7.6. **L'algorithme de Bézout-Euclide.** Soient $a > b$ deux nombres naturels. Si $b = 0$ alors $\text{pgcd}(a, b) = 0$. Si $b \neq 0$ il existe nombres naturels q, r tels que $a = qb + r$ et $0 \leq r < b$ et $\text{pgcd}(a, b) = \text{pgcd}(b, r)$, par lemme 7.2. C'est une étape dans l'algorithme d'Euclide pour calculer le $\text{pgcd}(a, b)$. Nous n'avons par montré ce lemme encore, car nous voulons faire un peu plus !

Lemme 7.3. *Soient $a > b$ deux nombres naturels et $d = \text{pgcd}(a, b)$.*

Si $b = 0$ alors $\text{pgcd}(a, b) = a$ et $d = 1 \cdot a + 0 \cdot b$.

Si $b \neq 0$, par division avec reste il existe des entiers q et r tels que $a = qb + r$ et $0 \leq r < b$.

(i) Alors $d = \text{pgcd}(a, b) = \text{pgcd}(b, r)$.

(ii) Si $d = sb + tr$, pour deux entiers s, t, alors $d = ta + (s - tq)b$.

Ou en mots : si on peut écrire d comme une combinaison $\mathbb{Z}$-linéaire de b et r, alors on peut aussi écrire d comme une combinaison $\mathbb{Z}$-linéaire de a et b.

Démonstration. (i) Soit $n \geq 1$ un diviseur de b. Si $n|a$, alors aussi $n|(a - qb)$ et $n|r$. par contre si $n|r$, aussi $d|(qb + r)$ et $n|a$. En mots : n est diviseur en commun de a et b si et seulement si n est diviseur en commun de b et r. En particulier, $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

(ii) Par substitution

$$d = sb + tr = sb + t(a - qb) = ta + (s - tq)b.$$

□

Ce lemme nous donne par récurrence un façon de trouver deux entiers s, t tel que $sa + tb = \text{pgcd}(a, b)$. Après avoir utlisé l'algorithme d'Euclide pour calculer le pgcd, on monte du bas vers le haut.

7.7. **Méthode par substitutions.** Nous référons au calcul de $\text{pgcd}(1351, 1064)$. On avait :

$$\begin{aligned}
1351 &= 1 \cdot 1064 + 287 \\
1064 &= 3 \cdot 287 + 203 \\
287 &= 1 \cdot 203 + 84 \\
203 &= 2 \cdot 84 + 35 \\
84 &= 2 \cdot 35 + 14 \\
35 &= 2 \cdot 14 + 7 \\
14 &= 2 \cdot 7 + 0.
\end{aligned}$$

Ce qui donne

$$\begin{aligned} 287 &= 1351 - 1 \cdot 1064 \\ 203 &= 1064 - 3 \cdot 287 \\ 84 &= 287 - 1 \cdot 203 \\ 35 &= 203 - 2 \cdot 84 \\ 14 &= 84 - 2 \cdot 35 \\ 7 &= 35 - 2 \cdot 14 \\ 0 &= 14 - 2 \cdot 7. \end{aligned}$$

En commençant par

$$7 = 35 - 2 \cdot 14,$$

on monte successivement dans la chaîne des divisions-avec-restes d'Euclide. On substitue le reste obtenu dans l'étape avant, puis on fait une réarrangement des termes, et on obtient une autre combinaison $\mathbb{Z}$-linéaire.

En exemple : On substitue $14 = 84 - 2 \cdot 35$ dans $7 = 35 - 2 \cdot 14$, puis on réarrange, et on obtient $-2 \cdot 84 + 5 \cdot 35$. Et on continue. Voir aussi [R, Exemple 1,p. 129], pour cette méthode-par-substitutions. Explicitement :

$$\begin{aligned} 7 &= 35 - 2 \cdot 14 = 35 - 2 \cdot (84 - 2 \cdot 35) = \\ &= -2 \cdot 84 + 5 \cdot 35 = -2 \cdot 84 + 5 \cdot (203 - 2 \cdot 84) = \\ &= 5 \cdot 203 + (-12) \cdot 84 = 5 \cdot 203 + (-12) \cdot (287 - 203) = \\ &= (-12) \cdot 287 + 17 \cdot 203 = (-12) \cdot 287 + 17 \cdot (1064 - 3 \cdot 287) = \\ &= 17 \cdot 1064 + (-63) \cdot 287 = 17 \cdot 1064 + (-63)(1351 - 1064) = \\ &= (-63) \cdot 1351 + 80 \cdot 1064. \end{aligned}$$

En effet $(-63) \cdot 1351 + 80 \cdot 1064 = -85113 + 85120 = 7$ est la combinaison $\mathbb{Z}$-linéaire cherchée.

7.8. **Méthode de Bézout.** Nous préférons une autre méthode. Cette méthode commence en haut avec deux combinaisons $\mathbb{Z}$-linéaire triviales. On descend à droite du "=" selon l'algorithme d'Euclide, et on fait les mêmes soustractions à gauche du "=", pour maintenir le =.

En exemple : On commence avec les deux combinaisons $\mathbb{Z}$-linéaires de 1351 et 1064 triviales :

$$\begin{aligned} 1 \cdot 1351 + 0 \cdot 1064 &= 1351 \\ 0 \cdot 1351 + 1 \cdot 1064 &= 1064 \end{aligned}$$

Parce que $287 = 1351 - 1064$ on a aussi

$$\begin{aligned} 287 &= 1351 - 1064 \\ &= [1 \cdot 1351 + 0 \cdot 1064] - [0 \cdot 1351 + 1 \cdot 1064] \\ &= (1-0) \cdot 1351 + (0-1) \cdot 1064. \end{aligned}$$

D'où une autre combinaison $\mathbb{Z}$-linéaires de 1351 et 1064 :

$$\begin{aligned} 1 \cdot 1351 + 0 \cdot 1064 &= 1351 \\ 0 \cdot 1351 + 1 \cdot 1064 &= 1064 \\ 1 \cdot 1351 + (-1) \cdot 1064 &= 287 \end{aligned}$$

