Bases de l'Arithmétique & Cryptologie Romantique

Ninon Devis: ninon.devis@ircam.fr

TD5

Exercice 19 – Lagrange, Bézout et les groupes

Dans tout cet exercice les groupes sont finis et commutatifs. Une notation utilisée ici et par la suite pour éviter les problèmes liés à l'opération du groupe : pour tout entier k strictement positif [k]g représente k opérations de g avec lui-même et [−1]g est l'inverse de g dans le groupe. La notation [0]g représentera donc l'élément neutre du groupe.

1. Rappeler ce qu'est l'ordre d'un élément g d'un groupe fini.

- Il s'agit du plus petit entier positif k tel que: $[k]g = [0]g$.

2. Donner l'ordre de chacun des éléments du groupe additif Z/30Z.

- L'ordre d'un élément n est le plus petit facteur par lequel multiplier n pour obtenir un multiple 30.
- Ce multiple de 30 obtenu est le $\text{ppcm}(n, 30)$.

Exercice 19 – Lagrange, Bézout et les groupes

2. Donner l'ordre de chacun des éléments du groupe additif Z/30Z.

- Le facteur est donc $30/\text{pgcd}(n, 30)$
- Ce qui nous donne:

$1 : 30/\text{pgcd}(1,30) = 30/1 = 30$ ordre $1 = 30$.

$2 : 30/\text{pgcd}(2,30) = 30/2 = 15$

$3 : 30/\text{pgcd}(3,30) = 10$

$4 : 30/\text{pgcd}(4,30) = 15$

$5 : 30/\text{pgcd}(5,30) = 6$

$6 : 30/\text{pgcd}(6,30) = 5$.

Exercice 19 – Lagrange, Bézout et les groupes

3. Soit g un élément d'un groupe fini. On note ω(g) l'ordre de g. Montrer que pour tout entier k non nul, si [k]g = 0 alors ω(g) divise k.

- Soit k un entier non nul, tel que [k]g = 0.

La division euclidienne de k par ω(g) s'écrit: $k = q \times \omega(g) + r$ avec $0 \leq r < \omega(g)$

En effectuant k opérations de g: $[k]g = [q\,\omega(g) + r]g$

$= [q][\omega(g)]g + [r]g$

$= [0]g + [r]g$

car $[\omega(g)]g = [0]g$.

Exemple sur la question 2 où il s'agit du groupe additif Z/30Z:

- pour 1, ordre 30 d'où: $\omega(g) = 30 \quad g = 1 \quad \underbrace{1 + 1 + \dots + 1}_{30 \text{ fois}} = 30 = 0[30]$
- pour 2, ordre 15 d'où: $\omega(g) = 15 \quad g = 2 \quad \underbrace{2 + 2 + \dots + 2}_{15 \text{ fois}} = 30 = 0[30]$
- pour 3, ordre 10 d'où:
- …

Exercice 19 – Lagrange, Bézout et les groupes

On a: $[k]g = [0]g + [r]g$

Or par hypothèse: $[k]g = 0$ donc si $r \neq 0$, on a trouvé un entier r non nul tel que:

$$[r]g = 0 \quad \text{et} \quad r < \omega(g)$$

Or $\omega(g)$ est déjà le plus petit facteur par lequel multiplier g pour obtenir un multiple.

On a donc nécessairement: $r = 0$ $\qquad k = q\,\omega(g)$

$$\left(k = q\,\omega(g) + r \right)$$

➔ Donc $\omega(g)$ divise k !

On a montré que: si $[k]g = 0$ alors $\omega(g) \mid k$

Exercice 19 – Lagrange, Bézout et les groupes

$[k]g = [0]g$

4. En notant ω(a) l'ordre d'un élément a d'un groupe fini. Montrer que ω([k]a) = ω(a) / pgcd(ω(a), k) pour tout k ∈ Z\{0}. Qu'en déduisez-vous pour ω([−1]a) et dans le cas où k est premier avec ω(a). Si [k]g = 0 alors ω(g) | k ← minimalité

- Par définition de ω(a), on a: $[\omega(a)]a = [0]a$
- Par définition de ω([k]a): $\omega([k]a)[k]a = [0]a$
- Et on peut écrire: $[\omega([k]a)][k]a = [\underbrace{\omega([k]a)k}_{=k}]a$
- Donc par minimalité de ω(a):

$$\omega(a) \mid \omega([k]a)k$$

On pose g = pgcd (ω(a), k) alors:

$\exists \lambda, \mu$ tels que $\omega(a) = \lambda g$ et $k = \mu g$ λ, μ sont premiers entre eux

On a donc: $\omega(a) \mid \omega([k]a)k \iff \lambda \cancel{g} \mid \omega([k]a)\mu \cancel{g} \iff \lambda \mid \omega([k]a)\mu$

Or λ, μ sont premiers entre eux : $\boxed{\lambda \mid \omega([k]a)}$

(deux nombres premiers entre eux n'admettent aucun diviseur commun à part 1)

Exercice 19 – Lagrange, Bézout et les groupes

$\omega(a) = \lambda g$

- Par ailleurs: $[\lambda][k]a = \left[\frac{\omega(a)}{g}\right][k]a$

$$= \left[\frac{k}{g}\right]\underbrace{[\omega(a)]a}_{[0]a} = [0]a$$

$$[0]a = \omega([k]a)[k]a$$

$[k]g = 0$

$\Rightarrow \omega(g) \mid k$

Par minimalité de ω([k]a):

$\omega([k]a) \mid \lambda$

D'où, on a:

$\lambda \mid \omega([k]a)$ et $\omega([k]a) \mid \lambda \Rightarrow \omega([k]a) = \lambda$

et par définition:

$$\lambda = \frac{\omega(a)}{\mathrm{pgcd}(\omega(a), k)} \Rightarrow \boxed{\omega([k]a) = \frac{\omega(a)}{\mathrm{pgcd}(\omega(a), k)}}$$

Exercice 19 – Lagrange, Bézout et les groupes

5. Soit a et b deux éléments d'un groupe fini (commutatif). Montrer que $\omega(a \circ b)$ est un diviseur de $\text{ppcm}(\omega(a), \omega(b))$.

- $\omega(a) \mid \text{ppcm}(\omega(a), \omega(b))$ donc $[\text{ppcm}(\omega(a), \omega(b))]a = [0]a$
  $\omega(b) \mid \text{ppcm}(\omega(a), \omega(b))$ donc $[\text{ppcm}(\omega(a), \omega(b))]b = [0]b$.
- D'où:

$[k]g = 0 \Rightarrow \omega(g) \mid k$.

$$[\underline{\text{ppcm}(\omega(a), \omega(b))}](a \circ b) =$$

$$\underbrace{[\text{ppcm}(\omega(a), \omega(b))]a}_{[0]a} \circ \underbrace{[\text{ppcm}(\omega(a), \omega(b))]b}_{[0]b} = \underline{[0](a \circ b)}$$

$\Rightarrow \omega(a \circ b) \mid \text{ppcm}(\omega(a), \omega(b))$

Exercice 19 – Lagrange, Bézout et les groupes

6. Montrer que tout groupe d'ordre premier est cyclique. $\exists x \mid \forall y \in G, \exists k$ tel que $y = x^k \to G = \langle x \rangle$

$\hookrightarrow p$

- Rappels:
  - Cardinal d'un groupe = ordre du groupe.
  - Un groupe est cyclique si il existe un élément *a* du groupe tel que tout élément du groupe puisse s'exprimer sous forme d'un multiple de *a*.
  - Théorème de Lagrange: Pour tout groupe fini *G* et tout sous-groupe *H* de *G*, l'ordre de *H* (c'est-à-dire son cardinal) divise celui de *G*.

Soit $a \neq 1 \in G$. Alors 1 et $a \in \langle a \rangle$ ($a^0 = 1$ et $a^1 = a$)

Donc $\mathrm{card}(\langle a \rangle) \geq 2$

De plus $\mathrm{card}(\langle a \rangle) \mid p$ (ordre de G) $\to$ cf Lagrange.

Or p est premier donc $\mathrm{card}(\langle a \rangle) = p$ $\Rightarrow$ D'où $G = \langle a \rangle$.

Exercice 20 – Arithmétique modulaire et complexité

1. Soit n un entier et a un élément de Z/nZ. Si a est inversible peut-il être un diviseur de zéro (argumentez votre réponse) ? Si a est diviseur de zéro, comment calculer l'entier b ∈ Z/nZ tel que ab = 0 ?

- On suppose que a est inversible et qu'il existe b tel que ab = 0.

$b = 1b = (a^{-1}a)b = a^{-1}ab = a^{-1}0 = 0$ donc $b = 0$.

➔ Si a est inversible alors a n'est pas diviseur de 0.

