Compléments en Mathématiques Discrètes: Cours 2 .

Michaël Quisquater (Maître de Conférences,UVSQ)

Rappel du cours 1

- Opération binaire, associativité, commutativité, neutre, inverse
- Groupe, sous-groupe
- Anneau
- Corps, corps commutatif
- Les structures algébriques des entiers

Notion de plus grand commun diviseur

Définition

Le plus grand commun diviseur de $a, b \in \mathbb{Z}$ *est un naturel* $d \in \mathbb{N}$ *tel que* $d \mid a$ *et* $d \mid b$ *et s'il existe un naturel* $d' \in \mathbb{N}$ *tel que* $d' \mid a$ *et* $d' \mid b$ *alors* $d' \mid d$.

Le symbole $pgcd(a, b)$ *représentera ce nombre.*

Rem.: $pgcd(a, b) = pgcd(b, a) = pgcd(-a, b)$, $pgcd(0, 0)??$.

Exemple:

- $2 \mid 30$ et $2 \mid 36$
- $6 \mid 30$ et $6 \mid 36$ donc 2 n'est pas $pgcd(30, 36)$.
- Aucun nombre plus grand que 6 divise 30 et 36. Donc $pgcd(30, 36) = 6$.

Relative primalité

Définition

Deux entiers a et b sont dits relativement premiers si $pgcd(a, b) = 1$.

Remarque: Notons qu'un nombre premier est relativement premier aux nombres qui lui sont strictement inférieurs.

Calcul de pgcd: Première méthode

Première méthode: conséquence du théorème fondamental de l'arithmétique:

Corollaire

Considérons les naturels non-nuls a et b et leur factorisation $a = \prod_{i \in I} p_i^{\alpha_i}$ et $b = \prod_{j \in J} p_j^{\beta_j}$ avec $I, J \subset \mathbb{N}_0$ et avec $\alpha_i, \beta_j \in \mathbb{N}_0$ pour $i \in I$ et $j \in J$. Alors, le plus grand commun diviseur positif de ces nombres est donné par la formule:

$$pgcd(a, b) = \prod_{i \in I \cap J} p_i^{\min(\alpha_i, \beta_i)} .$$

De plus, si a est un naturel non-nul et b est nul, alors $pgcd(a, 0) = a$.

Notion de plus grand commun diviseur
Calcul de pgcd
Théorème de Bezout et algorithme d'Euclide étendu
Classe et relation d'équivalence
Conclusion
Via la factorisation
Via l'algorithme d'Euclide

Calcul de pgcd: Première méthode (exemple)

Exemple: Considérons les nombres $15 = 3 \cdot 5$ et $18 = 2 \cdot 3^2$. Nous avons

$$15 = \prod_{i \in I} p_i^{\alpha_i} \text{ avec } I = \{2, 3\}, p_2 = 3, p_3 = 5 \text{ et } \alpha_2 = 1, \alpha_3 = 1 ,$$

et

$$18 = \prod_{i \in J} p_i^{\beta_i} \text{ avec } J = \{1, 2\}, p_1 = 2, p_2 = 3 \text{ et } \beta_1 = 1, \beta_2 = 2 .$$

Par conséquent, $I \cap J = \{2\}$. Il s'ensuit

$$pgcd(15, 18) = \prod_{i \in I \cap J} p_i^{\min(\alpha_i, \beta_i)} = p_2^{min(1,2)} = 3^{min(1,2)} = 3 .$$

Calcul de pgcd: Deuxième méthode

La première méthode nécessite la factorisation des nombres $\rightarrow$ difficile!

