IT-University
Cours d'arithmétique

Table des matières

1 Arithmétique sur $\mathbb{Z}$

Dans toute la suite $\mathbb{N}$ et $\mathbb{Z}$ désigneront respectivement l'ensemble des entiers naturels (y compris zéro) et l'ensemble des entiers relatifs. On rappel aussi qu'on dispose deux lois de composition sur $\mathbb{Z}$, qui à tout entiers x et y, `la somme` $x + y$ et `le produit` xy. Pour tout entier x, on notera par $|x|$ la valeur absolue de x, i.e, le plus grand entre x et $-x$.

Theorem 1.1 (**Propriété Fondamental de l'Arithmétique**). *Toute partie non vide de* $\mathbb{N}$ *admet un plus petit élément.*

Preuve. On a déjà une preuve en cours d'analyse. □

Il est important de noter qu'on peut avoir presque tout les résultats importants en arithmétique élémentaire à partir de cette propriété. Donc, le titre de "fondamental" qu'on lui donne est bien justifié.

1.1 Division euclidienne

Theorem 1.2. *Soient a et b deux entiers tels que $b \neq 0$. Il existe un* **unique** *couple $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ tel que l'on ait:*

- $a = qb + r$;
- $0 \leq r < |b|$.

Définition 1.3. *Soient a et b deux éléments de $\mathbb{Z}$. On dit que b* ***divise*** *a ou que b est un* ***diviseur*** *de a, ou bien encore que a est un* ***multiple*** *de b s'il existe k entier tel que*

$$a = bk.$$

Si b est non nul, cette condition signifie que le reste de la division euclidienne de a par b est nul.

Exercice 1.1.

1. Quels sont le quotient et le reste de la division euclidienne:
   - de 456765 par 641;
   - de -456765 par 641;
   - de 456765 par -641.
2. Soient a et n deux entiers naturels non nuls. Montrer que $a - 1$ divise $a^n - 1$.
3. Déterminer tous les entiers naturels n tels que $n + 1$ divise $n^2 + 1$.

1.2 Sur les nombres premiers

Définition 1.4. *On appelle* ***nombre premier*** *tout entier $p \geq 2$ dont les seuls diviseurs positifs sont 1 et p.*

Exemples 1.5. *Donner la liste des nombres premiers inférieurs à 100.*

Dans toute la suite, notons par $\mathbb{P}$ l'ensemble des nombres premiers.

Theorem 1.6. *L'ensemble $\mathbb{P}$ des nombres premiers est infini.*

Preuve. □

Lemme 1.7. *Soit p un entier supérieur à 2. Alors, p est premier si et seulement si p n'est pas le produit de deux entiers strictement plus grands que 1.*

Preuve. Exercice. □

Lemme 1.8. *Tout entier supérieur ou égal à 2 est un produit de nombres premiers. En particulier, tout entier $n \geq 2$ possède un diviseur premier.*

Preuve. Procéder par récurrence, puis utiliser le lemme précédent. □

Lemme 1.9 (Lemme d'Euclide)**.** *Si un nombre premier divise un produit d'entiers relatifs, il divise l'un de ces entiers. En particulier, si un nombre premier divise un produit de nombres premiers, il est égal à l'un d'eux.*

Theorem 1.10 (**Théorème Fondamental de l'Arithmétique**)**.** *Tout entier $n \geq 2$ s'écrit de façon unique sous la forme:*

$$n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}, \tag{1}$$

où les n_i sont des entiers naturels non nuls, et où les p_i sont des nombres premiers vérifiant $p_{i-1} < p_i$ pour tout $i = 2, \ldots, r$. On dit que l'égalité (1) est la décomposition de n en produit de nombres premiers.

