Arithmétique – Partie 4 : Congruences

Exercice 1.

Simplifier les expressions suivantes (sans calculatrice). Par exemple "simplifier $72\ [7]$" signifie "trouver n entre 0 et 6 tel que $72 \equiv n\ [7]$" ; la réponse est $n = 2$.

— $45\ [7]$, $39\ [7]$, $45+39\ [7]$, $45 \times 39\ [7]$, $45^2\ [7]$, $39^3\ [7]$.

— $1052\ [22]$, $2384\ [22]$, $2384-1052\ [22]$, $1052^2 \times 2384\ [22]$.

Indications 1.

Pour les calculs modulo 7 on se ramène à un entier compris entre 0 et 6. Modulo 22 on se ramène à un entier compris entre 0 et 21.

Correction 1.

1. — $45 = 42+3 = 7\times 6+3$, ainsi $45 \equiv 3\ [7]$.
   — $39 = 35+4 = 7\times 5+4$, ainsi $39 \equiv 4\ [7]$.
   — Pour réduire $45+39$, on ne fait pas d'abord la somme, on utilise en premier nos réductions précédentes :
   $$45+39 \equiv 3+4 \equiv 7 \equiv 0\ [7].$$
   Ainsi, sans effort, on sait que $45+39$ est divisible par 7.
   — $45\times 39 \equiv 3\times 4 \equiv 12 \equiv 5\ [7]$.
   — $45^2 \equiv 3^2 \equiv 9 \equiv 2\ [7]$.
   — $39^3 \equiv 4^3 \equiv 64 \equiv 1\ [7]$.
2. — $1052 = 22\times 47+18$ donc $1052 \equiv 18\ [22]$.
   — $2384 = 22\times 108+8$ donc $2384 \equiv 8\ [22]$.
   — $2384-1052 \equiv 8-18 \equiv -10 \equiv 12\ [22]$.
   — $1052^2 \times 2384 \equiv 18^2 \times 8\ [22]$. Or $18^2 = 324 \equiv 16\ [22]$ donc $1052^2\times 2384 \equiv 16\times 8 \equiv 128 \equiv 18\ [22]$.

Exercice 2.

1. Calculer 2^{500} modulo 13 (utiliser le petit théorème de Fermat).
2. Calculer 1000^{123} modulo 17.
3. Calculer 3^{1234} modulo 15 (attention on ne peut pas appliquer le petit théorème de Fermat, étudier d'abord 3^k modulo 15 pour les petites valeurs de k).

Indications 2.

1. Le petit théorème de Fermat nous dit que $2^{12} \equiv 1\ [13]$, il faut ensuite écrire $500 = 12\times ? + ?$.
2. Commencer par simplifier le calcul en réduisant $1000\ [17]$.

Correction 2.

1. — 13 est un nombre premier (et ne divise pas 2), alors le petit théorème de Fermat nous dit que $2^{12} \equiv 1\ [13]$. Ainsi les puissances sont périodiques de période 12 : $2^0 \equiv 1\ [13]$, $2^{12} \equiv 1\ [13]$, $2^{24} \equiv 1\ [13]$, $2^{36} \equiv 1\ [13]$,...
   — Il s'agit maintenant d'approcher 500 au plus près par un multiple de 12, on effectue donc la division euclidienne de 500 par 12 :
   $$500 = 12 \times 41 + 8$$
   Ainsi $500 = 492 + 8$ où 492 est un multiple de 12.
   — On peut maintenant réduire 2^{500} modulo 13 :
   $$2^{500} = 2^{492+8} = 2^{492} \times 2^8 \equiv 1 \times 2^8\ [13]$$
   — Il reste à calculer 2^8 modulo 13. $2^8 = 256 \equiv 9\ [13]$. Ainsi
   $$2^{500} \equiv 1 \times 9 \equiv 9\ [13].$$

2. — On commence par réduire 1000 modulo 17, comme $1000 = 17 \times 58 + 14$ alors $1000 \equiv 14\ [17]$. On sait que si $a \equiv b\ [n]$ alors $a^k \equiv b^k\ [n]$ donc $1000^k \equiv 14^k\ [17]$. On va donc calculer $14^{123}\ [17]$.
   — Le petit théorème de Fermat nous dit que $14^{16} \equiv 1\ [17]$ car 17 est un nombre premier. On obtient donc aussi $14^{32} \equiv 1\ [17]$, $14^{48} \equiv 1\ [17]$,...
   — On cherche le multiple de 16 le plus proche en dessous de 123, comme $123 = 16 \times 7 + 11$ alors $123 = 112 + 11$ où 112 est un multiple de 16. Ainsi :
   $$14^{123} = 14^{112+11} = 14^{112} \times 14^{11} \equiv 1 \times 14^{11}\ [17].$$
   — Il reste à calculer 14^{11} modulo 17. Pour éviter de faire des calculs avec des entiers trop gros, on calcule les puissances successives de 14 et on réduit modulo 17 à chaque étape :
   $$\begin{gathered} 14^1 \equiv 14\ [17] \\ 14^2 = 196 \equiv 9\ [17] \\ 14^3 = 14 \times 14^2 \equiv 14 \times 9 \equiv 126 \equiv 7\ [17] \\ 14^4 = 14 \times 14^3 \equiv 14 \times 7 \equiv 98 \equiv 13\ [17] \\ 14^5 = 14 \times 14^4 \equiv 14 \times 13 \equiv 182 \equiv 12\ [17] \\ \cdots \\ 14^{11} = 14 \times 14^{10} \equiv 10\ [17] \end{gathered}$$
   — Conclusion : $1000^{123} \equiv 14^{123} \equiv 14^{11} \equiv 10\ [17]$.