Une autre méthode existe et est appelée "algorithme d'Euclide". Elle est basée sur le résultat suivant:

Théorème

Considérons les entiers $a, b, c \in \mathbb{Z}$. Alors,

$$pgcd(a, b) = pgcd(a + b \cdot c, b)\,.$$

Calcul de pgcd: Deuxième méthode (suite)

Preuve. Soit $d_1 = pgcd(a, b)$ et $d_2 = pgcd(a + b \cdot c, b)$, $c \in \mathbb{Z}$
Montrons que $d_1 \mid d_2$. Par définition du pgcd, d_1 divise a et b. Par conséquent, d_1 divise $a + b \cdot c$ et b. Par la définition du pgcd, nous déduisons que $d_1 \mid d_2$ ou encore

$$d_2 = s \cdot d_1 \text{ pour } s \in \mathbb{Z}. \tag{1}$$

Montrons que $d_2 \mid d_1$. Appliquons le point précédent aux nombres $a = a + b \cdot c$ et $b = b$ et $c = -c$. Nous avons $pgcd(a + b \cdot c, b) \mid pgcd((a + b \cdot c) + b \cdot (-c), b) = pgcd(a, b)$ ou

$$d_1 = s' \cdot d_2 \text{ pour } s' \in \mathbb{Z}. \tag{2}$$

(2) et (1) $\rightarrow s \cdot s' = 1$. Par conséquent, $s = s' = 1$ ou $s = s' = -1$. Comme le pgcd est toujours positif, seul le cas $s = s' = 1$ est possible. Le résultat suit.

Calcul de pgcd: Deuxième méthode (algorithme d'Euclide)

$pgcd(126, 35)$?

Observons que $126 = 35 \cdot 3 + 21$ (on divise 126 par 35). Donc,

$$pgcd(126, 35) = pgcd(35 \cdot 3 + 21, 35) = pgcd(35, 21)$$

De même, $35 = 21 \cdot 1 + 14$. Donc,

$$pgcd(35, 21) = pgcd(21 \cdot 1 + 14, 21) = pgcd(21, 14)$$

Aussi, $21 = 14 \cdot 1 + 7$. Donc,

$$pgcd(21, 14) = pgcd(14 \cdot 1 + 7, 14) = pgcd(14, 7)$$

Finalement, $14 = 7 \cdot 2 + 0$. Donc,

$$pgcd(14, 7) = pgcd(7 \cdot 2 + 0, 7) = pgcd(7, 0) = 7$$

Calcul de pgcd: Deuxième méthode (suite)

Conclusions: Pour calculer le plus grand commun diviseur de deux entiers r_0 et r_1 (non-nuls simultanément), il suffit d'effectuer la séquence des divisions Euclidiennes:

$$\begin{aligned}
r_0 &= r_1 \cdot q_1 + r_2 \\
r_1 &= r_2 \cdot q_2 + r_3 \\
r_2 &= r_3 \cdot q_3 + r_4 \\
&\cdots \\
r_{n-2} &= r_{n-1} \cdot q_{n-1} + r_n \\
r_{n-1} &= r_n \cdot q_n + 0
\end{aligned}$$

Le dernier reste non-nul est le $pgcd(r_0, r_1)$

Remarque: la séquence s'arrêtera toujours car les restes r_i's sont strictement décroissants.

Calcul de pgcd: Deuxième méthode (algorithme d'Euclide)

Algorithme 1 : Algorithme d'Euclide: Calcul de pgcd

Données : $a, b \in \mathbb{Z}$ non-nuls simultanément.
Résultat : $pgcd(a, b)$
$r_0 = \mid a \mid, r_1 = \mid b \mid, k = 1.$
tant que $r_k \neq 0$ **faire**
  $r_{k+1} :=$ le reste de la division de r_{k-1} par r_k
  $k = k + 1$
fin
retourner $pgcd(a, b) = r_{k-1}$.

Calcul de pgcd: Algorithme d'Euclide (exemple): bis

Exemple: $pgcd(126, 35)$

$$r_0 = 126,\ r_1 = 35,\ r_2 = 21,\ r_3 = 14,\ r_4 = 7 \text{ et } r_5 = 0.$$

Le pgcd est donc 7.

Théorème de Bezout: introduction

Imaginez un groom qui travaille dans un hôtel de luxe. Sa fonction consiste à effectuer le service d'étage. Cet hôtel est tellement imposant que l'on peut considérer qu'il possède un nombre infini d'étages positifs et négatifs.

Un jour, en arrivant à l'hôtel, notre apprenti groom se rend compte que l'unique ascenceur de l'hôtel ne peut plus monter et descendre que par 5 ou 7 étages, relativement à l'étage où il est arrêté. L'ascenseur s'arrête par contre à n'importe quel étage si on l'appelle.