Preuve. □

Maintenant, pour qu'on puisse factoriser un entier, une question naturel se pose: `Comment décider si un entier naturel` $n \geq 2$ `est un nombre premier ou non?`
Il existe de nombreux tests permettant parfois de reconnaître si un entier est premier ou non. C'est toute une théorie qu'on appelle tests de primalité. Il sera difficile pour nous d'aborder ce sujet en première année. Par contre, le résultat suivant est utile:

Proposition 1.11. *Soit n un entier supérieure ou égal à 2. Si n n'est pas premier, alors n possède un diviseur premier p vérifiant l'inégalité $p^2 \leq n$.*

Preuve. Exercice. □

Exemples 1.12. *En utilisant le résultat précédent, on va montrer que $n = 641$ est premier. Si 641 n'était pas premier, n admet un diviseur premier inférieur à $\sqrt{641} \leq 26$. Les nombres premiers plus petits que 25 sont 2, 3, 5, 7, 11, 13, 17, 19 et 23. On vérifiera alors qu'aucun de ces nombres ne divise 641 en utilisant le théorème de la division euclidienne.*

Soit N un entier naturel supérieur ou égal à 2. Il existe un procéder pour déterminer tout les nombres premiers inférieurs à N. Le plus connu s'appelle `le crible d'Eratosthène.` Le procéder de criblage utilise seulement l'opération de multiplication d'entiers. Le principe est le suivant:

- On écrit d'abord dans un tableau tous les entiers jusqu'à N;
- Puisque 2 est un nombre premier, On raye ensuite tous les multiples de 2 du tableau, autres que 2;
- On garde le premier plus petit entier qui n'a pas encore rayé (qui est 3 en cet stade). Puis, on raye tous les multiples de 3, autres que 3;
- A chaque étape on raye tous les multiples du plus petit entier qui n'a pas encore été rayé;
- On arrête si on avait tous cribler tout les entiers inférieurs à $\sqrt{N}$. Tout les restes sont des nombres premiers.

Par exemple, si on veut avoir la liste de nombres premiers inférieurs à 100, on raye tous les multiples de 2, 3, 5 et 7 (qui sont les nombres premiers inférieurs à $\sqrt{100} = 10$). On peut aussi, bien évidement, utiliser ce crible en testant si un nombre est premier ou non.

Exercice 1.2.

1. Montrer que 3571 est un nombre premier.
2. Montrer que si $2^n - 1$ est un nombre premier, il en est de même de n. Un nombre de la forme $2^n - 1$, avec n premier, s'appelle un nombre de Mersenne.
3. Montrer que si $2^n + 1$ est premier, alors n est une puissance de 2. Un nombre de la forme $2^{2^n} + 1$ s'appelle un nombre de Fermat. Montrer que pour $n = 1, 2, 3$ et 4 le nombre $2^{2^n} + 1$ est premier. Mais par contre, $2^{32} + 1$ n'est pas premier.
4. Démontrer que l'entier $1 + 2 + 2^2 + 2^3 + \ldots + 2^{2019}$ n'est pas premier.
5. Implémenter sur C ou C++ le crible d'Eratosthène. En déduire le 100001 ième nombre premier. Donner la liste de nombres premiers inférieurs à 2000000.
6. Trouver le plus grand facteur premier du nombre 600851475143.

1.3 Valuation p-adique d'un entier

Dans cette sous-section, n et p désigneront successivement un entier relatif et un nombre premier. L'application

$$v_p : \mathbb{Z} \longrightarrow \mathbb{N} \cup \{+\infty\}$$

définie par:

i). Si l'on a $n \geq 2$, alors $v_p(n)$ est l'exposant de p dans la décomposition de n en produit de nombres premiers. Plus précisément:

- Si p ne divise pas n, on a $v_p(n) = 0$;
- Si $n = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$ est la décomposition de n en produit de nombres premiers ($n_i \geq 1$), on a:

$$v_{p_i}(n) = n_i \quad \text{pour} \quad i = 1, 2, \ldots, r.$$

ii). On pose $v_p(0) = +\infty$ et $v_p(1) = 0$;

iii). Si $n \geq 1$, on a $v_p(-n) = v_p(n)$.

