TD1. Divisibilité, congruences, PGCD dans $\mathbb{Z}$

1 Divisibilité

Exercice 1. Faire la liste de tous les entiers relatifs qui divisent 12.

Exercice 2. Montrer par récurrence sur n que pour tout entier impair a et tout entier naturel n, le nombre 2^{n+1} divise $a^{2^n} - 1$.

2 Division euclidienne

Exercice 3. Ecrire les divisions euclidiennes de 23 par 7, de -23 par 7, de 23 par -7 et de -23 par -7.

Exercice 4. Déterminer tous les entiers naturels qui, dans la division euclidienne par 3, donnent un quotient égal au double du reste.

Exercice 5. On fait la division euclidienne d'un entier n par 137 et par 143. Les quotients sont égaux et les restes respectifs sont 131 et 5. Quel est cet entier n ?

3 Congruences

Exercice 6. On utilise dans cet exercice $\{0, 1, \ldots, n-1\}$ comme système de représentants des classes modulo n, pour chaque $n \in \mathbb{N}^*$. *Réduire* un nombre modulo n, c'est donner, parmi $0, 1, \ldots, n-1$, le représentant de sa classe.

a. Réduire modulo 3 les nombres suivants :

$$10\,;15\,;123\,;157\,;145771$$

b. Réduire modulo 12 :

$$28\,;178$$

Exercice 7. Montrer que pour tout $n \in \mathbb{Z}$, 3 divise $n(n+1)(n+2)$.

Exercice 8. Montrer par récurrence sur n que pour tout entier naturel n, on a $n^3 \equiv n \mod 3$.

Exercice 9. RIB. Le numéro N d'un compte bancaire au format RIB comporte 23 chiffres et se décompose comme suit.

$$N = \underbrace{r_{22}r_{21}r_{20}r_{19}r_{18}}_{B}\ \underbrace{r_{17}r_{16}r_{15}r_{14}r_{13}}_{G}\ \underbrace{r_{12}r_{11}r_{10}r_9r_8r_7r_6r_5r_4r_3r_2}_{C}\ \underbrace{r_1r_0}_{K}$$

- l'entier B est le code banque,
- l'entier G le code guichet,
- l'entier C est le numéro du compte
- et K s'appelle la clé du RIB.

La clé K, qui comporte toujours deux chiffres, est telle que $N \equiv 0 \mod 97$. Retrouver la clé manquante dans le RIB suivant :

11803 00793 403194511227 ??

Exercice 10. "Relèvements"

1. Quelles sont les classes de congruences modulo 2 possibles pour les entiers congrus à 3 mod 4 ? Et pour ceux congrus à 1 mod 8 ?

2. Quelles sont les classes de congruences modulo 4 possibles pour les entiers congrus à 1 mod 2 ?

3. Quelles sont les classes de congruences modulo 8 possibles pour les entiers congrus à 1 mod 2 ?

Exercice 11. Critères de divisibilité

1. Rappeler la classe de congruence de 10 respectivement modulo 3, modulo 9, modulo 11.

2. Soit a un entier naturel, notons $a_{n-1}, \ldots, a_0$ les chiffres de l'écriture en base 10 de a, ainsi $a = \sum_{i=0}^{n-1} a_i \times 10^i$.

a. Démontrer que $3|a$ si et seulement si $3|\sum_{i=0}^{n-1} a_i$ (critère de divisibilité par 3).

b. Démontrer que $9|a$ si et seulement si $9|\sum_{i=0}^{n-1} a_i$ (critère de divisibilité par 9).

c. Démontrer que $11|a$ si et seulement si $11|\sum_{i=0}^{n-1} (-1)^i a_i$ (critère de divisibilité par 11).

d. Parmi les nombres suivants, lesquels sont divisibles par 11 ?

$$1111111\,;11111111\,;143\,;1232\,;1524334251$$

e. Donner d'autres exemples de nombres entiers naturels "palindromes" divisibles par 11.

Exercice 12. "Preuve par 9"

Nos grands-parents, lorsqu'ils faisaient une multiplication à l'école primaire, vérifiaient leur calcul en faisant la "preuve par 9". Voici un exemple :
Après avoir posé, à la main, la multiplication 17×35, et trouvé 595, on fait les calculs suivants :

On "réduit" les opérandes :

- $1 + 7 = 8$
- $3 + 5 = 8$
- et $8 \times 8 = 64$ se "réduit" en $6 + 4 = 10$ qui se "réduit" en $1 + 0 = 1$.