Parce que $1064 - 3 \cdot 287 = 203$ on a aussi

$$\begin{aligned} 203 &= 1064 - 3 \cdot 287 \\ &= [0 \cdot 1351 + 1 \cdot 1064] + (-3) \cdot [1 \cdot 1351 + (-1) \cdot 1064] \\ &= (0-3) \cdot 1351 + (1 + (-3)(-1)) \cdot 1064. \end{aligned}$$

D'où

$$\begin{aligned} 1 \cdot 1351 + 0 \cdot 1064 &= 1351 \\ 0 \cdot 1351 + 1 \cdot 1064 &= 1064 \\ 1 \cdot 1351 + (-1) \cdot 1064 &= 287 \\ (-3) \cdot 1351 + (4) \cdot 1064 &= 203 \end{aligned}$$

On répète et on obtient :

$$\begin{aligned} 1 \cdot 1351 + 0 \cdot 1064 &= 1351 \\ 0 \cdot 1351 + 1 \cdot 1064 &= 1064 \\ 1 \cdot 1351 + (-1) \cdot 1064 &= 287 \\ (-3) \cdot 1351 + (4) \cdot 1064 &= 203 \\ (4) \cdot 1351 + (-5) \cdot 1064 &= 84 \\ (-11) \cdot 1351 + (14) \cdot 1064 &= 35 \\ (26) \cdot 1351 + (-33) \cdot 1064 &= 14 \\ \mathbf{(-63) \cdot 1351 + (80) \cdot 1064} &= \mathbf{7} \end{aligned}$$

Et voilà : la dernière ligne qui correspond au dernier reste non-zéro donne notre réponse : on a écrit le $\text{pgcd}(a, b)$ comme une combinaison $\mathbb{Z}$-linéaires de a et b. Je vois cet algorithme (appelé *l'algorithme de Bézout*) comme l'algorithme de Euclide (la partie droite du "=") renforcé par de l'administration ((la partie gauche du "=") . Ça donne aussi une preuve constructive du théorème

suivant de Bézout ! C'est presque toujours le cas : si on doit calculer quelque chose avec des entiers, l'algorithme de Bézout/Euclide joue un role.

Théorème 7.6 (Bézout)**.** *Soient n, m deux entiers avec $d = \text{pgcd}(n, m)$.*
Alors il existe des entiers s, t tel que $sn + tm = d$.

Démonstration. Sans perte de généralité on peut supposer que n et m sont des nombres naturels. Si $m = 0$, alors $1 \cdot n + 0 \cdot m = d$, si $n \geq 0$ et $-1 \cdot n + 0 \cdot m = d$, si $n < 0$. Et le résultat est vrai.

Si $m > 0$: l'algorithme de Bézout fonctionne pour calculer tels s et t. □

Remarque. On peut aussi donner une preuve par induction. Faire ça !

Une variation en terme d'existence de solutions entières des équations linéaires.

Théorème 7.7. *Soient a, b, c trois nombres entiers. Posons $d = \text{pgcd}(a, b)$.*
Considérons l'équation

$$ax + by = c.$$

Il est possible de résoudre cette équation avec des entiers (c.-à-d. de trouver deux entiers x et y tels que l'équation est satisfaite) si et seulement si $d|c$.

Démonstration. Supposons deux entiers x, y existent tels que $ax + by = c$. On a $d|a$ et $d|b$ donc aussi $d|(ax + by)$ et nécessairement $d|c$.

Par contre, supposons $d|c$. Alors il existe un entier n tel que $c = dn$. Par le théorème de Bézout ils existent deux entiers s, t tels que $d = as + bt$ donc $c = dn = a(sn) + b(tn)$. Et on voit que le pair $x = sn$ et $y = tn$ forme une solution de l'équation. □

Remarque. En algèbre linéaire on étudie la question si (et comment) on peut résoudre les équations linéaires, si les coefficients et les solutions sont éléments d'un corps, par exemple $\mathbb{Q}$. Par exemple avec la méthode de Gauss il est essentiel qu'on peut diviser. Dans notre cas nos coefficients et solutions doivent être dans $\mathbb{Z}$, qui n'est pas un corps (car on ne peut pas diviser en général).

Pour notre équation on peut facilement trouver une solution dans $\mathbb{Q}$ généralement. Par exemple si $a \neq 0$, prends pour y un entier quelconque, et puis pour $x = \frac{c-by}{a}$. Mais il faut bien choisir y pour que $x \in \mathbb{Z}$ aussi, et ça n'est pas toujours possible.

Remarque. Soient a, b, c trois entiers. Posons $d = \text{pgcd}(a, b)$. Considérons l'équation $ax + by = c$, et supposons $d|c$

(i) Le théorème nous dit seulement qu'il y a une solution entière. Mais la preuve nous donne la suggestion comment trouver une solution :

Commence par trouver deux nombres entiers n, m tels que $an + bm = d$, par l'algorithme de Bézout/Euclide. Il existe un entier q tel que $qd = c$. Donc $a(qn) + b(qm) = qd = c$, et on peut prendre $x = qn$ et $y = qm$.

(ii) Il y a d'autres solutions que la solution (x, y) trouvée dans (i). Il existe deux entiers a' et b' tels que $a'd = a$ et $b'd = b$, et $xa' + yb' = 1$ (donc $\text{pgcd}(a, b) = 1$) (pourquoi ?). Soit $h \in \mathbb{Z}$ quelconque. Posons $x' = x + b'h$ et $y' = y - a'h$. Alors

$$ax' + by' = a(x + b'h) + b(y - a'h) = ax + by + (a'db'h - b'da'h) = c;$$

alors (x', y') est aussi une solution entière de l'équation.

7.9. **Conséquences théoriques et pratiques.** Sans doute vous connaissez la propriété suivante d'un nombre premier p : Si p divise un produit de deux nombres entiers, alors p divise l'un ou l'autre (ou tous les deux). Aussi, vous savez probablement que chaque nombre naturel est le produit de nombres premiers, *et* que ce produit est *essentiellement unique*. Est-ce que vous avez jamais vu une preuve de ces résultats (autre que *"le prof (ou le livre) le dit, donc c'est vrai"*) ?

Pour montrer ces résultats il faut utiliser le théorème de Bézout ! ! Je ne connais aucune autre méthode. Donc c'est déjà une raison pourquoi ce théorème est très important et utile, et mérite d'être bien connu par vous.