est appelé `valuation p-adique`. On dit aussi $v_p(n)$ est `la valuation p-adique` de n.
Comme un exemple, Posons $n = 539000$. On a $n = 2^3 \cdot 5^3 \cdot 7^2 \cdot 11$, de sorte que l'on a $v_2(n) = 3,\ v_5(n) = 3,\ v_7(n) = 2,\ v_{11}(n) = 1$ et donc pour tout nombre premier p distinct de 2, 5, 7 et 11, on a $v_p(n) = 0$.
Ainsi, on peut écrire le Théorème Fondamental de l'Arithmétique comme suit:
Tout entier relatif n non nul s'écrit de manière unique, à l'ordre près des facteurs, sous la forme :

$$n = \epsilon \prod_{p \in \mathbb{P}} p^{v_p(n)}$$

où $\epsilon = -1$ si $n \leq -1$ et $\epsilon = 1$ si $n \geq 1$.
Il est important de noter que:

$$v_p(n) \geq 1 \quad \text{si et seulement si} \quad p \text{ divise } n.$$

Proposition 1.13. *Soient a et b deux entiers relatifs et p un nombre premier. On a:*

i). $v_p(ab) = v_p(a) + v_p(b)$;

ii). $v_p(a+b) \geq \mathrm{Min}(v_p(a), v_p(b))$. *Si de plus,* $v_p(a) \neq v_p(b)$, *on a* $v_p(a+b) = \mathrm{Min}(v_p(a), v_p(b))$;

iii). Pour que a divise b, il faut et il suffit que l'on ait $v_p(a) \leq v_p(b)$ pour tout $p \in \mathbb{P}$.

Preuve. Exercice. □

Maintenant soient a et b deux entiers non tous nuls. Considérons les entiers naturels d et m définis par:

$$d := \prod_{p\in\mathbb{P}} p^{\mathrm{Min}(v_p(a),v_p(b))}, \quad m := \prod_{p\in\mathbb{P}} p^{\mathrm{Max}(v_p(a),v_p(b))}.$$

L'entier d ainsi défini vérifie les deux propriétés suivantes:

- L'entier d est un diviseur commun à a et b;
- Tout diviseur commun à a et b divise d.

Tandis que l'entier m satisfait les deux conditions suivantes:

- L'entier m est un multiple commun à a et b;
- Tout multiple commun à a et b est un multiple de m.

Les entiers d et m sont appelés respectivement `le plus grand commun divise` et `le plus petit commum multiple` de a et b. On les note respectivement par pgcd(a, b) et ppcm(a, b).

Définition 1.14. *On dit que a et b sont premiers entre eux si* $\mathrm{pgcd}(a, b) = 1$. *Ainsi,* $\mathrm{pgcd}(a, b) = 1$ *si et seulement si pour tout $p \in \mathbb{P}$, on a* $\mathrm{Min}(v_p(a), v_p(b)) = 0$.

Exercice 1.3.

1. Calculer $v_2(10560)$. Pour tout $p \in \mathbb{P}$ calculer $v_p(196000)$.
2. En utilisant l'application valuation p-adique, démontrer que $\sqrt{2}$ n'appartient pas à l'ensemble $\mathbb{Q}$ des nombres rationnels. Soit a un nombre rationnel strictement positif. Donner une condition nécessaire et suffisante pour que $\sqrt{a}$ appartienne à $\mathbb{Q}$.
3. Soient p et q deux nombres premiers distincts. Montrer que pq divise $p^{q-1} + q^{p-1} - 1$.
4. Déterminer le pgcd et le ppcm de 2800 et 120.
5. Trouver tous les couples d'entiers naturels (a, b) pour lesquels on a $\mathrm{pgcd}(a, b) = 5$ et $\mathrm{ppcm}(a, b) = 8160$.
6. Soient a et b deux entiers non tous nuls. Notons respectivement par d et m leur $\mathring{pgcd}$ et leur $\mathring{ppcm}$. Montrer que:
   i). Les entiers $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux;
   ii). $dm = |ab|$;

1.4 L'Algorithme d'Euclide et L'équation $ax + by = c$

Dans cet sous-section, considérons deux entiers a et b tels que $a \geq b$. Notre but est de donner en détail un algorithme (utilisant seulement la division euclidienne) pour déterminer non seulement le pgcd de a et b, mais aussi de résoudre l'équation du type $ax + by = c$ dans $\mathbb{Z}^2$ où c est un entier donné.
Le théorème suivant est fondamental:

Theorem 1.15 (**Théorème de Bézout**). *Il existe deux entiers relatifs u et v tel que l'on ait:*

$$\text{pgcd}(a, b) = au + bv.$$

De plus, les entiers a et b sont premiers entre eux si et seulement si il existe deux entiers u et v tels que $au + bv = 1$.