Notre groom pourra-t-il n'utiliser que l'ascenceur (et non pas l'escalier) pour accéder à tous les étages et effectuer ainsi son service à moindre fatigue?

Théorème de Bezout: introduction (suite)

Question: notre groom est-il capable d'accéder à tous les étages, à partir d'un étage donné?

Simplification: Peut-il peut accéder au premier étage en partant du rdc?

Cela revient à se demander si en montant (resp. descendant) x fois de 7 étages et en descendant (resp. montant) y fois de 5 étages, il arrive au premier.

Théorème de Bezout: introduction (suite)

Modélisation

Existe-t-il $x, y \in \mathbb{Z}$ tels que $7 \cdot x + 5 \cdot y = 1$?

Solution: Observons que pour $x = 3$ et $y = -4$ la relation est vérifiée. Le groom devra dont monter 3 fois de 7 étages et ensuite descendre 4 fois de 5 étages pour arriver au premier.

Solution du cas général: Le groom pourra également arriver au -1 en inversant la procédure; cela revient à multiplier x et y par -1. Finalement, il pourra accéder à n'importe quel étage z en multipliant x et y par z.

Théorème de Bezout: introduction (suite)

Remarque: si les nombres $a = 7$ et $b = 5$ n'avaient pas étés relativement premiers, le problème aurait été sans solution.

En effet, dans ce cas il existe $k \in \mathbb{Z}$ (différent de -1 et 1) tel que $a = k \cdot a'$ et $b = k \cdot b'$.

Par conséquent, le problème revient à déterminer $x, y \in \mathbb{Z}$ tels que $k \cdot a'x + k \cdot b'y = 1$. Cette dernière identité est impossible car le membre de gauche est un multiple k (différent de -1 et 1) de $a' \cdot x + b' \cdot y$ et ne peut donc pas être égal à 1.

Le théorème de Bezout répond à la question d'existence de solution de l'équation $a \cdot x + b \cdot y = c$ dans un cas assez général.

Théorème de Bezout

Théorème

(Théorème de Bezout) Soit deux entiers a et b non simultanément nuls. Alors, il existe $x, y \in \mathbb{Z}$ tel que

$$a \cdot x + b \cdot y = pgcd(a, b) .$$

Les nombres x et y sont appelés les coefficients de Bezout.

Théorème de Bezout (intuition de la preuve)

Reprenons notre exemple: soit $a = 126$ et $b = 35$.

On cherche $x, y \in \mathbb{Z}$ tels que $126x + 35y = pgcd(126, 25) = 7$

Considérons la séquence de divisions Euclidiennes:

$$\begin{array}{ll}
126 = 35 \cdot 3 + 21 & 21 = 126 - 35 \cdot 3 \\
35 = 21 \cdot 1 + 14 & 14 = 35 - 21 \cdot 1 \\
21 = 14 \cdot 1 + 7 & 7 = 21 - 14 \cdot 1 \\
14 = 7 \cdot 2 + 0 & 0 = 14 - 7 \cdot 2
\end{array}$$

But: Exprimer 7 en fonction de 126 et 35.

Méthode: exprimer successivement 126, 35, 21,14 et 7 en fonction de 126 et 35

Théorème de Bezout (intuition de la preuve)

$$\begin{aligned} r_0 &= 126 = 1 \cdot 126 + 0 \cdot 35 \\ r_1 &= 35 = 0 \cdot 126 + 1 \cdot 35 \\ r_2 &= 21 = 126 - 35 \cdot 3 \\ r_3 &= 14 = 35 - 21 \cdot 1 \\ r_4 &= 7 = 21 - 14 \cdot 1 \\ r_5 &= 0 = 14 - 7 \cdot 2 \end{aligned}$$

$$\begin{aligned} r_0 &= x_0 \cdot 126 + y_0 \cdot 35 \\ r_1 &= x_1 \cdot 126 + y_1 \cdot 35 \\ r_2 &= (x_0 \cdot 126 + y_0 \cdot 35) - q_1 \cdot (x_1 \cdot 126 + y_1 \cdot 35) \\ r_3 &= \\ r_4 &= \end{aligned}$$