3. On ne peut pas appliquer le petit théorème de Fermat car 15 n'est pas pas un nombre premier. On commence donc par étudier $3^k \equiv 1\ [15]$ pour les petites valeurs de k :

k	3^k	$3^k\ [15]$
1	3	3
2	9	9
3	27	12
4	81	6
5	243	3
6	729	9
7	2187	12
8	6561	6
9	19683	3

On voit apparaître une période de longueur 4 (même si on n'obtient pas 1 comme résultat) : par exemple si l'exposant est congru à 1 modulo 4 (i.e. $k = 1, 5, 9, \ldots$) :

$$3^1 \equiv 3\,[15] \qquad 3^5 \equiv 3\,[15] \qquad 3^9 \equiv 3\,[15] \qquad \ldots$$

Si l'exposant est congru à 2 modulo 4 (i.e. $k = 2, 6, 10, \ldots$) :

$$3^2 \equiv 9\,[15] \qquad 3^6 \equiv 9\,[15] \qquad 3^{10} \equiv 9\,[15] \qquad \ldots$$

Dans notre cas l'exposant est $k = 1234$. On écrit alors $1234 = 4 \times 308 + 2$. Ainsi $k \equiv 2\,[4]$, donc

$$3^{1234} \equiv 9\,[15].$$

Exercice 3.

Les deux premières questions reprennent un exercice précédent et montrent l'efficacité des congruences pour les calculs.

1. Soit $n = p^2$ le carré d'un entier. Déterminer les valeurs possibles de n modulo 4.
2. Montrer que si n est un entier naturel somme de deux carrés d'entiers alors n modulo 4 n'est jamais égal à 3.
3. Soit $n = p^2$ le carré d'un entier. Déterminer les valeurs possibles de n modulo 8.
4. Montrer que si n est un entier naturel somme de trois carrés d'entiers alors n modulo 8 n'est jamais égal à 7.

Indications 3.

Modulo 4, p est congru à 0, 1, 2 ou 3, donc p^2...

Correction 3.

1. Soit $n = p^2$. Modulo 4, p est congru à 0, 1, 2 ou 3. Calculons alors la valeur de p^2 modulo 4 dans chacun de ces cas.

$p\,[4]$	$p^2\,[4]$
0	0
1	1
2	$2^2 \equiv 4 \equiv 0$
3	$3^2 \equiv 9 \equiv 1$

   Conclusion : pour $n = p^2$ alors $n\,[4]$ est congru soit à 0, soit à 1 (mais ne peut pas être 2, ni 3).

2. Soit $n = p^2 + q^2$. D'après la question précédente p^2 et q^2 sont congrus à 0 ou 1 modulo 4. Il y a donc 4 cas possibles, mais dans tous les cas la somme ne peut pas faire 3 ($0+0=0$, $0+1=1$, $1+0=1$, $1+1=2$).
3. Soit $n = p^2$. Modulo 8, p est congru à l'un des entiers $0, 1, \ldots, 7$. Calculons la valeur de p^2 modulo 8 dans chacun de ces cas.

$p\,[8]$	$p^2\,[8]$
0	0
1	1
2	4
3	$3^2 \equiv 9 \equiv 1$
4	$4^2 \equiv 16 \equiv 0$
5	$5^2 \equiv 25 \equiv 1$
6	$6^2 \equiv 36 \equiv 0$
7	$7^2 \equiv 49 \equiv 1$

Conclusion : pour $n = p^2$ alors $n\,[8]$ est congru soit à 0, soit à 1, soit à 4 (mais ne peut pas être 2, 3, 5, 6, ni 7).

4. Soit $n = p^2 + q^2 + r^2$. Chaque carré vaut 0 ou 1 ou 4 modulo 8. La somme de trois tels termes ne peut pas faire 7 (toutes les autres valeurs de 0 à 6 sont possibles). Donc n n'est pas congru à 7 modulo 8.

Exercice 4.

