La Première Méthode Générale de Factorisation des Polynômes

Maurice Mignotte, Doru Stefanescu

La Première Méthode Générale de Factorisation des Polynômes

Autour d'un mémoire de F. T. Schubert

Maurice Mignotte et **Doru Ştefănescu**

Résumé: Nous présentons deux ouvrages peu connus de N. Bernoulli (1708) et de F. T. Schubert (1794) sur la factorisation des polynômes à coefficients entiers ainsi que les recherches de L. Kronecker et B. A. Hausmann sur le même sujet. La méthode de factorisation de Bernoulli–Schubert utilise le calcul des différences finies et l'interpolation par différences finies. Elle a été redécouverte par Kronecker (1882), qui a utilisé l'interpolation de Lagrange. Les deux procédés permettent de factoriser des polynômes dont les degrés et les coefficients sont petits. Un algorithme qui combine les résultats de Bernoulli–Schubert et Kronecker a été obtenu par B. Hausmann. Sa méthode est plus efficace pour des polynômes stables. Ces trois méthodes sont brièvement comparées avec les algorithmes modernes de factorisation.

Abstract: We present two little known papers of N. Bernoulli (1708) and F. T. Schubert (1794) on the factorization of integer polynomials as well as the work of L. Kronecker and B. Hausmann on the same topic. The factorization method of Bernoulli–Schubert uses finite differences calculus and interpolation by finite differences. It was rediscovered by Kronecker (1882), who used Lagrange interpolation. Both procedures allow the effective factorization of polynomials having small degrees and coefficients. An algorithm combining both results of Bernoulli–Schubert and Kronecker was obtained by B. A. Hausmann. His method is particularly useful for the factorization of stable polynomials. The three methods are briefly compared with modern factorization algorithms.

Introduction

Die Definition der Irreductibilität entbehrt so lange einer sicherer Grundlage, als nicht eine Methode angegeben ist, mittels deren bei einer bestimmten, vorgelegten Function entschieden werden kann, ob dieselbe der aufgestellten Definition gemäss irreductibel ist oder nicht.

La définition de l'irréductibilité manque d'une base solide, aussi longtemps qu'on n'a pas inventé une méthode par laquelle il serait possible de décider si une fonction donnée est irréductible ou non selon cette définition.

(L. Kronecker, 1882)

L'étude de la décomposition d'un polynôme à coefficients entiers dans un produit de polynômes irréductibles remonte au XVII^{e} siècle. Après les procédés inventés par I. Newton et G. W. Leibniz pour trouver les diviseurs linéaires et quadratiques, un véritable algorithme général de factorisation n'a été construit que par Nicolas (I) Bernoulli et F. T. Schubert.

La première publication est due à N. Bernoulli (1687–1759). Elle date de 1708 mais sa diffusion a été très limitée et on peut penser qu'elle a été quasiment inconnue du milieu mathématique. La publication de F. T. Schubert (1758–1829), date de 1798, parue dans le journal de l'Académie des Sciences de Saint–Pétersbourg[1]. Le mémoire de Schubert, aussi écrit en Latin, a été lui aussi peu connu par la communauté mathématique[2]. Tandis que les recherches de L. Kronecker de 1882 sur le même sujet ont joui d'une notoriété rapide.

Il semble que ce travail de Nicolas Bernoulli avait échappé à l'attention des mathématiciens du XX^{e} siècle. À notre connaissance il n'a pas été cité depuis 1900. Même un ouvrage aussi important que l'Encyclopédie des Sciences Mathématiques [Enc. Sci. Math., 1992] ignore les mémoires de N. Bernoulli et F. T. Schubert. Au contraire, Schubert a été cité au moins deux fois: en 1908 par M. Cantor [Moritz Cantor, 1908] p. 137 et en 1981 par D. Knuth [Donald E. Knuth, 1981], p. 431.

Nous allons présenter ces mémoires peu connus de N. Bernoulli et F. T. Schubert ainsi que le développement ultérieur de ces idées dans des travaux des XIX^{e} et XX^{e} siècles. Le travail de Nicolas Bernoulli sur la factorisation des polynômes à coefficients entiers est, à notre connaissance, le premier ouvrage où on donne une méthode générale pour la décomposition d'un polynôme entier en produit de polynômes irréductibles. Sa méthode a été retrouvée[3] par F. T. Schubert.

[1] C'est un rapport présenté à l'Académie de St–Pétersbourg, dont il était membre, le 19 juin 1794.