Théorème 7.8. *(i) Soient a, b, c trois entiers tels que $a|bc$ et $\text{pgcd}(a, b) = 1$. Alors $a|c$.*
(ii) Soit p un nombre premier tel que $p|bc$. Alors $p|b$ ou $p|c$.

Démonstration. (i) Voir aussi [R, p.130, lemme 1]. Par le théorème de Bézout, th. 7.6, ils existent deux entiers s, t tels que $sa + tb = 1$. Donc on a aussi $sac + tbc = c$. Par hypothèse il existe aussi un nombre entier u tel que $au = bc$. Donc en substituant on obtient $c = sac + tau = (sc + tu)a$, ce qui montre que $a|c$.

(ii) Si le nombre premier p ne divise pas b alors le plus grand diviseur en commun est 1. Donc l'hypothése de (i) est satisfaite et on peut conclure. □

Avec plus de facteurs :

Corollaire 7.2. *Si p est un nombre premier tel que $p|(n_1 n_2 \dots n_s)$. Alors il existe un i ($1 \leq i \leq s$) tel que $p|n_i$.*

Voir aussi [R, p.130, lemme 2].

Exercice 7.1. Soient a, b, c trois entiers. Posons $d = \text{pgcd}(a, b)$; il y a donc deux entiers a', b' tels que $a'd = a$, $b'd = b$. Et supposons $d|c$. Supposons aussi $ax + by = c$, et $ax' + by' = c$ pour deux pairs d'entiers (x, y) et (x', y'). Utiliser le théorème pour montrer qu'il existe un entier $h \in \mathbb{Z}$ tel que $(x' - x) = b'h$ et $(y' - y) = -a'h$.

Pourquoi peut-on conclure que la méthode de la remarque précédente produit *tous* les solutions entières de l'équation $ax + by = c$?

7.10. **Factorisation unique.** N'importe quel nombre naturel $n > 1$ s'écrit comme un produit de nombres premiers, disons $n = p_1 p_2 \dots p_s$, comme nous avons déjà montré avec une preuve par induction généreuse. Aprés un réarrangement des facteurs, si nécessaire, on peut supposer que

$$p_1 \leq p_2 \leq p_3 \leq \dots \leq p_s.$$

Après, l'expression devient *unique*. Voir aussi [R, p.105, th. 2 et p.130-131] e

Théorème 7.9. *Soit $n > 1$ un nombre naturel. Si $n = p_1 p_2 \dots p_s$ et $n = q_1 q_2 \dots q_t$ sont deux factorisations de n comme produits de nombres premiers tels que $p_1 \leq p_2 \leq \dots \leq p_s$, et $q_1 \leq q_2 \leq \dots \leq q_t$. Alors $s = t$ et $p_1 = q_1$, $p_2 = q_2, \dots, p_s = q_s$.*

Démonstration. Commençons par remarquer que si $n = p_1 p_2 \dots p_s$, alors chaque p_i est un diviseur de n. Et si p est un nombre premier, alors p n'a pas de diviseur > 1 sauf p. Donc la seule factorisation

première est trivialement : $p = p$. Nous allons montrer l'unicité de la factorisation par induction généreuse.

Le début. Pour $n = 2$ il n'y a qu'une seule factorisation, car 2 est un nombre premier.

Soit $n \geq 2$ et supposons pour chaque $2 \leq m \leq n$ la factorisation première pour m est unique. Si $n+1$ est premier, il y a une seule factorisation, comme déjà remarqué. Supposons $n+1$ est composé et $n+1 = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$ sont deux factorisations ordonnées. Les p_i et q_j sont tous des nombres premiers qui divisent n. Soit $p \geq 2$ le plus petit nombre premier qui divise n. Alors $p | p_1 p_2 \dots p_s$ implique $p = p_i$ pour un i, par cor.7.2. Par minimalité nécessairement $p = p_1$. Et de même façon $p = q_1$. Donc $p_1 = q_1$. Nous avons supposé que $n+1$ n'est pas premier, donc si nous posons $m = p_2 \dots p_s = q_2 \dots q_t$, alors $2 \leq m \leq n$. Donc par l'hypothèse d'induction, m a une seule factorization. C'est à dire $p_2 = q_2$, $p_3 = q_3 \dots$. Donc aussi les deux factorisations de $n+1$ coïncident.

Par induction généreuse on conclut que l'unicité de la factorisation première est vraie. □

Remarque. Soit $n > 1$ alors on peut aussi écrire *uniquement*

$$n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s},$$

où $p_1 < p_2 < \dots < p_s$ sont des nombres premiers et les a_i des nombres naturels.

7.11. **Une autre manière de calculer le** pgcd **et le** ppcm**.** En général, trouver une factorisation première est très laborieux. Mais si on a déjà factorisé n et m on peut facilement calculer $\text{pgcd}(n, m)$.

Théorème 7.10. *Supposons* $n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$, *et* $m = p_1^{b_1} p_2^{b_2} \dots p_s^{b_s}$, *où* $p_1 < p_2 < \dots < p_s$, *les* $a_i \geq 0$ *et les* $b_i \geq 0$.

Alors

$$\text{pgcd}(n, m) = p_1^{c_1} p_2^{c_2} \dots p_s^{c_s},$$

et

$$\text{ppcm}(n, m) = p_1^{d_1} p_2^{d_2} \dots p_s^{d_s},$$

où c_i *est le minimum de* $\{a_i, b_i\}$ *et* d_i *est le maximum de* $\{a_i, b_i\}$.

Démonstration. Voir aussi [R, p. 110] Ce résultat suit de l'observation qu'un nombre naturel $r = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$ divise n si et seulement si $e_1 \leq a_1$, $e_2 \leq a_2$, $\dots$, $e_s \leq a_s$. (Montrer ça.) □

Remarque. Probablement on "savait ça" déjà, sans avoir vu une vraie preuve ! Maintenant vous pouvez utilisez ce résultat à votre guise dans vos propres preuves, car c'est montré. Est-ce que vous "connaissez" d'autres faits à propos des entiers qui sont encore sans preuve (voir aussi §7.19 plus tard) ! ?

Exemple 7.3. Le pgcd de $m = 2^0 3^5 7^1 11^1$ et $n = 2^2 3^3 7^2 11^1$ est $2^0 3^3 7^1 11^1$ et le ppcm est $2^2 3^5 7^2 11^1$.