- Si a est diviseur de 0: $pgcd(a, n) > 1$

$a = a'd$ et $n = n'd$ (a', n' premiers entre eux)

$0 < n' < n$ donc si $b = n'$ alors $ab = a'dn' = a'n = 0 \bmod n$

Exercice 20 – Arithmétique modulaire et complexité

2. (Algorithme d'Euclide étendu) Estimer a priori le nombre de calculs à effectuer pour déterminer le pgcd et la relation de Bézout entre 1014 et 5005. Effectuer l'ensemble des calculs intermédiaires et présenter les sous la forme d'un tableau.

- L'algorithme permet de calculer très efficacement PGCD.
- Soit a et b tels que a > b:
  - l'algorithme fera au plus: $\log_\varphi(b)$ boucles — φ nombre d'or !
  - Ici: $\lfloor \log_\varphi(1014) \rfloor = 14$ boucles
  - Le nombre d'opérations élémentaires s'obtient par: $O(\log a \log b)$
  - Ici: $O(\log(1014)\log(5005))$.

Exercice 20 – Arithmétique modulaire et complexité

2. Déterminer le pgcd et la relation de Bézout entre 1014 et 5005.

A chaque étape :

Relation de Bezout

$r_i = u_i a + v_i b$

$5005 = 4 \times 1014 + 949$

puis : $u_{i+1} = u_{i-1} - q_i \times u_i$

$= 1 - 0 \times 4 = 1$

$v_{i+1} = v_{i-1} - q_i \times v_i$

$= 0 - 4 \times 1 = -4$

$1014 = 1 \times 949 + 65$

$u_{i+1} = 0 - 1 \times 1 = -1$

$v_{i+1} = 1 - (-4) = 5$

i	r_{i-1}	q_i	r_i	r_{i+1}	u_{i+1}	v_{i+1}
-1					1	0
0			5005	1014	0	1
1	5005	4	1014	949	1	-4
2	1014	1	949	65	-1	5
3	949	14	65	39	15	-74
4	65	1	39	26	-16	79
5	39	1	26	13	31	-153
6	26	2	13	0	-78	385

Exercice 20 – Arithmétique modulaire et complexité

2. Déterminer le pgcd et la relation de Bézout entre 1014 et 5005.

Le PGCD est donné par:

le dernier reste positif

→ ici 13

$u_6 a + v_6 b = r_6$ (rouge)

$31 \times 5005 - 153 \times 1014 = 13$.

En vert:

$0 = r_7 = u_7 a + v_7 b$

PGCD > 1 ⇒ a, b diviseurs de 0.

u_7 inverse de a

v_7 inverse de b

i	r_{i-1}	q_i	r_i	r_{i+1}	u_{i+1}	v_{i+1}
-1					1	0
0			5005	1014	0	1
1	5005	4	1014	949	1	-4
2	1014	1	949	65	-1	5
3	949	14	65	39	15	-74
4	65	1	39	26	-16	79
5	39	1	26	13	31	-153
6	26	2	13	0	-78	385

Exercice 20 – Arithmétique modulaire et complexité

2. L'entier 1014 est-il un inverse ou un diviseur de zéro dans Z/5005Z? Si c'est un inverse calculer l'entier b ∈ Z/5005Z tel que $1014 \times b = 1 \bmod 5005$. Si c'est un diviseur de zéro calculer l'entier b ∈ Z/5005Z tel que $1014 \times b = 0 \bmod 5005$.

i	r_{i-1}	q_i	r_i	r_{i+1}	u_{i+1}	v_{i+1}
- 1					1	0
0			5005	1014	0	1
1	5005	4	1014	949	1	-4
2	1014	1	949	65	-1	5
3	949	14	65	39	15	-74
4	65	1	39	26	-16	79
5	39	1	26	13	31	-153
6	26	2	13	0	-78	385

PGCD > 1 donc 1014 diviseur de 0 dans $\mathbb{Z}/5005\mathbb{Z}$

et $u_7 a + v_7 b = r_7$

→ $-78 \times 5005 + 385 \times 1014 = 0$

donc : $385 \times 1014 = 0 \bmod 5005$

→ 1014 a pour inverse 385 !