Notion de plus grand commun diviseur
Calcul de pgcd
Théorème de Bezout et algorithme d'Euclide étendu
Classe et relation d'équivalence
Conclusion
Théorème de Bezout
Algorithme d'Euclide étendu

Théorème de Bezout (intuition de la preuve)

$$\begin{aligned} r_0 &= 126 = 1 \cdot 126 + 0 \cdot 35 \\ r_1 &= 35 = 0 \cdot 126 + 1 \cdot 35 \\ r_2 &= 21 = 126 - 35 \cdot 3 \\ r_3 &= 14 = 35 - 21 \cdot 1 \\ r_4 &= 7 = 21 - 14 \cdot 1 \\ r_5 &= 0 = 14 - 7 \cdot 2 \end{aligned}$$

$$\begin{aligned} r_0 &= x_0 \cdot 126 + y_0 \cdot 35 \\ r_1 &= x_1 \cdot 126 + y_1 \cdot 35 \\ r_2 &= (x_0 - q_1 x_1) \cdot 126 + (y_0 - q_1 y_1) \cdot 35 \\ r_3 &= \\ r_4 &= \end{aligned}$$

19 / 32 Michaël Quisquater (Maître de Conférences,UVSQ) Compléments en Mathématiques Discrètes: Cours 2 .

Théorème de Bezout (intuition de la preuve)

$$
\begin{aligned}
r_0 &= 126 = 1 \cdot 126 + 0 \cdot 35 \\
r_1 &= 35 = 0 \cdot 126 + 1 \cdot 35 \\
r_2 &= 21 = 126 - 35 \cdot 3 \\
r_3 &= 14 = 35 - 21 \cdot 1 \\
r_4 &= 7 = 21 - 14 \cdot 1 \\
r_5 &= 0 = 14 - 7 \cdot 2
\end{aligned}
$$

$$
\begin{aligned}
r_0 &= x_0 \cdot 126 + y_0 \cdot 35 \\
r_1 &= x_1 \cdot 126 + y_1 \cdot 35 \\
r_2 &= x_2 \cdot 126 + y_2 \cdot 35 \\
r_3 &= \\
r_4 &=
\end{aligned}
$$

Notion de plus grand commun diviseur
Calcul de pgcd
Théorème de Bezout et algorithme d'Euclide étendu
Classe et relation d'équivalence
Conclusion
Théorème de Bezout
Algorithme d'Euclide étendu

Théorème de Bezout (intuition de la preuve)

$$
\begin{aligned}
r_0 &= 126 = 1 \cdot 126 + 0 \cdot 35 \\
r_1 &= 35 = 0 \cdot 126 + 1 \cdot 35 \\
r_2 &= 21 = 126 - 35 \cdot 3 \\
r_3 &= 14 = 35 - 21 \cdot 1 \\
r_4 &= 7 = 21 - 14 \cdot 1 \\
r_5 &= 0 = 14 - 7 \cdot 2
\end{aligned}
$$

$$
\begin{aligned}
r_0 &= x_0 \cdot 126 + y_0 \cdot 35 \\
r_1 &= x_1 \cdot 126 + y_1 \cdot 35 \\
r_2 &= x_2 \cdot 126 + y_2 \cdot 35 \\
r_3 &= (x_1 \cdot 126 + y_1 \cdot 35) - q_2 \cdot (x_2 \cdot 126 + y_2 \cdot 35) \\
r_4 &=
\end{aligned}
$$

19 / 32 Michaël Quisquater (Maître de Conférences,UVSQ) Compléments en Mathématiques Discrètes: Cours 2 .

Théorème de Bezout (intuition de la preuve)

$$\begin{aligned} r_0 &= 126 = 1 \cdot 126 + 0 \cdot 35 \\ r_1 &= 35 = 0 \cdot 126 + 1 \cdot 35 \\ r_2 &= 21 = 126 - 35 \cdot 3 \\ r_3 &= 14 = 35 - 21 \cdot 1 \\ r_4 &= 7 = 21 - 14 \cdot 1 \\ r_5 &= 0 = 14 - 7 \cdot 2 \end{aligned}$$

$$\begin{aligned} r_0 &= x_0 \cdot 126 + y_0 \cdot 35 \\ r_1 &= x_1 \cdot 126 + y_1 \cdot 35 \\ r_2 &= \ x_2 \cdot 126 + y_2 \cdot 35 \\ r_3 &= (x_1 - q_2 x_2) \cdot 126 + (y_1 - q_2 y_2) \cdot 35 \\ r_4 &= \end{aligned}$$