[2] À l'exception des références qu'on trouve dans l'histoire des mathématiques de M. Cantor [Moritz Cantor, 1908], p. 137 et dans le traité [Donald E. Knuth, 1981], p. 431.

[3] et présentée avec plus de détails

Le problème de la factorisation effective des polynômes constitue une des questions de base dans le domaine du calcul formel qui a connu un essor formidable depuis le début des annéees 70.

Il faut dire que des algorithmes beaucoup plus efficaces, et de principes radicalement différents, ont été inventés dans les dernières décennies. Ils permettent d'obtenir la factorisation d'un polynôme à coefficients entiers extrêmement vite par l'intermédiaire des ordinateurs.

Résumons la chronologie de ce que nous allons présenter:

- 1683, 1707 Newton
- 1708 Leibniz, Hermann, N. Bernoulli
- 1745 N. Bernoulli
- 1761 D. Bernoulli
- 1793/1796 Schubert
- 1880/1882 Kronecker
- 1937 Hausmann

1 L'algorithme de Bernoulli–Schubert

Les ouvrages sur la factorisation des polynômes à coefficients entiers avant Bernoulli–Schubert se concentrent généralement sur la recherche des facteurs linéaires et quadratiques. Evidemment pour les diviseurs linéaires ce problème est résolu dès qu'on a trouvé toutes les racines rationnelles du polynôme à factoriser. Des procédés pour trouver ces racines étaient déja connus au milieu du XVII^{e} siècle, v. [Enc. Sci. Math., 1992], p. 209–210.

Newton, *Arithmetica Universalis*

Newton a exposé une méthode systématique pour trouver les diviseurs linéaires et quadratiques dans son traité *Arithmetica Universalis* [Isaac Newton, 1707]. On trouve dans ce livre une section intitulée *De inventione Divisorum* où il énonce des règles pour trouver les facteurs d'un polynôme et discute plusieurs exemples.

On pourra noter que cet ouvrage correspond à la rédaction d'un cours professé par Newton depuis 1683 et qui proposait une présentation unifiée de l'arithmétique et de l'algèbre.

La méthode de factorisation des polynômes à des coefficients entiers de Newton repose sur l'étude des tableaux de différences finies et l'interpolation des polynômes par différences finies.

C'est un des outils qui a été fréquemment utilisé jusqu'au début du XX^{e} siècle, voir plus loin l'opinion de Van der Waerden [Bartel L. Van der Waerden, 1937] sur l'utilité de l'interpolation par différences finies pour la factorisation des polynômes.

Les différences finies

La méthode de Newton utilise les tableau de différences finies. En effet, si $y_0, \ldots, y_n$ sont des nombres réels, soient

$$\begin{array}{lcl}
\Delta^1(y_0,\ldots,y_n) & = & \{y_1-y_0, y_2-y_1, \ldots, y_n-y_{n-1}\} \\
 & = & \{y_0^{(1)}, y_1^{(1)}, \ldots, y_{n-1}^{(1)}\}, \\
\Delta^2(y_0,\ldots,y_n) & = & \Delta^1(y_0^{(1)},\ldots,y_{n-1}^{(1)}) \\
 & = & \{y_1^{(1)}-y_0^{(1)}, y_2^{(1)}-y_1^{(1)}, \ldots, y_{n-1}^{(1)}-y_{n-2}^{(1)}\} \\
 & = & \{y_0^{(2)}, y_1^{(2)}, \ldots, y_{n-2}^{(2)}\}, \\
\ldots\ldots\ldots\ldots & \ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\Delta^i(y_0,\ldots,y_n) & = & \Delta^1(y_0^{(i-1)},\ldots,y_{n-i}^{(i-1)}), \\
\ldots\ldots\ldots\ldots & \ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{array}$$

La suite $\Delta^i(y_0,\ldots,y_n)$ est *la différence* d'ordre i de la suite $y_0,\ldots,y_n$ et

$$\Delta^1(y_0,\ldots,y_n), \Delta^2(y_0,\ldots,y_n), \ldots, \Delta^i(y_0,\ldots,y_n), \ldots$$

est le *tableau des différences* de la suite $y_0,\ldots,y_n$.

