $2$, quand elle les ordonne en rangées de $5$, il lui en reste $1$ et quand elle les ordonne en rangées de $7$, il lui en reste $3$. Combien Alice a-t-elle de billes ?

*Exercice 12.* Alice collectionne les billes. Elle sait qu'elle en a moins de $100$, et quand elle les ordonne en rangées de $4$, il lui en reste $2$, quand elle les ordonne en rangées de $6$, il lui en reste $1$ et quand elle les ordonne en rangées de $7$, il lui en reste $3$. Combien Alice a-t-elle de billes ?

*Exercice 13.* Alice collectionne les billes. Elle sait qu'elle en a moins de $100$, et quand elle les ordonne en rangées de $4$, il lui en reste $2$, quand elle les ordonne en rangées de $6$, il lui en reste $4$ et quand elle les ordonne en rangées de $7$, il lui en reste $4$. Combien Alice a-t-elle de billes ?

On raconte que pour compter leur armée, des généraux chinois de l'Antiquité demandaient à leurs soldats de s'organiser en rangées de différents nombres (5,7,8,9,11 par exemple) et ils regardaient le nombre de soldats qui n'avaient plus de place dans une rangée, et utilisaient alors ce qu'on connaît maintenant sous le nom de théorème des restes chinois pour calculer leurs effectifs avec relativement peu de calculs.

*Exercice 14.* Trouver les solutions entières de l'équation $x^3 - y^3 = 24$.

*Exercice 15.* Soit $p$ premier. Quels sont les nombres qui sont égaux à leur inverse modulo $p$ ?

*Exercice 16.* Quels sont les entiers positifs $n$ tels que $\dfrac{9n^2+31}{n^2+7}$ soit entier ?

*Exercice 17.* Quel est le dernier chiffre de $2018^{2019^{2020}}$ ?

*Exercice 18.* Quel est le reste de la division euclidienne de $2018^{2019^{2020}}$ par $11$ ?

## Toujours des exercices, mais plus durs

*Exercice 19.* (Démonstration de petit Fermat)
On considère l'ensemble $A = \{1, 2, \ldots, p-1\}$ des nombres entre $1$ et $p-1$. Soit $a$ un nombre entier, notons $f(n)$ le reste de la division euclidienne de $a \times n$ par $p$.
1) Montrer que $A = \{f(1), f(2), \ldots, f(p-1)\}$.

2) En considérant le produit de tous les éléments, déduire que $a^{p-1} \equiv 1 \pmod p$.

*Exercice 20.* (Wilson)
On note $n! = 1 \times 2 \times 3 \times \cdots \times n$ (prononcé factorielle $n$). Par exemple, $3! = 6, 6! = 720, 7! = 5040$.
1) Soit $p$ un entier. Montrer que si $(p-1)! \equiv -1 \pmod p$, alors $p$ est premier.
2) Faire l'exercice $15$.
3) En regroupant les inversibles par paires, montrer que si $p$ est premier, alors $(p-1)! \equiv -1 \pmod p$.

On a ainsi donné un moyen de savoir avec certitude si un nombre est premier ou pas, sans regarder ses facteurs ! Cependant ce n'est pas très utile pour faire un programme disant si un nombre est premier ou non, puisque le calcul de $(p-1)!$ modulo $p$ est très long.

*Exercice 21.* Soit $n$ un entier impair, et on suppose que dans sa décomposition en facteurs premiers, les exposants sont toujours $1$ (on dit que $n$ est *squarefree*). Combien de nombres parmi $1, \dots, n$ sont leurs propres inverses modulo $n$ ?
*Indice : commencer par faire l'exercice* $15$.

*Exercice 22.* Trouver tous les $p, q > 5$ premiers tels que $pq \mid (5^p - 2^p)(5^q - 2^q)$