Notion de plus grand commun diviseur
Calcul de pgcd
Théorème de Bezout et algorithme d'Euclide étendu
Classe et relation d'équivalence
Conclusion
Théorème de Bezout
Algorithme d'Euclide étendu

Théorème de Bezout (intuition de la preuve)

$$\begin{aligned} r_0 &= 126 = 1 \cdot 126 + 0 \cdot 35 \\ r_1 &= 35 = 0 \cdot 126 + 1 \cdot 35 \\ r_2 &= 21 = 126 - 35 \cdot 3 \\ r_3 &= 14 = 35 - 21 \cdot 1 \\ r_4 &= 7 = 21 - 14 \cdot 1 \\ r_5 &= 0 = 14 - 7 \cdot 2 \end{aligned}$$

$$\begin{aligned} r_0 &= x_0 \cdot 126 + y_0 \cdot 35 \\ r_1 &= x_1 \cdot 126 + y_1 \cdot 35 \\ r_2 &= \ x_2 \cdot 126 + y_2 \cdot 35 \\ r_3 &= \ x_3 \cdot 126 + y_3 \cdot 35 \\ r_4 &= \end{aligned}$$

Théorème de Bezout (intuition de la preuve)

$$\begin{aligned}
r_0 &= 126 = 1 \cdot 126 + 0 \cdot 35 \\
r_1 &= 35 = 0 \cdot 126 + 1 \cdot 35 \\
r_2 &= 21 = 126 - 35 \cdot 3 \\
r_3 &= 14 = 35 - 21 \cdot 1 \\
r_4 &= 7 = 21 - 14 \cdot 1 \\
r_5 &= 0 = 14 - 7 \cdot 2
\end{aligned}$$

$$\begin{aligned}
r_0 &= x_0 \cdot 126 + y_0 \cdot 35 \\
r_1 &= x_1 \cdot 126 + y_1 \cdot 35 \\
r_2 &= x_2 \cdot 126 + y_2 \cdot 35 \\
r_3 &= x_3 \cdot 126 + y_3 \cdot 35 \\
r_4 &= (x_2 \cdot 126 + y_2 \cdot 35) - q_3 \cdot (x_3 \cdot 126 + y_3 \cdot 35)
\end{aligned}$$

Notion de plus grand commun diviseur
Calcul de pgcd
Théorème de Bezout et algorithme d'Euclide étendu
Classe et relation d'équivalence
Conclusion
Théorème de Bezout
Algorithme d'Euclide étendu

Théorème de Bezout (intuition de la preuve)

$$\begin{aligned}
r_0 &= 126 = 1 \cdot 126 + 0 \cdot 35 \\
r_1 &= 35 = 0 \cdot 126 + 1 \cdot 35 \\
r_2 &= 21 = 126 - 35 \cdot 3 \\
r_3 &= 14 = 35 - 21 \cdot 1 \\
r_4 &= 7 = 21 - 14 \cdot 1 \\
r_5 &= 0 = 14 - 7 \cdot 2
\end{aligned}$$

$$\begin{aligned}
r_0 &= x_0 \cdot 126 + y_0 \cdot 35 \\
r_1 &= x_1 \cdot 126 + y_1 \cdot 35 \\
r_2 &= x_2 \cdot 126 + y_2 \cdot 35 \\
r_3 &= x_3 \cdot 126 + y_3 \cdot 35 \\
r_4 &= (x_2 - q_3 x_3) \cdot 126 + (y_2 - q_3 y_3) \cdot 35
\end{aligned}$$

19 / 32 Michaël Quisquater (Maître de Conférences,UVSQ) Compléments en Mathématiques Discrètes: Cours 2 .