La méthode de Newton

Newton commence la présentation de sa méthode par énoncer deux règles, v. [Isaac Newton, 1802] p. 46–47. La première décrit la manière de trouver les diviseurs d'un nombre entier positif. Dans la seconde il écrit: ≪*Si la quantité, après avoir été divisée par tous les diviseurs simples, demeure encore composée, et qu'on soupçonne qu'elle contienne quelque diviseur composé; disposez–la selon les dimensions de quelqu'une de ses lettres, et substituez successivement à la place de cette lettre, trois ou un plus grand nombre de termes de la progression arithmétique* 3, 2, 1, 0, −1, −2. *Et il en résultera autant de valeurs différentes, que vous écrirez avec les diviseurs à côté des termes de la progression qui les auront produites; ayant soin d'écrire aussi chaque diviseur avec un signe positif et un signe négatif. Comparez les diviseurs qui se trouvent dans une ligne avec ceux des autres lignes, pour voir s'ils ne formeraient pas une progression arithmétique. Et pour cela, commencez par les plus forts, pour descendre aux plus faibles, en suivant la même marche que la progression arithmétique* 3, 2, 1, 0, −1, −2. *Si cette recherche vous fournit quelque progression dont les termes ne diffèrent que d'une unité, ou quelque nombre qui divise la plus haute puissance de la quantité proposée, écrivez cette progression dans le même ordre que la première, plaçant chacun de ses termes à côté de la ligne des diviseurs qui l'a produit; et le terme qui, dans cette progression, répondra au terme* 0 *de la*

progression primitive, étant divisé par la différence des termes, et joint à la lettre à laquelle il avait été substitué, formera une quantité avec laquelle il faudra tenter la division. ≫

Dans le reste de la section sur "*la manière de trouver les diviseurs*" il considère plusieurs polynômes particuliers et analyse leurs factorisations possibles.

Pour le polynôme $x^3-x^2-10x+6$, par exemple, il choisit les valeurs $x = -1$, 0, 1 et obtient les entiers -4, 6, $+14$. Ensuite il construit le tableau suivant avec les diviseurs positifs des valeurs absolues de ces nombres. Il présente ainsi le tableau suivant:

1	4	1, 2, 4	+4
0	6	1, 2, 3, 6	+3
−1	14	1, 2, 7, 14	+2

Ensuite il s'aperçoit que les termes de la dernière colonne forment une progression arithmétique et en déduit que le polynôme $x+3$ est un diviseur[4] et que l'autre facteur est $xx-4x+2$: ≪*Ensuite comme le terme le plus élevé* x^3 *n'a de diviseur que l'unité, je cherche parmi les diviseurs quelque progression dont les termes ne diffèrent que d'une unité, et qui, en descendant des plus forts aux plus faibles, décroissent comme ceux de la progression* 1, 0, -1. *Je ne trouve qu'une progression de cette espèce, c'est* 4, 3, 2. *Je prends donc le terme* $+3$ *qui se trouve dans la même ligne que* 0 *de la première progression* 1, 0, -1, *je le joins à* x, *et je tente la division par* $x+3$; *elle réussit, et j'obtiens pour quotient* $xx-4x+2$. ≫

Newton a envisagé le problème de la factorisation des polynômes à coefficients entiers dans son grand cours d'algèbre fait à Cambridge entre 1673 et 1683 qu'il a envisagé ce problème. Le manuscrit de ce cours a été déposé par Newton pendant l'hiver 1683–1684 et porte le nom *Arithmeticæ Universalis Liber Primus*. Il se trouve dans les *Mathematical Papers*

édités par D. T. Whiteside [Isaac Newton, 1972].

Il faut noter que Newton s'aperçoit que l'interpolation pourrait conduire à des diviseurs linéaires à coefficients rationnels qui ne soient pas des entiers. Il trouve que le polynôme $6y^4-y^3-21yy+3y+20$ a le facteur $y+\frac{4}{3}$, et remarque qu'en le multipliant par le diviseur 3 du coefficient dominant on obtient $3y+4$, qui est un diviseur à coefficients entiers.

Dans son cours (v. [Isaac Newton, 1972], p. 46) ainsi que dans *Arithmetica Universalis* (v. [Isaac Newton, 1802], p. 49–50), Newton donne également une méthode pour trouver les diviseurs quadratiques: ≪*Substituez dans la proposée, à la place de la lettre, quatre ou un plus grand nombre de termes de la progression* 3, 2, 1, 0, -1, -2, -3 . *Placez tous*

les diviseurs des nombres qui en résulteront dans les mêmes lignes que les termes de la progression; élevez les termes de la progression au quarré; multipliez ces quarrés par quelque diviseur numérique du terme le plus élevé de la quantité

[4] V. [Isaac Newton, 1761] p. 62., ou l'édition française [Isaac Newton, 1802] p. 47.

