Université Paris 12 Février 2014
Licences d'Informatique et de Mathématiques
2013-2014

TD de Mathématiques Discrètes
TD 2 - Éléments inversibles, indicatrice d'Euler, chiffrement affine

Fait par : Farah AIT SALAHT

Exercice 1

1. Déterminer tous les éléments inversibles de $\mathbb{Z}/20\mathbb{Z}$.
2. Calculer $\varphi(20)$, puis comparer avec le résultat de la question précédente.

Corrigé :

Proposition 1 *Pour tout entiers $k \in \mathbb{Z}$, l'élément $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est premier à n.*

Soit $k \in \mathbb{Z}$. On a les équivalences :

$$\begin{aligned} k \text{ est premier à } n &\iff \exists\, u,\, v \in \mathbb{Z},\ k\,u + n\,v = 1 \text{ (théorème de Bézout)} \\ &\iff \exists\, u \in \mathbb{Z},\ k\,u \equiv 1 \bmod n \\ &\iff \exists\, u \in \mathbb{Z},\ (\overline{k})\,(\overline{u}) = \overline{1}\ dans\, \mathbb{Z}/n\mathbb{Z} \\ &\iff \overline{k} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z}. \end{aligned}$$

1. Dans l'anneau $\mathbb{Z}/20\mathbb{Z}$, les inversibles sont :

$$\overline{1},\ \overline{3},\ \overline{7},\ \overline{9},\ \overline{11} = -\overline{9},\ \overline{13} = -\overline{7},\ \overline{17} = -\overline{3},\ \overline{19} = -\overline{1}$$

Le groupe des inversibles $(\mathbb{Z}/20\mathbb{Z})$=$\{\pm\overline{1},\ \pm\overline{3},\ \pm\overline{7},\ \pm\overline{9}\}$, il y a 8 éléments
Calculons 'linverse de $\overline{9}$. On a la relation de Bézout $9 \times 9 - 4 \times 20 = 1$, d'où $9 \times 9 \equiv 1\text{mod}20$ et $(\overline{9})\,(\overline{9}) = \overline{1}$. Ainsi, $(\overline{9})^-1 = \overline{9}$.
De même, puisque $7 \times 3 \equiv 1\text{mod}20$, on a $(\overline{7})\,(\overline{3}) = \overline{1}$, donc $\overline{7}$ et $\overline{3}$ sont inverses l'un de l'autre.
Par suite, $-\overline{7}$ et $-\overline{3}$ sont aussi inverses l'un de l'autre.

2. $\varphi(20)$

Théorème : pour tout $n \geq 2$, si la décomposition de n est

$$n = \prod_{0 \leq i \leq t} p_i^{\alpha_i}.$$

Alors on a

$$\varphi(n) = \prod_{0 \leq i \leq t} (p_i - 1)\, p_i^{\alpha_i - 1}.$$

Pour le calcul de φ on utilise la formule vue en cours, qui donne $\varphi(20) = 2 * (5 - 1) = 8$

Exercice 2

1. Démontrer que pgcd(49, 72) = 1 en utilisant l'algorithme d'Euclide.
2. En utilisant l'algorithme d'Euclide étendu, trouver des coefficients entiers u et v tels que $49u + 72v = 1$.
3. En déduire la valeur de l'inverse de 49 dans $\mathbb{Z}/72\mathbb{Z}$.
4. Refaire les questions 1 et 2 avec 436 et 237, ainsi que 534 et 408.
5. Trouver les inverses de 169, 187, 338 et 209 dans $\mathbb{Z}/420\mathbb{Z}$.

Corrigé :

1. pgcd(49, 72) = 1 :
   - PGCD(72 , 49) = PGCD(49 , 23) car $72 = 49 \times 1 + 23$
   - PGCD(49 , 23) = PGCD(23 , 3) car $49 = 23 \times 2 + 3$
   - PGCD(23 , 3) = PGCD(3 , 2) car $23 = 3 \times 7 + 2$
   - PGCD(3 , 2) = PGCD(2 , 1) car $3 = 2 \times 1 + 1$
   - PGCD(2 , 1) = PGCD(1 , 0) car $2 = 1 \times 2 + 0$
   - PGCD(1 , 0) =1.
2. **(a)** Bezout, $au + bv = pgcd(a; b)$. La formule est $u = v'$ et $v = u' - \lfloor \frac{a}{b} \rfloor v'$, ce qui permet le calcul recursif des valeurs :