Le résultat trouvé, 595, se réduit en $5 + 9 + 5 = 19$
qui se réduit en $1 + 9 = 10$
et encore en $1 + 0 = 1$.

La réduction du côté opérandes étant égale à la réduction du côté résultat, nos grands-parents concluaient que leur calcul était juste.

1. De quelle réduction s'agit-il ?

2. Ma grand-mère a trouvé 559. Que donne sa "preuve par 9" ?

3. Quels sont les raisonnements corrects ? :

- si le calcul de la multiplication est juste, alors la preuve par 9 donne la même réduction côté opérandes et côté résultat.
- si la preuve par 9 donne la même réduction côté opérandes et côté résultat, alors le calcul de la multiplication est juste.
- si le calcul de la multiplication est faux, alors la preuve par 9 ne donne pas la même réduction des deux côtés.
- si la preuve par 9 ne donne pas la même réduction des deux côtés, alors le calcul de la multiplication est faux.

Exercice 13. Soit n un entier relatif non multiple de 5. Montrer que 5 divise $(n^2-1)(n^2-4)$

Exercice 14. Le but de l'exercice est de réduire $100^{1000} \mod 13$.

1. Montrer que la suite des réductions modulo 13 des puissances de 9 est périodique.

2. Y a-t-il une puissance de 9 qui vaut $1 \mod 13$?

3. En déduire $100^{1000} \mod 13$.

Exercice 15.

1. Montrer que le carré de tout nombre impair est congru à $1 \mod 8$.

2. Montrer que le carré de tout nombre pair est congru à 0 ou $4 \mod 8$.

3. Soient a, b, c des entiers impairs.
Déterminer le reste modulo 8 de $a^2+b^2+c^2$ et de $2(ab+bc+ca)$.

4. En déduire que ni $a^2+b^2+c^2$ ni $ab+bc+ca$ ne sont des carrés d'entiers.

4 PGCD, Algorithme d'Euclide

Exercice 16. Rappeler pourquoi faire les divisions euclidiennes successives de l'algorithme d'Euclide fournit le pgcd de deux entiers a et b.

Exercice 17. Calculer le pgcd des nombres suivants en appliquant l'algorithme d'Euclide.

a. 525 et 275

b. 1023 et 909

c. 195 et 143.

Exercice 18.

1. Montrer que deux entiers consécutifs non nuls sont toujours premiers entre eux.

2. Soient a et b des entiers naturels non nuls premiers entre eux. Montrer que $\text{pgcd}(a+b, a-b)$ vaut 1 ou 2. Donner un exemple pour chacun des cas.

3. Soit k un entier. Montrer que $2k+1$ et $9k+4$ sont premiers entre eux.

Exercice 19. Idées sur la complexité de l'algorithme d'Euclide
Un algorithme est fait pour être programmé. Plusieurs questions se posent :

- L'algorithme se termine-t-il dans tous les cas ?
- Quelle est sa complexité, c'est-à-dire le nombre d'opérations à effectuer ?

Dans cet exercice, on s'intéresse au nombre de divisions euclidiennes à faire dans l'algorithme d'Euclide, on en cherche un majorant en la taille des opérandes.

1. Rappeler pourquoi cet algorithme se termine dans tous les cas.

2. Soient a, b des entiers strictement positifs, avec $a > b$. Notons $r_1, r_2, \ldots, r_n, r_{n+1} = 0$ les restes successifs dans l'algorithme d'Euclide pour chercher $\text{pgcd}(a, b)$. Le but de cette question est de montrer qu'en deux divisions, le reste est au moins divisé par 2. On pose $r_0 = b$.

a. Montrer que pour tout $i \geqslant 0$ tel que $i + 2 \leqslant n + 1$:
- si $r_{i+1} \leqslant r_i/2$, alors $r_{i+2} < r_i/2$.
- sinon, $r_{i+2} = r_i - r_{i+1}$, donc on a aussi $r_{i+2} < r_i/2$.

b. En déduire que pour tout $i \geqslant 0$ tel que $2i \leqslant n + 1$, on a $r_{2i} < \dfrac{b}{2^i}$.

3. a. Soit k le plus petit entier tel que $\dfrac{b}{2^k} < 2$.

b. Montrer que $k = E[\log_2(b)]$ et que $E[\log_2(b)]$ est le nombre de bits dans l'écriture binaire de b.

c. Montrer que

a. si $2k \leqslant n + 1$, alors on détermine le pgcd en $2k$ divisions euclidiennes,

b. sinon, on a besoin de moins de $2k$ divisions euclidiennes.

4. Conclure.