1. Montrer que $p = 101$ est un nombre premier.
2. Soit a un entier avec $1 \leqslant a < p$. Montrer que $\mathrm{pgcd}(a, p) = 1$.
3. Écrire le théorème de Bézout pour le pgcd précédent ; en déduire qu'il existe $u \in \mathbb{Z}$ tel que $au \equiv 1\,[p]$. *Un tel u s'appelle un **inverse** de a modulo p.*
4. Trouver un inverse de $a = 15$ modulo $p = 101$.
5. Trouver une solution de l'équation d'inconnue x (un entier) : $15x \equiv 7\,[101]$.
6. Reprendre tout l'exercice avec $p = 103$.

Indications 4.

Ici le théorème de Bézout s'écrit $au + pv = 1$. Le u est l'inverse cherché.

Correction 4.

1. $p = 101$ n'est pas divisible par $k = 2, 3, 5, 7$ qui sont les diviseurs premiers possibles $\leqslant \sqrt{101}$, donc c'est un nombre premier.
2. Si d est un diviseur commun à a et à p alors $d = 1$ ou $d = p$ car p est un nombre premier. Mais comme d doit être plus petit que a (et $a < p$) alors $d < p$. Conclusion : $d = 1$, ce qui prouve que a et p sont premiers entre eux.
3. Le théorème de Bézout avec a, $b = p$ et $d = \mathrm{pgcd}(a, p) = 1$ donne l'existence de deux entiers u, v tels que :
$$au + pv = 1.$$
Autrement dit $au - 1 = -pv$. Ce qui implique que $au \equiv 1\,[p]$.
4. Pour $a = 15$ et $p = 101$ les coefficients de Bézout u, v sont obtenus par remontée de l'algorithme d'Euclide. Après calculs on trouve :
$$a \times 27 + 101 \times (-4) = 1.$$
Donc avec $u = 27$ on a $au \equiv 1\,[101]$ c'est-à-dire $15 \times 27 \equiv 1\,[101]$. 27 est donc un inverse de 15 modulo 101.
5. Toujours avec $a = 15$, l'équation à résoudre est $ax \equiv 7\,[101]$. On a envie de diviser par a pour trouver x. Pour l'écrire de façon correcte, on va plutôt multiplier à gauche et droite par l'inverse de a (c'est-à-dire par $u = 27$), pour obtenir une équation équivalente :
$$(au)x \equiv 7u\,[101]$$
Mais $au \equiv 1\,[101]$ (par construction de u), donc on obtient
$$x \equiv 7u\,[101]$$
Ici $u = 27$ donc $x = 7 \times 27 = 189 \equiv 88\,[101]$. On vérifie facilement qu'avec $x = 88$ on a bien $15 \times 88 \equiv 7\,[101]$. C'est aussi ce que l'on retrouve si l'on part de la relation de Bézout (trouvée à la question 4) et qu'on la multiplie par 7.

6. Avec $a = 15$ et $p = 103$ on trouve $au + pv = 1$ pour $u = -48$, $v = 7$. Un inverse de 15 modulo 103 est donc $u = -48$. Si on préfère un entier positif on peut prendre $u' = 55$ (qui est congru à -48 modulo 103). Une solution de l'équation $15x \equiv 7\,[103]$ est donc $x = 76$, car $7u = 7 \times (-48) = -336 \equiv 76\,[103]$.

Exercice 5.

Les **nombres de Fermat** F_n sont les entiers définis pour $n \in \mathbb{N}$ par

$$F_n = 2^{2^n} + 1$$

1. Montrer que pour tout entier naturel n, on a $F_{n+1} = (F_n - 1)^2 + 1$.
2. Démontrer que pour $n \geqslant 2$, l'écriture décimale des nombres de Fermat (F_n) se termine par le chiffre 7.

Indications 5.

On rappelle que 2^{2^n} signifie $2^{(2^n)}$. Utiliser un raisonnement par récurrence et les congruences modulo 10.

Correction 5.

1. On calcule :
$$(F_n - 1)^2 + 1 = (2^{2^n})^2 + 1 = 2^{2^n \times 2} + 1 = 2^{2^{n+1}} + 1 = F_{n+1}$$
2. L'écriture décimale d'un entier N se termine par le chiffre 7 si et seulement si on a $N \equiv 7\,[10]$. Démontrons donc par récurrence la proposition : "$F_n \equiv 7\,[10]$", pour $n \geqslant 2$.
Initialisation. Pour $n = 2$, on a :
$$F_2 = 2^{2^2} + 1 = 16 + 1 = 17 \equiv 7\,[10]$$
Hérédité. Supposons que pour un entier $n \geqslant 2$, on ait en effet $F_n \equiv 7\,[10]$. On a alors :
$$F_{n+1} = (F_n - 1)^2 + 1 \equiv (7 - 1)^2 + 1 = 36 + 1 = 37 \equiv 7\,[10]$$
Ainsi la proposition est bien héréditaire.
Conclusion. On a bien démontré par récurrence que tous les nombres de Fermat F_n, pour $n \geqslant 2$, sont congrus à 7 modulo 10 : leur écriture décimale se termine donc par le chiffre 7.