Corollaire 7.3. *Si* n *et* m *sont positifs, alors*

$$n \cdot m = \text{pgcd}(n, m) \cdot \text{ppcm}(n, m)$$

Démonstration. Voir aussi [R, p. 111]. Ça suit du théorème, car $a_i + b_i = \text{Min}\{a_i, b_i\} + \text{Max}\{a_i, b_i\}$. □

Donc pour calculer $\text{ppcm}(n, m)$ il suffit de calculer $\text{pgcd}(n, m)$.

7.12. **Vérifier si un nombre est premier.** Donné un nombre naturel $n > 1$, il est un travail laborieux de tester si n est un nombre premier ou pas. Mais le théorème suivant aide un peu.

Théorème 7.11. *Soit $n > 1$ un nombre naturel tel que $p \not| n$ pour chaque nombre premier p tel que $p \leq \sqrt{n}$ (ou $p^2 \leq n$). Alors n est un nombre premier.*

Démonstration. Soit $n = p_1 p_2 \dots p_s$ une factorisation, où chaque p_i est premier et par hypothèse $p_i^2 > n$. Nous allons présenter une preuve par contradiction. Supposons n n'est pas premier, alors $s \geq 2$ et

$$n^2 = p_1^2 p_2^2 \dots p_s^2 > n^s \geq n^2.$$

Que $n^2 > n^2$ est une contradiction. Donc on conclut que n est premier. □

Exemple 7.4. Par exemple 113 est premier. Preuve : les nombres premiers $\leq \sqrt{113}$ sont $2, 3, 5, 7$ et 11 et aucun divise 113.

7.13. **Il existe une infinité de nombres premiers.** Nous allons présenter la fameuse preuve par l'absurde d'Euclide du théorème qu'll existe une infinité de nombres premiers.

Théorème 7.12. *Il existe une infinité de nombres premiers.*

Démonstration. Supposons qu'il existe *seulement* un nombre fini, disons N, de nombres premiers. Soient $p_1, p_2, p_3, \dots, p_N$ ces nombres premiers (parmi eux se trouvent bien sûr 2, 3, 5, 7, 11.) Considérons le très grand nombre

$$n = 1 + (p_1 \cdot p_2 \cdot p_3 \cdots p_{N-1} \cdot p_N).$$

Comme pour chaque nombre naturel, il existe un nombre premier p qui divise n.

Ce nombre premier p se trouve nécessairement sur la liste de de tous les nombres premiers plus haut : il existe un $1 \leq i \leq N$ tel que $p = p_i$. Mais n s'écrit comme 1 plus un p_i-multiple ; donc p_1 ne divise pas n, car il y aura un reste 1 après division par p_i.

Alors p divise n ET $p = p_i$ ne divise pas n. C'est absurde.

On conclut que l'hypothèse qu'il existe seulement un nombre fini de nombres premiers est fausse ! Le théorème est donc vrai, car c'est l'opposé de cette fausse hypothèse. □

Remarque. La preuve par l'absurde que $\sqrt{2}$ n'est pas une fraction était aussi déjà donnée par Euclide (et autres avant lui), voir[R, ex. 15, p. 164].

7.14. **Représenter un entier sur une autre base que** 10**.** Nous avons l'habitude d'écrire les entiers en forme décimale. Par exemple, 12054 veut dire 4 unités + 5 dix + 0 cent + 2 mille + 1 dix-mille.

$$12054 = 1 \cdot 10^4 + 2 \cdot 10^3 + 0 \cdot 10^2 + 5 \cdot 10^1 + 4 \cdot 10^0.$$

On peut aussi utiliser une base autre que 10, par exemple les bases 2 et 16 sont utilisées en informatique. Voir [R, p. 121, 122].

Soit $b > 0$ la base choisie, alors on peut écrire n'importe quel nombre naturel n sur la forme

$$n = [c_s c_{s-1} \dots c_1 c_0]_b = c_s b^s + c_{s-1} b^{s-1} + \dots + c_1 b^1 + c_0 b^0,$$

et chaque "chiffre" c_i est plus petit que b.

Possiblement il faut inventer des notations pour les chiffres ! Par exemple, pour base 16 on utilise les 16 chiffres

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E$$

($A = 10, B = 11, C = 12, D = 13, E = 14, F = 15$).

Par exemple $N = [2AE0B]_{16}$ signifie dans notre notation décimale usuelle le nombre

$$N = 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0 = 175627.$$

Comment écrire un nombre N sur la base $b > 1$? Avec division-avec-reste par b répété !

Par division avec reste il y a q_0 et c_0 tel que $N = q_0 b + c_0$, et $0 \leq c_0 < b$.

Puis il y a q_1 et c_1 tel que $q_0 = q_1 b + c_1$, et $0 \leq c_1 < b$.

Puis il y a q_2 et c_2 tel que $q_1 = q_2 b + c_2$, et $0 \leq c_2 < b$.

Puis il y a q_3 et c_3 tel que $q_2 = q_3 b + c_3$, et $0 \leq c_3 < b$.

Et cetera. On arrête dès que q_i devient 0. Alors

$$N = [c_s c_{s-1} \dots c_1 c_0]_b.$$

Exemple, si $b = 16$ et $N = 357911$.

$$\begin{aligned} 357911 &= 22368 \cdot 16 + 11 \\ 22368 &= 1398 \cdot 16 + 0 \\ 1398 &= 87 \cdot 16 + 6 \\ 87 &= 5 \cdot 16 + 7 \\ 5 &= 0 \cdot 16 + 5 \end{aligned}$$

Donc

$$357911 = [5760B]_{16}.$$

Exemple 7.5. Soit $b > 0$ et $n = [c_s c_{s-1} \dots c_1 c_0]_b$. Alors $b|n$ si et seulement si le dernier chiffre c_0 est 0. Sur base $b = 7$ le nombre $n = [55563450]_7 = 4805661$ est divisible par 7. Facile à voir dans la représentation de base 7 (dernier chiffre est 0) mais pas si facile de voir en forme décimale.

7.15. **Conséquences pour $\mathbb{Z}/m\mathbb{Z}$.** Souvent dans les mathématiques on doit résoudre des équations linéaires "modulo m". Le suivant est une version "modulo m" du th.7.7.