$\mp C$ *du terme immédiatement supérieur qui se trouve dans la même ligne que le terme* 1 *de la première progression ; soit enfin* A *un diviseur numérique du terme le plus élevé, et* l *la lettre de la quantité proposée ; alors* $Al \pm B \pm C$ *sera un diviseur qu'il faudra essayer* (5).

Soit, par exemple, la proposée $x^4 - x^3 - 5x^2 + 12x - 6$; à la place de x j'écris successivement 3, 2, 1, 0, — 1, — 2. Les nombres qui en résulteront, seront 39, 6, 1, — 6, — 21, — 26. J'écris chacun d'eux, avec tous ses diviseurs, dans la ligne du terme de la première progression qui l'a produit.

J'élève chacun des termes de la première progression au quarré, et j'écris tous ces quarrés dans une colonne ; je les multiplie par un diviseur numérique du terme le plus élevé de la proposée ; j'ajoute successivement à ces produits tous les diviseurs pris en plus et en moins, ce qui me donne des sommes et des différences que j'écris dans leurs lignes respectives. Ensuite parcourant ces nouvelles quantités en comparant chaque terme d'une ligne à ceux des autres lignes, j'écris dans de nouvelles colonnes toutes les progressions que cet examen me procure. Toutes ces opérations peuvent se voir dans l'exemple suivant.

3	39	1, 3, 13, 39.	9	— 30, — 4, 6, 8, 10, 12, 22, 48.	— 4	6
2	6	1, 2, 3, 6.	4	— 2, 1, 2, 3, 5, 6, 7, 10.	— 2	3
1	1	1.	1	0, 1.	0	0
0	6	1, 2, 3, 6.	0	— 6, — 3, — 2, — 1, 1, 2, 3, 6.	2	— 3
— 1	21	1, 3, 7, 21.	1	— 20, — 6, — 2, 0, 2, 4, 8, 22.	4	— 6
— 2	26	1, 2, 13, 26.	4	— 22, — 9, 2, 3, 5, 6, 17, 30.	6	— 9

Je prends successivement 2 et — 3 qui se trouvent dans la même ligne que le 0 de la première progression, je les prends, dis-je, successivement pour $\mp C$, et je prends respectivement pour $\mp B$ les

[Isaac Newton. 1802], p. 50.

proposée; ajoutez successivement à ces produits les diviseurs des nombres qui ont résulté de vos suppositions; retranchez–les ensuite, et écrivez ces sommes et ces différences dans le même ordre que les termes de la première progression; cherchez toutes les progressions qui peuvent se rencontrer dans ces sommes et ces différences, en allant des termes d'une ligne à ceux de la ligne suivante. Soit, par exemple, $\mp C$ *le terme d'une progression de cette espèce qui se trouve dans la même ligne que le terme* 0 *de la première progression; soit* $\mp B$ *la différence qu'on obtient en retranchant* $\mp C$ *du terme immédiatement supérieur qui se trouve dans la même ligne que le terme* 1 *de la première progression; soit enfin* A *un diviseur numérique du terme le plus élevé, et* l *la lettre de la quantité proposée; alors* $All \pm Bl \pm C$ *sera un diviseur qu'il faudra essayer.* $\gg$

Il considère comme premier exemple

$$x^4 - x^3 - 5x^2 + 12x - 6 = 0\,,$$

et trouve, par cette méthode, x^2+2x-2 et x^2-3x+3 comme diviseurs possibles et conclut que $\ll$*la réduction réussit pour chacun des deux* $\gg$.

Les successeurs de Newton

Les contemporains de Newton ont été vivement intéressés par ces résultats et ils ont essayé de comprendre le procédé de factorisation de Newton et de donner des justifications de la règle indiquée par lui. Parmi eux on peut citer G. W. Leibniz, J. Hermann, N. Bernoulli (I), et plus tard D. Bernoulli et puis F. T. Schubert.

Leibniz

Leibniz a publié une récension d'*Arithmetica Universalis* dans *Acta Eruditorum*, Novembre, 1708, p. 519–526. Il reprend l'exemple du polynôme $x^2 - 10x + 6$ et le tableau de Newton ainsi que la factorisation de ce polynôme.

