

## Arithmétique de base

Programme : Nombres entiers, partie entière, divisibilité, division euclidienne, décomposition en base  $b$ , pgcd, ppcm, algorithme d'Euclide, théorème de Bezout, lemme de Gauss. Pour le détail du cours, voir le poly d'Arithmétique d'Animath.

### - Énoncés des exercices vus en cours -

**Exercice 1** Soit  $m$  un entier strictement positif, et soient  $r_1, \dots, r_m$  des nombres rationnels tels que  $r_1 + \dots + r_m = 1$ . Quelles sont les valeurs minimale et maximale atteintes par la fonction  $f(n) = n - \sum_{i=1}^m [r_i n]$  pour  $n \in \mathbb{N}^*$  ?

**Exercice 2** Montrer que pour tout  $n$ ,  $n^2 + n$  est divisible par 2.

**Exercice 3**

1. Déterminer le reste de la division euclidienne de  $9^{100}$  par 8.
2. Trouver le dernier chiffre de  $2012^{2012}$ .

**Exercice 4** (Problème des poids de Bachet) On dispose d'une balance à deux plateaux avec laquelle on veut pouvoir peser tout objet d'une masse entière comprise entre 1 et 40kg. Quel est le nombre minimal de poids de masse entière qui sont nécessaires à cela :

1. si on ne peut poser ces poids que sur un plateau de la balance ?
2. si on peut les poser sur les deux plateaux ?

**Exercice 5** Montrer que pour tout  $n$  entier la fraction  $\frac{21n+4}{14n+3}$  est irréductible.

**Exercice 6** Soient  $m, n$  des entiers strictement positifs. Déterminer le pgcd de

$\underbrace{1 \dots 1}_{m \text{ chiffres}}$  et de  $\underbrace{1 \dots 1}_{n \text{ chiffres}}$

**Exercice 7** Déterminer le pgcd de tous les nombres de la forme

$$(a - b)(b - c)(c - d)(d - a)(a - c)(b - d)$$

où  $a, b, c, d$  sont des entiers.

**Exercice 8** Soit  $p$  un nombre premier,  $k$  un entier compris entre 1 et  $p - 1$ . Montrer que  $p$  divise  $\binom{p}{k} = \frac{p!}{k!(p-k)!}$  (qui, on le rappelle, est entier).

- Corrigé -

Solution de l'exercice 1 Commençons par encadrer  $f(n)$  pour avoir une idée des extréma : pour tout  $i$ ,  $r_i n - 1 < [r_i n] \leq r_i n$ , d'où  $n - m < \sum_{i=1}^m r_i n \leq n$ , d'où  $0 \leq f(n) \leq m - 1$ . Nous allons montrer qu'en fait les valeurs 0 et  $m - 1$  sont atteintes. Soit  $A$  un dénominateur commun pour tous les  $r_i$  (on peut avoir l'idée de le considérer car il réalise l'égalité dans la toute première inégalité écrite), alors puisque  $r_i A$  est entier pour tout  $i$ ,  $f(A) = 0$ . D'autre part,  $f(A - 1) = A - 1 - \sum_{i=1}^m [r_i(A - 1)] = A - 1 - \sum_{i=1}^m (r_i A - 1) = m - 1$ .

Solution de l'exercice 2

Méthode 1 :  $n$  et  $n^2$  sont de la même parité, donc leur somme est paire.

Méthode 2 :  $n^2 + n = n(n + 1)$  est le produit de deux entiers consécutifs, dont un est nécessairement pair.

Solution de l'exercice 3

1. Puisque  $9 = 1 + 8$ , en développant on a  $9^{100} = (1 + 8)^{100} = 1 + 8A$  où  $A$  est un entier. Donc le reste est 1.
2. Remarquons d'abord que cela revient à chercher le reste de la division euclidienne de  $2012^{2012}$  par 10, qui est le même que celui de  $2^{2012}$ . Or les derniers chiffres successifs des puissances de deux sont 2, 4, 8, 6, 2..., périodiques de période 4, et  $2^n$  avec  $n$  divisible par 4 a toujours pour dernier chiffre 6, donc puisque 2012 est divisible par 4, la réponse est 6.

Solution de l'exercice 4

1. On est obligé de prendre un poids de 1kg pour pouvoir peser 1kg. Ensuite, pour pouvoir peser 2kg, on a deux possibilités : soit ajouter un autre poids de 1kg, soit ajouter un poids de 2kg. La 2ème solution est plus avantageuse car elle permet en même temps de peser 3kg. De même, pour peser 4kg, il est plus avantageux de choisir un poids de 4kg plutôt qu'un poids de 1 ou de 2kg, car cela permet de peser tout jusqu'à 7kg. Pour la

même raison, ensuite on choisit 8kg. On remarque que le choix de poids qui apparait est en fait la suite des puissances de deux. Pour en comprendre la raison, reformulons un peu le problème : nous voulons des entiers  $p_1, \dots, p_k$  (les poids) tels que tout entier  $n$  entre 1 et 40 puisse s'écrire  $n = e_1 p_1 + \dots + e_k p_k$  avec  $e_i \in \{0, 1\}$  ( $e_i = 1$  si le poids est utilisé pour peser  $n$ ,  $e_i = 0$  sinon) de la manière « la plus unique possible », car pour avoir un nombre de poids optimal, il faut que chaque pesée puisse se faire de peu de façons différentes, voire d'une unique façon. Or nous venons de voir une telle possibilité de décomposition, la décomposition en base 2, qui est même unique ! Prendre donc des poids égaux aux puissances de deux inférieures à 40, à savoir 1, 2, 4, 8, 16, 32, répond au problème. Mieux, avec cela on peut même mesurer tous les poids jusqu'à  $1 + \dots + 32 = 2^6 - 1 = 63$ .