Exercice 18 – Sur le PGCD et son calcul

$n = 216 \to 2+1+6 = 9$

- Rappels : Pour trouver les diviseurs premiers d'un nombre n:
  - 2 divise n si n est pair
  - 5 divise n si n se termine par 0 ou 5
  - 3 divise n si la somme des chiffres de n est multiple de 3
  - 7: On sépare le dernier chiffre du nombre (***371***) du reste (*37*).
    On multiplie ce chiffre par 2 ($1 \times 2 = 2$) et on le soustrait du nombre qui restait ($37 - 2 = 35$) Si ce nouveau nombre est divisible par 7, le nombre initial est divisible par 7. (Ici, 35 est divisible par 7, donc 371 l'est aussi)
  - 11 divise n si la somme des chiffres situés aux *positions paires* est égale à la somme des chiffres situés aux *positions impaires* modulo 11.
    - Exemple: 5181:
      - positions paires: $5 + 8 = 13 = 2 \bmod 11$
      - positions impaires: $1 + 1 = 2 \bmod 11$ => 5181 est divisible par 11
- Cf corrigés pour preuves

Exercice 18 – Sur le PGCD et son calcul

1. Donner la décomposition en produits d'éléments irréductibles des entiers $a = 1170$ et $b = 330$. Donner les listes $D(a)$ et $D(b)$ des diviseurs de a et b et calculer l'intersection $D(a) \cap D(b)$.

Le nombre de diviseurs d'un nombre est égal au produit des puissances de chacun de ses facteurs premiers, chacune augmentée de 1.

- $a = 1170 = 2^1 \times 3^2 \times 5^1 \times 13^1 \Rightarrow card(D(a)) = (1+1)\times(2+1)\times(1+1)\times(1+1) = 24$
- $b = 330 = \underline{2^1 \times 3^1 \times 5^1 \times 11^1} \Rightarrow card(D(b)) = (1+1)\times(1+1)\times(1+1)\times(1+1) = 16.$
- Pour trouver D(a) et D(b) on calcule chaque 'combinaison':
  - Exemple pour D(b):

$2^0 \times 3^0 \times 5^0 \times 11^0 = 1$	$2^0 \times 3^1 \times 5^0 \times 11^0 = 3$	$2^1 \times 3^1 \times 5^0 \times 11^0 = 6$	$2^1 \times 3^0 \times 5^0 \times 11^0 = 2$
$2^0 \times 3^0 \times 5^0 \times 11^1 = 11$	$2^0 \times 3^1 \times 5^0 \times 11^1 = 33$	$2^1 \times 3^1 \times 5^0 \times 11^1 = 66$	$2^1 \times 3^0 \times 5^0 \times 11^1 = 22$
$2^0 \times 3^0 \times 5^1 \times 11^0 = 5$	$2^0 \times 3^1 \times 5^1 \times 11^0 = 15$	$2^1 \times 3^1 \times 5^1 \times 11^0 = 30$	$2^1 \times 3^0 \times 5^1 \times 11^0 = 10$
$2^0 \times 3^0 \times 5^1 \times 11^1 = 55$	$2^0 \times 3^1 \times 5^1 \times 11^1 = 165$	$2^1 \times 3^1 \times 5^1 \times 11^1 = 330$	$2^1 \times 3^0 \times 5^1 \times 11^1 = 110$

Exercice 18 – Sur le PGCD et son calcul

1. Donner la décomposition en produits d'éléments irréductibles des entiers $a = 1170$ et $b = 330$. Donner les listes $D(a)$ et $D(b)$ des diviseurs de a et b et calculer l'intersection $D(a) \cap D(b)$.

On trouve ainsi: $D(b) = \{1, 2, 3, 5, 6, 10, 11, 15, 22, 30, 33, 55, 66, 110, 165, 330\}$

et avec la même méthode:

$D(a) = \{1, 2, 3, 5, 6, 9, 10, 13, 15, 18, 26, 30, 39, 45, 65, 78, 90, 117, 130, 195, 234, 390, 585, 1170\}$

Soit une intersection: $D(a) \cap D(b) = \{1, 2, 3, 5, 6, 10, 15, 30\}$

2. Déduire le PGCD de a et b.

Avec les valuations p-adiques :

$$\left.\begin{aligned} a &= 2^1 \times 3^2 \times 5^1 \times 11^0 \times 13^1 \\ b &= 2^1 \times 3^1 \times 5^1 \times 11^1 \times 13^0 \end{aligned}\right\} d = 2^1 \times 3^1 \times 5^1 = 30.$$

Exercice 18 – Sur le PGCD et son calcul

3. Rappeler la définition du PGCD vue en cours et basée sur les valuations p-adiques. Est-ce que cette définition permet de calculer efficacement le PGCD de deux entiers ?