Leibniz, qui n'était pas satisfait par la méthode de Newton, en donne une autre dans sa lettre adressée à Jakob Hermann de 6 Septembre 1708[5]. Cette lettre contient une note intitulée $\ll$*Methodus generalis investiganddi divisores formularum rationalium integralium ex datis divisoribus numerorum rationalum integrorum*$\gg$.

Il discute le cas des polynômes de degré 5 et considère comme exemple la factorisation du polynôme $2x^5+3x^4+8x^3+6xx+5x+6$ qu'il note $\odot$. Il cherche une factorisation en un produit d'un polynôme cubique $b+cx+dxx+ex^3$ avec un polynôme quadratique $\beta+\gamma x+\delta xx$. Il choisit un entier h plus grand que les coeffcients du polynôme à factoriser et remarque que la valeur du diviseur du polynôme $\odot$ en h est un diviseur de la valeur du polynôme à factoriser en ce point.

Pour le polynôme $2x^5+3x^4+8x^3+6xx+5x+6$ il prend $h = 10$ et obtient la valeur 238656. Ensuite il forme un tableau des diviseurs de ce nombre, et étudie

[5] V. [Gottfried Wilhelm Leibniz, 1859] p. 335–339.

ses proprietés. Il trouve qu'il n'existe pas de facteur linéaire[6] et finalement obtient les facteurs $2x^3 + x^2 + x + 2$ et $x^2 + x + 3$.

On trouve une excellente présentation de la méthode de Leibniz dans *Enc. Sci. Math.* [Enc. Sci. Math., 1992], t. I, 2ème partie, article de E. Netto et R. Le Vavasseur intitulé *Réductibilité dans le domaine des nombres rationnels*, p. 209–210. Leibniz considère uniquement des polynômes dont les coefficients sont positifs et il calcule la valeur du polynôme à factoriser pour un entier plus grand que tous les coefficients. Ce qui distingue sa méthode de celle de Newton est que Leibniz utilise une seule valeur du polynôme.

J. Hermann

Jakob Hermann (1678–1733) donne une démonstration dans sa lettre du 12 Juillet 1708 adressée à Leibniz[7]. Il considère un polynôme de degré m,

$$Ax^m + px^{m-1} + qx^{m-2} + rx^{m-3} \text{ etc } \ldots$$

et étudie les diviseurs possibles à coefficients entiers de la forme $ax \pm b$ et $axx \pm bc \pm c$, en utilisant des tableaux de différences finies des valeurs du polynôme à factoriser. Pour le cas d'un diviseur linéaire il utilise les valeurs 1, 0 et -1 et obtient que la progression arithmétique de la dernière colonne doit être $a \pm b$, $\pm b$, $-a \pm b$,

Dans le cas du polynôme $x^3 - x^2 + 10x + 6$ que considérait Leibniz, on trouve le facteur $x + 3$ obtenu par Newton.

Pour les diviseurs quadratiques Hermann considère les valeurs en 2, 1, 0, -1 etc et étudie un tableau dans lequel il pose les valeurs calculées en f, g, h, k:

$aff \pm bf \pm c$	$\pm bf \pm c$	$\pm 2b \pm c$
$agg \pm bg \pm c$	$\pm bg \pm c$	$\pm b \pm c$
$ahh \pm bh \pm c$	$\pm bh \pm c$	$\pm c$
$akk \pm bk \pm c$	$\pm bk \pm c$	$\mp b \pm c$

Nicolas (I) Bernoulli (1687–1759)

Neveu de Jacques et Jean Bernoulli, Nicolas Bernoulli[8] a étudié les mathématiques avec ses oncles. Il a beaucoup voyagé, a été professeur à Padoue et Bâle. La plus grande partie de ses recherches se trouve dans sa correspondance qui comprend presque 560 lettres, dont une grande partie avec Pierre Rémond de Montmort (1678–1719).

Nicolas Bernoulli a donné une autre démonstration de la méthode de Newton en 1708, mais qui n'a été publiée qu'en 1745[9]. Cette preuve a été communiquée

[6] Qu'il note $b + cx$.

[7] V. [Gottfried Wilhelm Leibniz, 1859] p. 328–332.

[8] Appelé aussi Nicolas (I) Bernoulli, pour le distinguer de son cousin Nicolas (II) Bernoulli (1695–1725).

[9] V. dans [Enc. Sci. Math., 1992] p. 210, la note de bas de page 700 de Gustaf Eneström.