Théorème 7.13. *Fixons trois nombres entiers a, b, m et supposons $m > 0$. Considérons l'équation*

$$ax \equiv_m b \text{ ou } ax \equiv b \bmod m.$$

Mettons $d = \text{pgcd}(a, m)$. On peut trouver un entier x qui satisfait cette équation si et seulement si $d|b$.

Démonstration. Supposons d'abord que pour $x \in \mathbb{Z}$ on a $ax \equiv b(\bmod m)$. Alors $m|(ax - b)$ et il existe un entier c tel que $ax - b = cm$. On a que $d|a$ et $d|m$ et on conclut que $d|(ax - cm)$ et $d|b$.

Par contre supposons $d|b$, donc il existe un entier c tel que $b = cd$. Par le théorème de Bézout, th. 7.6, ils existent des entiers s, t tels que $sa + tm = d$; et donc aussi $csa + ctm = cd = b$. Alors $csa - b$ est divisible par m et

$$csa \equiv_m b.$$

Alors $x = cs$ satisfait l'équation. □

Exemple 7.6. La preuve suggère même une méthode pour trouver une solution. Considérons l'équation

$$1351x \equiv 21 \bmod 1064$$

peut-on résoudre modulo 1064 ? Heureusement, nous avons déjà calculé que $\text{pgcd}(1351, 1074) = 7$, et 7 divise effectivement la partie droite 21 : une solution existe !

Pour trouver une solution, on commence par trouver s, t par la méthode de Bézout, tels que $s1351 + t1064 = 7$. Ce que nous avons aussi déjà fait !

$$(-63) \cdot 1351 + 80 \cdot 1064 = 7$$

donc en multipliant par 3 :

$$(-3 \cdot 63) \cdot 1351 + (3 \cdot 80) \cdot 1064 = 3 \cdot 7 = 21$$

et

$$(-3 \cdot 63) \cdot 1351 \equiv 21 \bmod 1064$$

Donc $x = -3 \cdot 63 = -189$ est une solution. Si on veut une solution positive on ajoute 1064, c.-à-d., $x = -189 + 1064 = 875$ est aussi une solution.

Par contre l'équation

$$1351x \equiv 29 \bmod 1064$$

on ne peut pas résoudre, car 7 ne divise pas 29 !

Corollaire 7.4. *Soit m un entier positif, et a, b, c des entiers. Si $ac \equiv bc \bmod m$ et $\text{pgcd}(c, m) = 1$, alors $a \equiv b \bmod m$.*

Démonstration. Voir [R, p.131, Th. 2]. Par Bézout, ils existent s et t tels que $sm + tc = 1$, donc $tc \equiv 1 \bmod m$. Donc si $ac \equiv bc \bmod m$ on a aussi $atc \equiv btc \bmod m$ et $a \equiv b \bmod m$. □

Remarque. Si a, b, c sont trois entiers et $ac = bc$. On ne peut pas conclure que $a = b$, sauf si on sait que $c \neq 0$.

Soit m un entier positif, et a, b, c des entiers. Si $ac \equiv bc \bmod m$ et $\text{pgcd}(c, m) = 1$, alors $a \equiv b \bmod m$. On a vraiment besoin de l'hypothèse que $\text{pgcd}(c, m) = 1$. Par exemple : $1 \cdot 2 \equiv 3 \cdot 2 \bmod 4$ mais $1 \not\equiv 3 \bmod 4$ (et $\text{pgcd}(2, 4) = 2 \neq 1$).

7.16. **Le petit théorème de Fermat.** [15] Mentionnons sans preuve le "petit théorème de Fermat".

Théorème 7.14 (Fermat)**.** *Soit p un nombre premier et a un entier. Alors*

$$a^p \equiv_p a.$$

15. Cette sous-section **n'est pas obligatoire** et ne fait pas partie de la matière examinée.

Voir [R, p. 137]. Une preuve sera donné dans le cours MAT2600, la théorie des groupes. Pour vous c'est seulement une curiosité sans doute. Mais c'est à l'origin de beaucoup d'applications, par exemple pour une communication secure entres les banques.

Exemple 7.7. Le nombre 11 est premier.

$$14^{11} \equiv_{11} 3^{11} \equiv_{11} 3^{2\cdot 5+1} \equiv_{11} (9)^5 \cdot 3 \equiv_{11} (-2)^5 \cdot 3 \equiv_{11} -32 \cdot 3 \equiv_{11} 1 \cdot 3 \equiv_{11} 3 \equiv_{11} 14.$$

En effet. Nous n'avions pas besoin de calculer 14^{11} et puis calculer le reste après division par 11. Le calcul modulaire est beaucoup plus agréable que le calcul ordinaire. Les nombres impliqué restent petits ! Et ce théorème aide beaucoup pour calculer les hautes puissances.

7.17. **La fonction "reste-modulo-m".** Soit $m > 0$ et a un entier. Soit r le reste de a après division par m. C'est l'unique nombre naturel r tel que $m|(a-r)$ et $0 \leq r < m$. Donc associer r à a est vraiment une *fonction* avec domaine $\mathbb{Z}$ et avec codomaine les nombres naturels entre 0 et $m-1$. On devrait écrire quelque chose comme

$$\text{Reste-après-division-par-}m(a) = r,$$

mais pour des raisons historiques on écrit $(a \bmod m) = r$, ou même

$$r = a \bmod m,$$

voir aussi [R, p. 111]. Aussi mod est un bouton sur certaines calculatrices, qui calcule le reste-modulo-m.

Malheureusement ça introduit possiblement une confusion avec la notation

$$r \equiv a \bmod m$$

pour la relation d'équivalence $r \equiv_m a$! Mais il y a des liens.

On a $r = a \bmod m$ *si et seulement si* $r \equiv a \bmod m$ et $0 \leq r < m$. Et $a \equiv b \mod m$ si et seulement si $(a \mod m) = (b \mod m)$.

7.18. **Le théorème chinois.** [16]

Exemple 7.8. Un problème très classique est de trouver un nombre N qui est congru à 2 mod 3, à 3 mod 5 et à 2 mod 7 simultanément !