2. Commençons de même par trouver à la main les premiers poids qu'il faut, en commençant avec un poids de 1kg. Pour peser 2kg, on pourrait prendre 2, mais aussi 3, et c'est cette solution-là qui s'avère la plus avantageuse, car elle permet aussi de peser 4. D'autre part, on ne peut prendre 4 directement car avec 1 et 4 on ne peut peser 2. On choisit donc 1 et 3. De même, la meilleure solution ensuite est de choisir 9, car cela permet de couvrir tous les poids de 5 à 13. On voit que cette fois-ci, les poids qui apparaissent sont des puissances de 3. Pour expliquer cela, écrivons la décomposition unique en base 3 d'un nombre  $n$  :  $n = e'_0 3^0 + \dots + e'_k 3^k$  avec des  $e'_i \in \{0, 1, 2\}$ . Comme dans notre problème il nous faut des coefficients dans  $\{-1, 0, 1\}$  (pour indiquer si un poids est utilisé, et si oui, de quel côté de la balance), nous allons appliquer à notre décomposition l'algorithme suivant : remplacer tous les termes de la forme  $2 \times 3^k$  par  $3^{k+1} - 3^k$ , puis regrouper par puissances de 3 et simplifier, et recommencer jusqu'à n'avoir que des coefficients -1, 0 ou 1. L'algorithme termine nécessairement car de nouveaux 2 ne peuvent apparaître que devant des puissances de 3 de plus en plus grandes. Sur un exemple, cela donne :

$$\begin{aligned}
 17 &= 1 \times 3^2 + 2 \times 3 + 2 \times 1 \\
 &= 1 \times 3^2 + 3^2 - 3 + 3 - 1 \\
 &= 2 \times 3^2 - 1 \\
 &= 3^3 - 3^2 - 1
 \end{aligned}$$

Ainsi, tout entier  $n$  s'écrit comme somme de puissances de 3 avec des coefficients  $-1, 0, 1$ , et on prouve que celle-ci est unique de la même manière que la décomposition en base 3 l'est. Donc les puissances de 3 donnent

bien une solution à notre problème, et il suffit de quatre poids 1, 3, 9, 27, pour peser tous les poids entre 1 et 40, et cette fois-ci, ce système de poids est même optimal au sens où il ne peut peser que ces poids-là (41 ne peut être pesé).

Solution de l'exercice 5  $2(21n+4) - 3(14n+3) = -1$ , donc  $\text{pgcd}(21n+4, 14n+3) = 1$ .

Solution de l'exercice 6 Supposons que  $m < n$  et écrivons  $n = mq + r$  la division euclidienne de  $n$  par  $m$ . Alors la division euclidienne de  $\underbrace{1\dots1}_{n \text{ chiffres}}$  par  $\underbrace{1\dots1}_{m \text{ chiffres}}$  s'écrit

$$\underbrace{1\dots1}_{n \text{ chiffres}} = \underbrace{1\dots1}_{m \text{ chiffres}} (10^{m(q-1)+r} + \dots + 10^{m+r} + 10^r) + \underbrace{1\dots1}_{r \text{ chiffres}}.$$

En appliquant l'algorithme d'Euclide on voit donc que le pgcd cherché est  $\underbrace{1\dots1}_{\text{pgcd}(m,n)}.$

Solution de l'exercice 7 Nous allons montrer que le pgcd cherché est 12. En effet, par le principe des tiroirs, parmi  $a, b, c, d$  il y a deux nombres congrus modulo 3, et donc leur différence est divisible par 3. Maintenant si on regarde modulo 4, on a deux possibilités : soit il y a deux nombres parmi  $a, b, c, d$  congrus modulo 4, et à ce moment-là leur différence est divisible par 4, soit  $a, b, c, d$  sont distincts modulo 4. Mais dans ce dernier cas, deux d'entre eux sont pairs et deux sont impairs, donc le produit qui nous intéresse a deux facteurs pairs. Ainsi, dans tous les cas, ce produit est divisible par 3 et par 4, donc par 12.

D'autre part, prenant  $a = 0, b = 1, c = 2, d = 3$ , le produit obtenu vaut  $-12$  donc le diviseur que nous avons trouvé est bien le pgcd.

Solution de l'exercice 8 Il suffit pour cela de prouver que  $k!(p-k)!$  divise  $(p-1)!$ , sachant que l'on sait qu'il divise  $p!$ . Or  $p$  est premier avec  $k!$  et avec  $(p-k)!$  (on a bien  $1 \leq k \leq p-1$ ), donc  $k!(p-k)!$  est premier avec  $p$ , ce qui conclut.