Théorème de Bezout (intuition de la preuve)

$r_0 = 126 = 1 \cdot 126 + 0 \cdot 35$
$r_1 = 35 = 0 \cdot 126 + 1 \cdot 35$
$r_2 = 21 = 126 - 35 \cdot 3$
$r_3 = 14 = 35 - 21 \cdot 1$
$r_4 = 7 = 21 - 14 \cdot 1$
$r_5 = 0 = 14 - 7 \cdot 2$

$r_0 = x_0 \cdot 126 + y_0 \cdot 35$
$r_1 = x_1 \cdot 126 + y_1 \cdot 35$
$r_2 = x_2 \cdot 126 + y_2 \cdot 35$
$r_3 = x_3 \cdot 126 + y_3 \cdot 35$
$r_4 = x_4 \cdot 126 + y_4 \cdot 35$

Théorème de Bezout (intuition de la preuve)

Conclusion:

- $x_0 = 1$, $y_0 = 0$, $x_1 = 0$ et $y_1 = 1$
- $x_{k+1} = x_{k-1} - q_k \cdot x_k$
- $y_{k+1} = y_{k-1} - q_k \cdot y_k$
- Les x_i et y_i correspondants au dernier reste non-nuls sont les coefficients cherchés.

Remarque: Rigoureusement, il faudrait prouver ces formules par récurrence (hors du cadre du cours)

Algorithme d'Euclide étendu: Calcul des coefficients de Bezout.

Algorithme 2 : Algorithme d'Euclide Etendu

Données : $a, b \in \mathbb{Z}$ non-nuls simultanément.
Résultat : $pgcd(a, b)$ et $x, y \in \mathbb{Z}$ tels que $ax + by = pgcd(a, b)$
$r_0 =| a |$, $r_1 =| b |$, $x_0 = 1$, $x_1 = 0$, $y_0 = 0$, $y_1 = 1$, $k = 1$.

tant que $r_k \neq 0$ **faire**
- $r_{k+1} :=$ reste de la division de r_{k-1} par r_k;
- $q_k :=$ quotient de la division de r_{k-1} par r_k;
- $x_{k+1} = -q_k \cdot x_k + x_{k-1}$;
- $y_{k+1} = -q_k \cdot y_k + y_{k-1}$;
- $k = k + 1$

fin
retourner $pgcd(x, y) = r_{k-1}$, $x = x_{k-1}$, $y = y_{k-1}$.

Algorithme d'Euclide étendu (exemple)

- Exemple: $a = 126$ et $b = 35$.

k	0	1	2	3	4	5
r_k	126	35	21	14	7	0
q_k	-	3	1	1	2	-
x_k	1	0	1	-1	2	-
y_k	0	1	-3	4	-7	-

On a donc que le $pgcd(126, 35) = 7$ et $x = 2$, $y = -7$.

Par conséquent, $126 \cdot 2 - 7 \cdot 35 = 7$.

Motivation

Observation: On ne peut représenter qu'un nombre fini de nombres dans un ordinateur (lié à la mémoire).

Conséquence: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sont des structures mal adaptées pour des calculs sur ordinateur (il existe cependant des parades).

Objectif: Construire des groupes, anneaux, corps (commutatifs) possédant un nombre fini d'éléments.

Bonus: les structures construites bénéficieront de propriétés additionnelles très utiles en cryptographie (vrai raison de ces structures)

Stratégie pour construire de nouveaux espaces

Idée1: Découper un espace possédant un nombre infini d'éléments en un nombre fini de sous-ensemble infinis.

Idée2: Définir une opération d'addition (resp. multiplications) sur ces sous-ensembles infinis. Cela signifie quà deux sous-ensembles on a va associer un troisième sous-ensemble. De même que 3+4=7 revient à associer aux nombres 3 et 4 le nombre 7.

Idée3: Représenter chacun des sous-ensemble par un de ses éléments et reconstruire la table en fonction de cette représentation.

Construction d'un groupe additif à deux éléments

- Découpe de l'ensemble des entiers en le sous-ensemble des nombres pairs et impairs.
- Définition d'une opération d'addition sur ces sous-ens.:

+	P	I
P	P	I
I	I	P

- On peut représenter, par exemple, les nombres pairs (resp. impairs) par 0 (resp. par 1). On obtient la table:

+	0	1
0	0	1
1	1	0

Construction d'un groupe additif à deux éléments

Remarques:

- Groupe additif fini commutatif (Exercice!)
- $1 + 1 = 0$: attention à l'interprétation!
- l'opération $+$ correspond au "XOR"

Généralisation à n éléments?