L'idée d'une *base* de l'algèbre linéaire s'applique ici aussi. Trouvons d'abord un n_1 tel que

$$n_1 \equiv 1 \bmod 3, n_1 \equiv 0 \bmod 5, n_1 \equiv 0 \bmod 7;$$

puis un n_2 tel que

$$n_2 \equiv 0 \bmod 3, n_2 \equiv 1 \bmod 5, n_2 \equiv 0 \bmod 7;$$

et un n_3 tel que

$$n_3 \equiv 0 \bmod 3, n_3 \equiv 0 \bmod 5, n_3 \equiv 1 \bmod 7.$$

Soient a, b, c quelconques et posons $n = an_1 + bn_2 + cn_3$, alors

$$n \equiv a \bmod 3, n \equiv b \bmod 5, n \equiv c \bmod 7.$$

16. Cette sous-section **n'est pas obligatoire**, et ne fait pas partie de la matière examinée.

Donnons les raisons. Par exemple, $n_1 \equiv 1 \bmod 3$, donc $an_1 \equiv a \bmod 3$. Puis $n_2 \equiv 0 \bmod 3$ et $n_3 \equiv 0 \bmod 3$, donc $(bn_2 + cn_3) \equiv 0 \bmod 3$. Et donc $n = an_1 + bn_2 + cn_c \equiv a \bmod 3$. Pareil pour les deux autres congruences.

Donc il suffit de trouver n_1, n_2 et n_3.

On remarque que n_1 est multiple de 5 et de 7, donc un multiple de $5 \cdot 7$, disons $n_1 = 5 \cdot 7 \cdot q_1$. On doit encore trouver q_1 tel que $n_1 = 5 \cdot 7 \cdot q_1 \equiv 1 \bmod 3$. On a que $5 \cdot 7 = 35$ et 3 sont relativement premier, donc on peut trouver q_1 pas Bézout. On voit que $q_1 = -1$ fonctionne, car $-35 \equiv 1 \bmod 3$. Donc prenons $n_1 = -35$.

De façon analogue : prenons $n_2 = 21$ et $n_3 = 15$. Le nombre cherché au début est alors $2n_1 + 3n_2 + 2n_3 = 23$. Ce n'est pas la seule solution, parce que par exemple $23 + 3 \cdot 5 \cdot 7$ fonctionne aussi.

On obtient du même façon le suivant.

Théorème 7.15 (Théorème Chinois)**.** *Soient m_1, m_2, m_3 trois nombres naturels positifs, qui sont deux à deux relativement premier.*

(i) Is existent n_1, n_2, n_3 tels que

$$n_1 \equiv 1 \bmod m_1, n_1 \equiv 0 \bmod m_2, n_1 \equiv 0 \bmod m_3;$$

$$n_2 \equiv 0 \bmod m_1, n_2 \equiv 1 \bmod m_2, n_2 \equiv 0 \bmod m_3;$$

$$n_3 \equiv 0 \bmod m_1, n_3 \equiv 0 \bmod m_2, n_3 \equiv 1 \bmod m_3.$$

Soient a_1, a_2, a_3 fois nombres entiers. Alors pour $N = an_1 + bn_2 + cn_3$ on a

$$N \equiv a_1 \bmod m_1, N \equiv a_2 \bmod m_2, N \equiv a_3 \bmod m_3.$$

(ii) Il y a un seul nombre naturel n tel que $n \equiv a_1 \bmod m_1, n \equiv a_2 \bmod m_2, n \equiv a_3 \bmod m_3$, et tel que $0 \leq n < m_1m_2m_3$. C'est le reste de N après division par $m_1m_2m_3$:

$$n = N \bmod (m_1m_2m_3).$$

Démonstration. Voir [R, p. 134].

(i) Par hypothèse $\operatorname{pgcd}(m_1, m_2 \cdot m_3) = 1$, donc par Bézout il existe q_1, s_1 tels que

$$q_1m_2m_3 + s_1m_1 = 1.$$

Prenons $n_1 = q_1m_2m_3$. Alors $n_1 \equiv 0 \bmod m_2, n_1 \equiv 0 \bmod m_3$ et $n_1 = 1 - s_1m_1 \equiv 1 \bmod m_1$.

On trouve ainsi aussi n_2 et n_3. Et parce que $bn_2 + cn_3 \equiv 0 \bmod n_1$ et $n_1 \equiv 1 \bmod n_1$ on obtient

$$N = an_1 + bn_2 + cn_3 \equiv a \bmod n_1.$$

Et de même pour les deux autres congruences.

(ii) supposons $n \leq n'$ sont deux solutions comme en (ii). Alors pour $m = n' - n$ on a $m \equiv 0 \bmod m_1, m \equiv 0 \bmod m_2, m \equiv 0 \bmod m_3$, ou m est divisible par m_1, m_2 et m_3, donc par leur plus petit multiple, qui est $m_1m_2m_3$, car ils sont deux à deux relativement premiers. Mais aussi $0 \leq n' - n < m_1m_2m_3$, ce qui implique que $n = n'$. □

7.19. **Dérivation des propriétés bien-connues de $\mathbb{N}$ à partir des propriétés essentielles.** [17]
Rappelons :

Les propriétés considérées *essentielles* de l'ensemble des nombres naturels $\mathbb{N} = \{0, 1, 2, 3, \ldots, n, n+1, \ldots\}$ sont les suivantes :

(1) Chaque nombre naturel n a un unique *successeur* dans $\mathbb{N}$, noté $n + 1$.

(2) Il existe un nombre naturel spécial, noté 0, et

(3) chaque nombre naturel n différent de 0 a un unique *prédécesseur* dans $\mathbb{N}$, noté $n - 1$. On a $(n + 1) - 1 = n$, pour tout $n \in \mathbb{N}$ et $(n - 1) + 1 = n$ pour tout $n \in \mathbb{N}$ tel que $n \neq 0$.

(4) **Si $E \subseteq \mathbb{N}$ est un sous-ensemble de $\mathbb{N}$ tel que (i) $0 \in E$ et (ii) pour chaque $n \in E$ aussi $n + 1 \in E$, alors nécessairement $E = \mathbb{N}$.**

Le successeur de 0 s'appelle 1, le successeur de 1 s'appelle 2, et cétera. Le prédecesseur de 1 est 0, le prédécesseur de 2 est 1. Mais 0 n'a pas de prédécesseur dans $\mathbb{N}$ (l'entier -1 n'est pas un nombre naturel).