Considérons maintenant les trois suites $(r_i), (u_i)$ et v_i associées à a et b définies comme suit:

- $r_0 = a$ et $r_1 = b$. Pour $i \geq 2$, on définit r_i comme étant le reste de la division euclidienne de r_{i-2} par r_{i-1};
- $u_0 = 1$ et $u_1 = 0$. Pour $i \geq 2$, on pose $u_i = u_{i-2} - u_{i-1}q_{i-1}$ où q_{i-1} est le quotient de la division euclidienne de r_{i-2} par r_{i-1};
- $v_0 = 0$ et $v_1 = 1$. Pour $i \geq 2$, on pose $v_i = v_{i-2} - v_{i-1}q_{i-1}$.

On peut montrer que la suite des restes (r_i) est une suite décroissante minorée donc convergente. Sa limite est 0, i.e, il existe $n \in \mathbb{N}$, tel que:

$$r_n \neq 0 \text{ et } r_{n+1} = 0.$$

De plus:

Theorem 1.16.

$$r_n = \text{pgcd}(a, b) = au_n + bv_n.$$

Il peut être commode de présenter les étapes de calculs sous la forme du tableau suivant :

	q_1	q_2	$\cdots$	q_n	
$r_0 = a$	$r_1 = b$	r_2	$\cdots$	r_n	$r_{n+1} = 0$
$u_0 = 1$	$u_1 = 0$	u_2	$\cdots$	u_n	
$v_0 = 0$	$v_1 = 1$	v_2	$\cdots$	v_n	

Pour mieux comprendre l'algorithme ci-dessus, voici un exemple concret que l'étudiant sera prié de refaire: Prenons $a = 17640$ et $b = 525$.

	35	1	1	2	
17640	525	315	210	105	0
1	0	1	-1	2	
0	1	-33	34	-67	

Ainsi on a:

$$\text{pgcd}(a,b) = 105 = 17640 \times 2 + 525 \times (-67).$$

Maintenant passons à la résolution dans $\mathbb{Z}^2$ d'équation du type

$$ax + by = c$$

où c est un entier donné. Notons par S l'ensemble des couples d'entiers (x, y) qui vérifient cet équation. En utilisant tout ce qu'on a fait jusqu'ici on a le résultat suivant:

Theorem 1.17. *Soit d le* pgcd *de a et b. Posons $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$. Alors:*

- *L'ensemble S est non vide si et seulement si d divise c;*
- *Si d divise c et que $(x_0, y_0) \in \mathbb{Z}^2$ est une solution particulière, on a:*

$$S = \left\{(x_0 + ka', y_0 - kb') \mid k \in \mathbb{Z}\right\}.$$

Il est important de noter que si l'équation admet de solutions (i.e d divise c), on peut prendre comme solution particulière le couple $(x_0 = u\frac{c}{d}, y_0 = v\frac{c}{d})$ où u et v sont des entiers obtenus en utilisant l'algorithme étendu d'Euclide.

Exercice 1.4.

1. Pour tout n entier naturel, déterminer le pgcd de $5n + 2$ et $12n + 5$.
2. Soit n un entier supérieur ou égal à 1. Déterminer le pgcd de $9n + 4$ et $2n - 1$.
3. Déterminer tout les entiers n de quatre chiffres tels que les restes des divisions euclidiennes de 21685 et 33509 par n soient respectivement 37 et 53.
4. Déterminer tout les couples $(x, y) \in \mathbb{Z}^2$ tels que $47x - 111y = 1$.
5. On dispose d'un récipient de 8 litres et d'un de 12 litres. Montrer qu'on peut remplir un bassin avec exactement 200 litres d'eau, en utilisant les deux récipients pour verser de l'eau dans le bassin ou pour en retirer.
6. Implémenter sur C ou C++ l'algorithme étendu d'Euclide avec comme "input" deux entiers a et b et comme "output" le pgcd ainsi que les entiers u et v tels que $au + bv = \text{pgcd}(a, b)$).

1.5 Numération en base b d'un entier

Soient b et N deux entiers naturels tels que $b \geq 2$.