> ”Dieu a inventé les nombres entiers, le reste est l'oeuvre des hommes”
>
> Kronecker (1823-1891)

- Comment découper $\mathbb{Z}$ en utilisant l'addition entière?
- Comment définir la correspondance (opération) entre les sous-ensembles en utilisant l'addition entière?
- Comment choisir un représentant de chaque sous-ensemble?
- Est-il possible de définir deux opérations de cette façon afin de construire un anneau?

Notion de classe de congruence modulo n

Objectif: Décrire une façon systématique de découper /partitionner l'ensemble des entiers en sous-ensembles.

Intuition: On a déja évoqué le partitionnement en les nombres pairs et impairs (voir ci-dessus).

Objectif intermédiaire: Comment partitionner les entiers en 7 morceaux?

- semaine=7 jours (lundi, mardi, mercredi, jeudi, vendredi, samedi, dimanche)
- L'ensemble des jours peut être divisé en l'ensemble des lundis, mardis etc. Du point de vue de la position du jour de la semaine, tous les jours appartenant à un de ces ensembles sont équivalents.

Notion de classe de congruence modulo n (suite)

Modélisons mathématiquement la notion de lundi, mardi etc.

Associons à chaque jour un élément de $\mathbb{Z}$. En particulier, nous avons les classes suivantes:

- Lu=$\{\ldots, -14, -7, 0, 7, 14, 21, \ldots\}$,
- Ma=$\{\ldots, -13, -6, 1, 8, 15, 22, \ldots\}$,
- Me=$\{\ldots, -12, -5, 2, 9, 16, 23, \ldots\}$,
- Je=$\{\ldots, -11, -4, 3, 10, 17, 24, \ldots\}$,
- Ve=$\{\ldots, -10, -3, 4, 11, 18, 25, \ldots\}$,
- Sa=$\{\ldots, -9, -2, 5, 12, 19, 26, \ldots\}$,
- Di=$\{\ldots, -8, -1, 6, 13, 20, 27, \ldots\}$,

Chaque nombre de $\mathbb{Z}$ appartient un et un seul ensemble (partition).

Notion de plus grand commun diviseur
Calcul de pgcd
Théorème de Bezout et algorithme d'Euclide étendu
Classe et relation d'équivalence
Conclusion
Motivation
Stratégie
Exemple introductif
Notion relation/classe d'équivalence modulo n

Notion de classe de congruence modulo n (suite)

On peut exprimer tout ce qui précède simplement en introduisant la notion de relation d'équivalence ou de congruence.

Définition (Relation d'équivalence ou de congruence modulo n)

Soit $n \in \mathbb{N}$. Deux éléments $x, y \in \mathbb{Z}$ sont dits équivalents, i.e. $x \sim_n y$, si et seulement si

$$x - y \text{ est un multiple de } n\,.$$

(on lit "x est équivalent à y" ou x est congru à y modulo n)

Cette procédure nous permet de "diviser" l'ensemble $\mathbb{Z}$ en morceau que l'on appelera "classe d'équivalence" ou classe de congruence.

Notion de classe de congruence modulo n (suite)

- Une classe d'équivalence $[a+n\mathbb{Z}]$ est définie comme l'ensemble des éléments de $\mathbb{Z}$ équivalents à a, i.e.

$$[a+n\mathbb{Z}] = \{x \in \mathbb{Z} \mid x \sim_n a\}\ .$$

- L'élément a est appelé le représentant de la classe a (pas unique!).
- Si a est le plus petit entier positif de la classe, il est dit minimal.
- Chaque élément de $\mathbb{Z}$ appartient à une et une seule classe d'équivalence.
- Une classe $[a+n\mathbb{Z}]$ est souvent notée de façon plus concise par $\overline{a}$ quand le contexte le permet.

Conclusion

- Notion de plus grand commun diviseur (pgcd)
- Calcul de pgcd (via la factorisation, algorithme d'Euclide)
- Théorème de Bezout et algorithme d'Euclide étendu
- Construction d'un groupe additif à deux éléments et généralisation?