Axiome 7.1. *L'ensemble des nombres naturels $\mathbb{N} = \{0, 1, 2, 3, \ldots, n, n+1, \ldots\}$ avec ces propriétés essentielles existe.*

Il est impossible de montrer la vérité de cet axiome (sans supposer quelque chose d'autre). On l'accepte. À partir de seulement ces propriétés essentielles nous allons déduire les autres propriétés bien connues par vous.

Comme déjà expliqué déjà, la dernière propriété essentielle mentionnée nous permet d'utiliser induction dans les preuves et définitions.

Théorème 7.16 (Principe d'induction)**.** *Soit $P(n)$ une fonction propositionnelle avec univers de discours $\mathbb{N}$. Supposons $P(0)$ vraie et supposons aussi que pour chaque $n \in \mathbb{N}$ l'implication $P(n) \to P(n + 1)$ est vrai. Alors $P(n)$ est vrai pour chaque $n \in \mathbb{N}$.*

La définition de l'addition.

Définition 7.4. *Fixons $a \in \mathbb{N}$. Nous allons définir pour chaque $n \in \mathbb{N}$ l'élément $a + n \in \mathbb{N}$. Au début $a + 0 = a$ et $a + 1$ est le successeur de a (qui existe et est unique par une des propriétés essentielles de $\mathbb{N}$). Puis supposons pour $n \in \mathbb{N}$ on a déjà défini $a + n$, alors on définit $a + (n + 1)$ comme le successeur de $a + n$, c.-à-d., par définition*

$$a + (n + 1) := (a + n) + 1.$$

Ainsi on a défini $a + n$ pour chaque $n \in \mathbb{N}$.

Démonstration. En effet l'addition $a + n$ est définie pour $n = 0$, et si c'est définie pour n alors c'est aussi définie pour $n + 1$. Par le principe d'induction, l'addition $a + n$ a été définie pour chaque $n \in \mathbb{N}$. □

La définition de la multiplication.

17. Cette sous-section **n'est pas obligatoire**, et ne fait pas partie de la matière examinée. C'est écrit pour ceux qui sont intéressés.

Définition 7.5. *Fixons $a \in \mathbb{N}$. Nous allons définir pour chaque $n \in \mathbb{N}$ l'élément $a \cdot n \in \mathbb{N}$. Au début on définit $a \cdot 0 := 0$, $a \cdot 1 := a$. Supposons pour $n \in \mathbb{N}$ on a déjà défini $a \cdot n$, alors on définit $a \cdot (n+1) := (a \cdot n) + a$. Ainsi on a défini $a \cdot n$ pour chaque $n \in \mathbb{N}$.*

Avec ces définitions ce n'est pas évident que $a + b = b + a$ et $a \cdot b = b \cdot a$, et qu'aussi les règles de l'associativité et de la distributivité sont satisfaites. Il faut les montrer !

L'associativité de l'addition :

Théorème 7.17. *Pour tous les nombres naturels a, b, c on a*

$$(a + b) + c = a + (b + c).$$

Démonstration. Fixons a et b. Nous allons montrer par induction sur n que $(a+b)+n = a+(b+n)$.

Début : Si $n = 0$ c'est vrai : $(a + b) + 0 = a + b = a + (b + 0)$, car par définition $N + 0 = N$ pour chaque nombre naturel N.

Étape d'induction. Supposons $(a + b) + n = a + (b + n)$, pour $n \geq 0$. Alors

$$(a + b) + (n + 1) = ((a + b) + n) + 1 = ((a + (b + n)) + 1 = a + ((b + n) + 1) = a + (b + (n + 1)).$$

Alors le théorème est vrai par induction. □

Pour montrer la commutativité de l'addition nous aurons besoin d'un lemme.

Lemme 7.4. *Pour chaque nombre naturel n on a*

$$0 + n = n + 0 = n \quad \textit{et} \quad 1 + n = n + 1.$$

Démonstration. (i) Rappel : par définition de l'addition on a $n + 0 = n$ et $0 + (n + 1) = (0 + n) + 1$ pour chaque nombre naturel n.

On montre que $0 + n = n + 0 = n$ par induction.

Début : si $n = 0$ c'est une tautologie : $0 + 0 = 0 + 0$.

Étape d'induction : Supposons par induction que $0 + n = n + 0 = n$. Donc

$$0 + (n + 1) = (0 + n) + 1 = n + 1 = (n + 1) + 0.$$

On conclut par induction.

Puis, on montre que $1 + n = n + 1$ par induction.

Début. Si $n = 0$ on a : $1 + 0 = 1 = 0 + 1$, car par définition 1 est le successeur de 0.

Étape d'induction : Supposons par induction que $1+n = n+1$. Alors par L'hypothèse d'inducton et l'associativité :

$$(n + 1) + 1 = (1 + n) + 1 = 1 + (n + 1).$$

Et donc par induction on conclut : $1 + n = n + 1$ pour chaque nombre naturel n. □

La commutativité de l'addition :

Théorème 7.18. *Pour tous nombres naturels n et m on a*

$$m + n = n + m.$$

Démonstration. Fixons m. Nous allons montrer le théorème par induction sur n.

Début : c'est le lemme précécent.

Étape d'induction : Supposons par induction que $m+n = n+m$, pour $n \geq 0$. Donc par définition de la multiplication, l'hypothése d'induction, l'associativité de l'addition, et le lemme

$$m + (n + 1) = (m + n) + 1 = (n + m) + 1 = 1 + (n + m) = (1 + n) + m = (n + 1) + m.$$

Donc par induction théorème est vrai. □

Un début de soustraction....

Théorème 7.19. *Si $a + n = b + n$ pour $a, b, n \in \mathbb{N}$, alors nécessairement $b = c$.*

Démonstration. Par induction sur n.

Début. Pour $n = 0$: $a + 0 = b + 0$ implique $a = b$, car $a + 0 = a$. Pour $n = 1$: si $a + 1 = b + 1$ alors a et b sont deux prédécesseurs de $m = a + 1 = b + 1$. Par une propriété essentielle il suit que $a = b$.