Theorem 1.18. *On peut écrire N de manière unique sous la forme:*

$$x = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0,$$

où n est un entier naturel, où $a_0, \ldots, a_n$ sont des entiers tels que $0 \leq a_i \leq b-1$ et où a_n est non nul. On dit que $N = a_n a_{n-1} \cdots a_1 a_0$ est l'écriture de N en base b et l'on écrit parfois $N = (a_n \cdots a_0)_b$ ou $N = \overline{a_n \cdots a_0}^b$.

Preuve. On a un résultat plus général déjà prouvé en cours d'analyse. □

Exercice 1.5.

1. Déterminer l'écriture en base 3 de 733456.
2. Soit N un entier naturel. Trouver une condition nécessaire et suffisante simple pour que n soit divisible, respectivement, par 2, 3, 5 et par 9.
3. Soit $N = (abcabc)_{10}$ un entier écrit en base 10. Montrer que N est divisible par 77.
4. Soit $N = (a_n a_{n-1} \cdots a_1 a_0)_{10}$ l'écriture de N en base 10. Montrer que

$$N \text{ est divisible par 11 si et seulement si } \sum_{i=0}^{n} (-1)^i a_i = 0.$$

5. Déterminer les nombres de deux chiffres qui s'écrivent ab en base 10 et ba en base 7.
6. Implémenter sur C ou C++ la conversion d'un entier naturel en base quelconque.

2 Arithmétique sur $\mathbb{Z}/n\mathbb{Z}$

2.1 L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de la loi addition et multiplication

Soit n un entier naturel non nul. Pour tout entier a et b, on dit que a est `congruent` à b `modulo` n s'il a le même reste que b après division euclidienne par n. Si c'est le cas on écrit:

$$a \equiv b \bmod n.$$

Soit a un entier. L'ensemble des entiers congruents à a modulo n est noté par $\overline{a}$, i.e:

$$\overline{a} := \{b \in \mathbb{Z} \mid a \equiv b \bmod n\}.$$

Ainsi:

$$a \equiv b \bmod n \quad \text{si et seulement si} \quad \overline{a} = \overline{b}.$$

Il est important de noter que si a, b, c et d sont des entiers, alors on a les propriétés suivantes:

- $a \equiv a \bmod n$;
- Si $a \equiv b \bmod n$, alors $b \equiv a \bmod n$;
- Si $a \equiv b \bmod n$ et $b \equiv c \bmod n$, on a $a \equiv c \bmod n$;
- Si $a \equiv b \bmod n$ et $c \equiv d \bmod n$, alors $a + c \equiv b + c \bmod n$ et $ac \equiv bd \bmod n$.

Finalement, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est définie par:

$$\mathbb{Z}/n\mathbb{Z} := \{\overline{a} \mid a \in \mathbb{Z}\}.$$

Comme les restes possibles après division euclidienne par n sont: $0, 1, 2, \ldots, n-1$, on conclut que:

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\right\}.$$

Maintenant on va munir $\mathbb{Z}/n\mathbb{Z}$ de deux lois binaires, à savoir la loi addition et la multiplication, induites par celles de $\mathbb{Z}$. D'après les propriétés ci-dessus, on conclut qu'on a, pour tout $\overline{a}$ et $\overline{b}$ dans $\mathbb{Z}/n\mathbb{Z}$:

- $\overline{a} + \overline{b} = \overline{a+b}$;
- $\overline{a} \cdot \overline{b} = \overline{ab}$.

S'il n'y a pas de confusion, on pourra omettre la barre sur les entiers. Mais, l'étudiant doit se souvenir toujours dans quel ensemble il travaille.