$a = 72$	$b = 49$	$u = -17$	$v = 25$
49	23	8	-17
23	3	-1	8
3	2	1	-1
2	1	0	1
1	0	1	0

   (b) Algorithme d'Euclide étendu

   $$\begin{aligned} 1 &= 3 - 2 \times 1 \\ &= 3 - (23 - 3 \times 7) \times 1 \\ &= 23 \times (-1) + 3 \times 8 \\ &= 23 \times (-1) + (49 - 23 * 2) \times 8 \\ &= 49 \times 8 + 23 \times (-17) \\ &= 49 \times 8 + (72 - 49 \times 1) \times (-17) \\ &= 72 \times (-17) + 49 \times 25 \end{aligned}$$

   D'où $u = -17$ et $v = 25$.
3. L'inverse existe car pgcd(49 ; 72) = 1. Une fois que l'on a $72 \times -17 + 49 \times 25 = 1$, on a facilement que $49 \times 25 \equiv 1[72]$.
4. Refaire les questions 1 et 2...

   (a) Pour 436 et 237 :
   - PGCD(436 ; 237) = PGCD(237 ; 199) car 436 = 237 x 1 + 199
   - PGCD(237 ; 199) = PGCD(199 ; 38) car 237 = 199 x 1 + 38
   - PGCD(199 ; 38) = PGCD(38 ; 9) car 199 = 38 x 5 + 9
   - PGCD(38 ; 9) = PGCD(9 ; 2) car 38 = 9 x 4 + 2
   - PGCD(9 ; 2) = PGCD(2 ; 1) car 9 = 2 x 4 + 1
   - PGCD(2 ; 1) = PGCD(1 ; 0) car 2 = 1 x 2 + 0

   Donc pgcd(436, 237) = 1
   Solution particulière de l'équation $436u + 237v = 1$ où $1 = pgcd(436, 237)$

- 436 = 1*237+199, 199 = 1*436 - 1*237
- 237 = 1*199+38, 38 = -1*436 + 2*237
- 199 = 5*38+9, 9 = 6*436 - 11*237
- 38 = 4*9+2, 2 = -25*436 + 46*237
- 9 = 4*2+1, 1 = 106*436 - 195*237

Solution particulière : (106,-195)
Solution particulière de l'équation $436u + 237v = 1$: $(106, -195)$

(b) Pour 534 et 408

- PGCD(534 ; 408) = PGCD(408 ; 126) car 534 = 408 x 1 + 126
- PGCD(408 ; 126) = PGCD(126 ; 30) car 408 = 126 x 3 + 30
- PGCD(126 ; 30) = PGCD(30 ; 6) car 126 = 30 x 4 + 6
- PGCD(30 ; 6) = PGCD(6 ; 0) car 30 = 6 x 5 + 0

Donc pgcd(534 ; 408) = 6
Solution particulière de l'équation $534u + 408v = 6$ où $6 = pgcd(534, 408)$

- 534 = 1*408+126, 126 = 1*534 - 1*408
- 408 = 3*126+30, 30 = -3*534 + 4*408
- 126 = 4*30+6, 6 = 13*534 - 17*408

Solution particulière : (13,-17)
Solution particulière de l'équation $534u + 408v = 6$: $(13, -17)$

5. Les inverses

(a) Résoudre $169x \equiv 1[420]$
Faisable car $pgcd(169, 420) = 1$
Solution particulière de l'équation $169u + 420v = 1$: $(169, -68)$
Donc, on a $169 \times 169 \equiv 1[420]$

(b) Resoudre $187x \equiv 1[420]$
Faisable car $pgcd(187, 420) = 1$
Solution particulière de l'équation $187u + 420v = 1$: $(-137, 61)$
Donc on a $187 \times -137 \equiv 1[420]$, autrement dit $187 \times 283 \equiv 1[420]$

(c) Résoudre $338x \equiv 1[420]$
Impossible, car $pgcd(338, 420) = 2$ (donc pas inversible dans Z/420Z)

(d) Résoudre $209x \equiv 1[420]$
Faisable car $pgcd(209, 420) = 1$
Solution particulière de l'équation $209u + 420v = 1$: $(209, -104)$
Donc on a $209 \times 209 \equiv 1[420]$.

Exercice 3

Résoudre dans $\mathbb{Z}$ les équations suivantes :

1. $7x \equiv 2 \pmod 9$.
2. $98x \equiv 79 \pmod{144}$.
3. $98x \equiv 4 \pmod{144}$.