Étape d'induction. Supposons $a+n = b+n$ implique que $a = b$. Supposons $a+(n+1) = b+(n+1)$, alors $(a + n) + 1 = (b + n) + 1$, donc par le cas spécial en haut, il suit $a + n = b + n$, donc par l'hypothèse d'induction on conclut $a = b$.

Donc le théorème est vrai. □

La distributivité :

Théorème 7.20. *Pour tous nombres naturels a, b, n on a*

$$(a + b) \cdot n = (a \cdot n) + (b \cdot n).$$

Démonstration. Par induction sur n.

Début. Pour $n = 0$ on a : $(a + b) \cdot 0 = 0 = 0 + 0 = (a \cdot 0) + (b \cdot 0)$.

Étape d'induction. Supposons $(a+b)\cdot n = (a\cdot n)+(b\cdot n)$.. On a par définition de la multiplication, l'associativité et la commutativité de l'addition, et l'hypothèse d'induction :

$$(a + b) \cdot (n + 1) = ((a + b) \cdot n) + (a + b) = ((a \cdot n) + (b \cdot n)) + (a + b) =$$

$$= ((a \cdot n) + a) + ((b \cdot n) + b) = ((a \cdot (n + 1)) + ((b \cdot (n + 1)).$$

Donc par le principe d'induction, le théorème est vrai. □

L'associativité de la multiplication :

Théorème 7.21. *Pour tous nombres naturels a, b, n on a*

$$(a \cdot b) \cdot n = a \cdot (b \cdot n).$$

Démonstration. Par induction sur n.

Début. Pour $n = 0$ on a : $(a \cdot b) \cdot 0 = 0 = a \cdot 0 = a \cdot (b \cdot n)$.

Étape d'induction. Supposons $(a \cdot b) \cdot n = a \cdot (b \cdot n)$. Alors par définition de la multiplication, l'hypothèse d'induction et la distributivité :

$$(a \cdot b) \cdot (n + 1) = ((a \cdot b) \cdot n) + (a \cdot b) = (a \cdot (b \cdot n)) + (a \cdot b) =$$

$$= a \cdot ((b \cdot n)) + b) = a \cdot (b \cdot (n + 1)).$$

Donc par le principe d'induction, le théorème est vrai. □

Lemme 7.5. *Pour chaque nombre naturel n on a*

$$0 \cdot n = n \cdot 0 = 0 \quad \textit{et} \quad 1 \cdot n = n \cdot 1 = n$$

Démonstration. Rappel : par définition de la multiplication on a $n \cdot 0 = 0$ et $n \cdot 1 = n$.

On montre que $0 \cdot n = 0$ par induction. Début : si $n = 0$ on a en effet $0 \cdot 0 = 0$. Étape d'induction : Supposons par induction que $0 \cdot n = 0$. Alors par définition de la multiplication, l'hypothèse d'induction, et par définition de l'addition

$$0 \cdot (n+1) = (0 \cdot n) + 0 = 0 + 0 = 0.$$

Donc par le principe d'induction, c'est vrai que $0 \cdot n$ pour chaque nombre naturel n.

On montre que $1 \cdot n = n$ par induction. Début : si $n = 0$ on a en effet $1 \cdot 0 = 0$, par définition. Supposons par induction que $1 \cdot n = n$. Alors par définition de la multiplication, l'hypothèse d'induction,

$$1 \cdot (n+1) = (1 \cdot n) + 1 = n + 1$$

Donc par le principe d'induction, c'est vrai que $1 \cdot n = n$ pour chaque nombre naturel n. □

La commutativité de la multiplication :

Théorème 7.22. *Pour tous nombres naturels a, n on a*

$$a \cdot n = n \cdot a$$

Démonstration. Par induction sur n. Début : si $n = 0$ on a en effet $a \cdot 0 = 0 = 0 \cdot a$ par le lemme. Aussi si $n = 1$ on a en effet $a \cdot 1 = a = 1 \cdot a$ par le lemme. Étape d'induction : Supposons par induction que $a \cdot n = n \cdot a$. Alors par définition de la multiplication, l'hypothèse d'induction, le lemme, la distributivité

$$a \cdot (n+1) = (a \cdot n) + a = (n \cdot a) + 1 \cdot a = (n+1) \cdot a.$$

Donc par le principe d'induction, le théorème est vrai. □

Lemme 7.6. *Soit $a \in \mathbb{N}$.*

(i) Si $a \neq 0$ alors pour chaque $n \in \mathbb{N}$ aussi $a + n \neq 0$.

(ii) Si $a \neq 0$ alors pour chaque non-zero $n \in \mathbb{N}$ aussi $a \cdot n \neq 0$.

Démonstration. (i) Par induction sur n.

Début $n = 0$: par hypothèse $a + 0 = a \neq 0$. Étape d'induction : Supposons $a + n \neq 0$. Le nombre naturel $a + (n+1) = (a+n) + 1$ est le successeur de $(a+n)$, donc ne peut pas être 0, car 0 n'a pas un prédécesseur.

Donc par induction pour chaque $n \in \mathbb{N}$ aussi $a + n \neq 0$.

(ii) Par induction sur $n \geq 1$.

Début $n = 1$: par hypothèse $a \cdot 1 = a \neq 0$. Étape d'induction : Supposons $n \geq 1$ et $a \cdot n \neq 0$. Nous avons $a \cdot (n+1) = (a \cdot n) + a$ et $(a \cdot n) \neq 0$ donc par (i) $a \cdot (n+1) \neq 0$. Donc par induction pour chaque non-zero $n \in \mathbb{N}$ aussi $a \cdot n \neq 0$. □

Comme conséquence, nous trouvons le résultat déjà utilisé plusieurs fois :

Corollaire 7.5. *Pour trois nombres natrurels : si $ab = ac$ et $a \neq 0$ alors $b = c$.*

Nous arrêtons ici notre début de retrouver tous le propriétés usuelles de $\mathbb{N}$ (et puis de $\mathbb{Z}$ et $\mathbb{Q}$), à partir les propriétés essentielles de $\mathbb{N}$.

Département de mathématiques et de statistique, Université de Montréal, C.P. 6128, succursale Centre-ville, Montréal (Québec), Canada H3C 3J7

E-mail address: broera@DMS.UMontreal.CA