Exemples 2.1. *Pour $n = 6$, on a les tables suivantes:*
Pour l'addition:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Pour la multiplication:

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

2.2 Element inversible de $\mathbb{Z}/n\mathbb{Z}$

Soit a un entier. On dit que $\overline{a}$ est `inversible` dans $\mathbb{Z}/n\mathbb{Z}$ s'il existe un entier u tel que

$$\overline{u} \cdot \overline{a} = \overline{1}$$

C'est à dire:

$$au \equiv 1 \bmod n.$$

Si c'est le cas, on dit que $\overline{u}$ est `l'inverse` de $\overline{a}$ dans $\mathbb{Z}/n\mathbb{Z}$. Noter bien que $\overline{u}$ est aussi inversible et que $\overline{a}$ est son inverse.
L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est noté par $(\mathbb{Z}/n\mathbb{Z})^{\times}$. D'après la table de multiplication ci-dessus, on a par exemple:

$$(\mathbb{Z}/6\mathbb{Z})^{\times} = \left\{\overline{1}, \overline{5}\right\}.$$

L'inverse de $\overline{1}$ est lui-même, de même pour $\overline{5}$.

Theorem 2.2. *Soit a un entier. L'élément $\overline{a}$ de $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si a et n sont premiers entre eux. C'est à dire:*

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{pgcd}(a,n) = 1\}.$$

Preuve. Supposons que $\overline{a}$ est inversible. Donc, il existe un entier u tel que $au \equiv 1 \bmod n$. C'est à dire, il existe un entier v tel que $au = 1 + nv$. D'après le théorème de Bézout, comme $au - nv = 1$, où u et v sont des entiers, alors $\text{pgcd}(a,n) = 1$. Supposons maintenant que $\text{pgcd}(a,n) = 1$. D'après Bézout encore, ils existent deux entiers u et v tels que $au + nv = 1$. Dans, $\mathbb{Z}/n\mathbb{Z}$, on a $\overline{au + nv} = \overline{au} + \overline{nv} = \overline{au} = \overline{1}$ car $\overline{nv} = 0$. D'où $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. □

Ainsi, pour vérifier si un élément $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$, il suffit de calculer le pgcd de a et n. S'ils sont premiers entre eux, on conclut que $\overline{a}$ est inversible. Pour calculer l'inverse, on cherche un couple d'entier (u,v) tel que

$$au + nv = 1$$

en utilisant l'algorithme d'Euclide. Ainsi, l'inverse de $\overline{a}$ est $\overline{u}$.

Exercice 2.2.

1. Déterminer l'ensemble $(\mathbb{Z}/32\mathbb{Z})^\times$. Montrer que 19 est inversible dans $\mathbb{Z}/32/Z$, puis calculer son inverse.
2. Soit p un nombre premier. Déterminer l'ensemble $(\mathbb{Z}/p\mathbb{Z})^\times$.
3. Calculer l'inverse de 641 dans $\mathbb{Z}/160652096310001\mathbb{Z}$.

2.3 La fonction indicatrice d'Euler

Soit n un entier naturel non nul. La fonction φ de $\mathbb{N}$ vers $\mathbb{N}$ définie par:

$$\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^\times$$

est appelée `fonction indicatrice d'Euler`. Autrement dit: $\varphi(n)$ est le nombre des entiers naturels premiers avec n et inférieurs à n. Elle vérifie les propriétés suivantes:

- Si p est un nombre premier, pour tout entier naturel $k \geq 1$, on a:
$$\varphi(p^k) = p^k - p^{k-1};$$
- Si n et m sont des entiers naturels non nuls premiers entre eux, on a:
$$\varphi(nm) = \varphi(n)\varphi(m).$$

D'où:

Theorem 2.3. *Si $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ la décomposition de n en facteurs premiers, on a:*

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Ceci nous amène à énoncer l'un des théorèmes les plus importants en arithmétique:

Theorem 2.4 (Euler)**.** *Soit a un entier premier avec n. Alors:*

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Exercice 2.3

1. Calculer $\varphi(100)$ et $\varphi(600851475143)$.
2. Posons $a = (1035125)^{5642}$. Déterminer le reste de la division euclidienne de a par 17.
3. Trouver le dernier chiffre (écrit en base 10) de l'entier $3^{7^{2020}}$.
4. Soient p un nombre premier impair et a, b deux entiers non divisibles par p, tels que p divise $a^2 + b^2$. Montrer que l'on a $p \equiv 1 \bmod 4$.
5. Montrer que 13 divise $2^{70} + 3^{70}$.