Corrigé :

1. Résoudre $7x \equiv 2[9]$
   La solution existe car 7 est premier, donc 7 est premier avec 9, donc leur pgcd divise 2, la solution cherchée. Solution particulière de l'équation $7u + 9v = 1$: $(4, -3)$. On a donc $7u \equiv 1[9]$, mais aussi $7x \equiv 2[9]$. On a donc $7ux \equiv 2u[9]$ et donc $x \equiv 2u[9]$. Finalement, $x \equiv 8[9]$.
2. on a pgcd(98,144)=2, et 79 impair, donc il n'y a pas de solution.
3. l'équation équivaut à $49x \equiv 2[72]$, que l'on peut résoudre en utilisant les résultats de l'exercice précédent

Exercice 4

On considère le chiffrement affine dans $\mathbb{Z}/76\mathbb{Z}$.

1. Combien existe-t-il de clés valides ?
2. Supposons que la clé secrète est $k = (9, 3)$. Calculer la fonction de déchiffrement.
3. Même question avec $2\,\mathrm{ppcm}(a, b) + 7\,\mathrm{pgcd}(a, b) = 111$.

Corrigé :

1. on a $76 = 4 * 19$ d'où $\varphi(76) = 2 * 18 = 36$
2. La clé secrète est $k = (a,\, b) = (9, 3)$

   Le problème revient à résoudre $y \equiv ax+b(\mathrm{mod}\, n)$ **et plus généralement : résolution des équations de la forme** $ax \equiv c(\mathrm{mod}\, n)$

   c.-à-d. y=9x+3 [76] d'où 9x=y-3 [76].
   Avec Euclide inversé on trouve que l'inverse de 9 modulo 76 est 17.

   $$\begin{aligned} 1 &= 9 - 4 \times 2 \\ &= 9 - (76 - 9 \times 8) \times 2 \\ &= 76 \times (-2) + 9 \times 17 \end{aligned}$$
   $(\overline{9})^{-1} = 17 (9 \times 17 = 153 = 2 * 76 + 1)$.

   D'où $x = 17(y - 3) = 17y - 51 = 17y + 25$ conclusion : d_k(y)=17y+25

Exercice 5

On considère le chiffrement affine dans $\mathbb{Z}/26\mathbb{Z}$.

1. On dispose des couples clair/chiffré (3, 10) et (10, 21). Quelle est la clé utilisée ?
2. Supposons que la clé secrète est $k = (9; 3)$. Calculer la fonction de déchiffrement.
3. Même question avec les couples clair/chiffré (3, 10) et (11, 22).

Corrigé :

1. il faut résoudre le système
   3a+b=10 [26]
   10a+b=21 [26]
   si on soustrait la 1ere eq à la 2eme on obtient 7a=11 [26]
   On calcule l'inverse de 7 mod 26 qui vaut 15, d'ou a=15*11=9 [26] puis b=10-3a=10-27=-17=9 [26]
   la clé est donc k=(9,9)

2. il faut résoudre
   3a+b=10 [26]
   11a+b=22 [26]
   si on soustrait la 1ere eq à la 2eme on obtient 8a=12 [26] qui équivaut à 4a=6[13]
   l'inverse de 4 mod 13 est 10, d'où a=10*6=60=8 [13]
   on en déduit donc que a est de la forme 8+13k, donc la valeur de a mod 26 est soit 8, soit 21. La valeur 8 est interdite car pour avoir une clé valide il faut pgcd(a,26)=1, et on a pgcd(8,26)=2. Donc a=21, puis b=10-3*21=-53=25
   la clé est donc k=(21,25)

Exercice 6

Démontrer que pour tout $n \geq 2$ on a

$$n = \sum_{d|n} \varphi(d)$$

Indice : si l'on met les n fractions $1/n$, $2/n$, ..., n/n, sous forme irréductible, quels sont les dénominateurs possibles ?

Corrigé :

Démonstration :
On considère les n fractions suivantes $1/n$, $2/n$, ..., $(n-1)/n$, n/n. On cherche à les mettre sous forme irréductible a/d, avec $pgcd(a, d) = 1$. On a nécessairement $d|n$. L'ensemble des d forme donc l'ensemble des diviseurs de n. Pour chaque d, il y a $\varphi(d)$ numérateurs a qui apparaissent. Donc si on considère un sous-ensemble constitué des fractions de dénominateur d, il contient $\varphi(d)$ éléments. Le nombre total de fraction est n, de manière évidente la somme des cardinaux de chaque sous-ensemble est n aussi donc on en déduit le résultat.