Tout entier *n* supérieur ou égal à 2 s'écrit de manière unique, à l'ordre près des facteurs et au signe près, comme un produit fini de nombres premiers. Le nombre de fois que l'entier premier *p* apparaît dans cette écriture s'appelle la valuation *p*-adique de *n*, notée $v_p(n)$.

→ Soit P l'ensemble des irréductibles d'un anneau A factoriel. On note $v_p(a)$ pour $a \in A$ et $p \in P$ le plus grand entier v tel que p^v divise a.

Par définition,

$$d = \prod_{p \in P} p^{\min(v_p(a), v_p(b))}$$

donc pour tout $p \in P$, $v_p(d) = \min(v_p(a), v_p(b))$

Cette définition permet théoriquement de calculer le PGCD. Il suffit de connaître la factorisation de a et b pour en déduire le PGCD.

Exercice 18 – Sur le PGCD et son calcul

4. calculer le PGCD de 1537 et 1643 à partir des valuations p-adiques de ces deux entiers.

On trouve (péniblement): $1537 = 29 \times 53$ et $1643 = 31 \times 53$

D'où PGCD = 53

5. En utilisant l'algorithme d'Euclide, calculer le PGCD de la question précédente. Qu'en concluez-vous ?

On réalise des divisions euclidiennes jusqu'à trouver un reste nul.

$$1643 = 1537 \times 1 + 106$$
$$1537 = 106 \times 14 + 53$$
$$106 = 53 \times 2 + 0$$

Factorisation délicate alors que l'application de l'algorithme d'Euclide est facile.

Exercice 18 – Sur le PGCD et son calcul

6. Rappeler la relation de Bachet-Bézout et la définition d'éléments premiers entre eux. Comment repérer une telle propriété sur deux entiers donnés à l'aide de la relation de Bachet-Bézout.

Rappels: si deux entiers a et n sont premiers entre eux, on sait qu'il existe deux nombres u et v tels que $au + nv = 1$. Modulo n, cette égalité devient $au = 1 \pmod{n}$.

7. Rappeler la définition du ppcm de deux entiers. Quel est la relation entre ab, pgcd(a, b) et ppcm(a, b).

ppcm = plus petit commun multiple

$ab = \text{pgcd}(a, b) \times \text{ppcm}(a, b)$

Si on a a et b on calcule le pgcd avec Euclide pour en déduire ppcm.

Exercice 17 – Questions de Cours

1. Dans un anneau A comment sont définis les éléments inversibles et les diviseurs de 0 ? Un diviseur de 0 peut-il être inversible ? Qu'est-ce qu'un anneau intègre ? Donnez un exemple d'un anneau qui l'est et un autre qui ne l'est pas.

- Un élément $x \in A$ est inversible ssi $\exists y \in A$ tq $yx = xy = 1$.
  On note x^{-1} l'inverse y de x.
- Un élément $x \in A^x$ est un diviseur de 0 ssi $\exists y \in A^x$ tq $xy = yx = 0$.
- Un diviseur de 0 peut il être inversible ? Supposons x inversible et zx = xz = 0,
  alors: $z = 1z = (x^{-1}x)z = x^{-1}xz = x^{-1}(xz) = x^{-1}0 = 0$
  ce qui implique que si x inversible et $zx = 0$ alors $z = 0$
  donc x n'est pas diviseur de 0.
- Un anneau intègre est un anneau commutatif $\neq$ de l'anneau nul et qui ne possède aucun diviseur de 0.
- Pour p et q premiers: $\mathbb{Z}/p\mathbb{Z}$ est intègre $\mathbb{Z}/p\times q\mathbb{Z}$ ne l'est pas !

Exercice 17 – Questions de Cours

2. Rappeler la définition d'irréductibilité pour un élément d'un anneau intègre. Quelle est la définition d'un anneau factoriel ?

- Un élément a ≠ 0 de A est irréductible si il est non inversible et si ses seuls diviseurs possibles sont de la forme u ou ua avec u un inversible de a.
- Un anneau est factoriel si tout élément non nul peut se décomposer de manière unique en produit d'éléments irréductibles.

3. Quelles caractéristiques (parmi celles citées plus haut) possède l'anneau des entiers Z ? Que sont les éléments irréductibles de Z ? (thm fond. d'arithm. d'Euclide)

- Z est factoriel et intègre
- Ses éléments irréductibles sont: les nombres premiers et leur opposés ! \o/