2.4 Le Théorème Chinois et système d'équations congruences

Soient n et m deux entiers naturels non nuls. Considérons le système d'équations suivant:

$$\begin{cases} x \equiv a \bmod n; \\ x \equiv b \bmod m. \end{cases} \tag{2}$$

où a et b sont des entiers.
Le théorème Chinois résout cet système dans $\mathbb{Z}/nm\mathbb{Z}$ comme suit:

Theorem 2.5 (Théorème Chinois)**.** *Le système d'équations (2) admet*

$$x = \overline{bun + avm}$$

comme solution unique dans $\mathbb{Z}/nm\mathbb{Z}$ où les entiers u et v vérifient l'équation:

$$un + vm = 1.$$

Exercice 2.4

1. *Résoudre dans $\mathbb{Z}/437\mathbb{Z}$ le système suivant:*

$$\begin{cases} x \equiv 7 \bmod 19; \\ x \equiv 10 \bmod 23. \end{cases}$$

2. *Résoudre dans $\mathbb{Z}$ le système suivant:*

$$\begin{cases} x \equiv 3 \bmod 101; \\ x \equiv 98 \bmod 641. \end{cases}$$

3. *Déterminer le plus petit entier naturel multiple de 7 et congru à 1 modulo 2, 3, 4, 5 et 6.*

3 Applications

3.1 Introduction au cryptosystème RSA

La cryptographie est l'étude de la science des communications par des messages codés qui ne pourront être lus que par leur destinataire. Un cryptosystème est un tel mode de communication. La cryptographie suscite en fait de l'intérêt depuis l'antiquité, compte tenu de la nécessité de pouvoir faire parvenir des messages qui ne puissent pas être déchiffrés par un hh intrus ii . L'algorithme RSA, qui a été découvert par Rivest, Shamir et Adleman en 1977, a constitué de ce point de vue une très importante avancée. C'est un algorithme à clé publique. Son efficacité repose sur le fait qu?il est difficile de factoriser un entier ayant disons plus de deux cents chiffres dans son écriture décimale i.e. dans son écriture en base 10.
Voici le Principe du cryptosystème RSA:Si un utilisateur A veut utiliser le cryptosystème RSA pour qu'il puisse recevoir un message d'un autre utilisateur B, il doit procéder comme suit:

1. Il choisit deux grands nombres premiers p et q et calcule $n = pq$. On choisit ces deux nombres premiers de tels sorte qu'il est "impossible" pour d'autre personne de factoriser l'entier naturel n;

2. Choisir un entier e premier avec $\varphi(n)$ tel que $1 < e < \varphi(n)$. La classe de e modulo $\varphi(n)$ est donc inversible dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$;

3. L'utilisateur détermine ensuite l'entier d, l'inverse de e dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$;

4. Il publie à la fin le couple (e, n), qui est `sa clé publique`, et il conserve en secret le couple $(d, \varphi(n))$ ainsi que les nombres premiers p et q , qui est `sa clé secrète.`

   Toute personne voulant écrire un message a l'utilisateur A utilise la clé public (e, n) pour chiffre le message. Tandis que l'utilisateur utilise sa clé secrète pour déchiffrer le message crypter.

Maintenant, si l'utilisateur B veut envoyer un message m à A, il doit procéder comme suit:

- Il calcule tout simplement $x = m^e$ et envoie la classe $\overline{x}$ de x modulo $\mathbb{Z}/n\mathbb{Z}$. Tout le monde peut recevoir la valeur $\overline{x}$, mais si on ne possède pas la clé secrète de A, on n'est pas sensé pouvoir déchiffrer le message facilement.

Enfin, si l'utilisateur A veut déchiffrer le message envoyer par B, il calcule $\overline{x}^d = m^{ed}$ dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$. Comme $ed \equiv 1 \ \mathrm{mod}\varphi(n)$. On a

$$ed = 1 + k\varphi(n)$$

pour un certain entier k. Or d'après le théorème d'Euler, dans $\mathbb{Z}/n\mathbb{Z}$, on a:

$$m^{k\varphi(n)} \equiv 1 \mathrm{mod}\ n.$$

D'où:

$$\overline{x}^d = m^{ed} \equiv m \ \mathrm{mod}\ n.$$

C'est ainsi, l'utilisateur pourra obtenir le message m.
Un exemple concret sera dirigé en classe.

3.2 Projet d'Euler