à Leibniz par son oncle Jean Bernoulli dans une lettre du 16 Mai 1708, v. [Gottfried Wilhelm Leibniz, 1856], p. 827–835. Dans cette lettre Jean Bernoulli propose à Leibniz de publier la note de son neveu, alors agé de 20 ans, dans *Acta Eruditorum*. Finalement ce texte a paru seulement en 1745 dans *Commercium philosophicum et mathematicum* de G. W. Leibniz et Jean Bernoulli **2**, p. 180, Lausanne et Genève (1745).

L'ouvrage de N. Bernoulli

Dans sa note, intitulée ≪*Regula Generalis Inveniendi Aequationes, per quas alia quepiam data, modo reducibilis sit, dividi potest* ≫, N. Bernoulli développe beaucoup plus cette procédure et il donne des tableaux détaillés sur la méthode des différences finies. Il se rapporte, par exemple, à l'équation $3x^3-4xx-6x+15=0$ et considère la suite 1, 1, 3, 7, 13, formée avec des diviseurs des valeurs absolues de ce polynôme en 2, 1, 0, −1, −2. Ensuite il considère le tableau

	differ. 1	differ. 2 per 2 divisae
1		
	0	
1		1
	−2	
3		1
	−4	
7		1
	−6	
13		

et trouve le facteur $xx-3x+3=0$.

Dans un autre exemple N. Bernoulli obtient la factorisation du polynôme $2x^7+2x^6-16x^5-13x^4+41x^3+22xx-32x-9$. Par sa méthode il trouve les diviseurs $2x^3-4x-1$ et $x^4+x^3-6xx-4x+9$, donc des facteurs cubiques et biquadratiques, au delà de ce que faisait Newton dans *Arithmetica Universalis*.

Il envisage de trouver tous les diviseurs possibles par cette méthode et donne une règle pour former les tableaux de différences. Il considère ≪*une équation* ≫

$$P+Qx+Rxx+Sx^3+Tx^4+Vx^5+Wx^6 \text{ etc. } = 0$$

et considère un diviseur possible de la forme

$$p+qx+rxx+sx^3+tx^4+vx^5 \text{ etc. } = 0\,.$$

Il considère les valeurs de ce diviseur possible en 3, 2, 1, 0, −1, −2, −3 et construit le tableau des différences itérées

quam oportet invenire. Auctis et minutis radicibus aequationis datae unitate et binario, divisores ultimorum terminorum provenientes minuantur divisore aliquo coefficientis primi termini ex gr. 1 multipl. per quadratoquadratum unitatis et binarii, numerique resultantes una cum divisoribus ultimi termini aequationis propositae sibi invicem subscribantur, et habebitur talis numerorum series, inter quos ab initio fere — 15. — 9. — 17. — 23

hi inveniuntur — 15.0.9.6. — 0.2.—2.—4

— 10, quorum differentiae — 1.3.0.—1.—3 —9

primas sunt — 15.—9.3. — 0.6.—2.—8

24, differentiae secundae per — 15.—13.—7—17.—10.—25

2 divisae —3.—6.—9, et differentiae tertiae per 3 divisae 1.1, quae quia sunt aequales, sumo 1, h.e. divisorem illum primi termini aequationis datae, qui singuli ultimorum terminorum divisores minuti sunt. pro coefficiente primi termini aequationis tentandae, differentiam ultimam, quae hic etiam est 1 et alias esset coefficiens primi termini aequationis cubicae, pro coefficiente secundi termini, medium inter divisores, qui est novenarius, pro ultimo termino, medium inter differentias secundas h. e. —6 pro coefficiente tertii (in aequatione cubica secundi) termini, et medium terminum vel primum ex duobus mediis inter primas differentias h. e. —9 pro summa coefficientium omnium terminorum excepto primo; hinc subtrahendo —5 summam coefficientium secundi et tertii termini, relinquitur —4 pro coefficiente quarti termini, ut adeo pro divisore quaesito habeamus $x^4 + x^3 - 6xx - 4x + 9 = 0$, per quam aequationem divisio succedit, prodeunte $2x^3 - 4x - 1 = 0$.

Demonstratio hujus Regulae.

Sit haec aequatio data; $P + Qx + Rxx + Sx^3 + Tx^4 + Vx^5 + Wx^6$ etc. $= 0$, quae sit divisibilis per aliam, quam pono esse hanc $p + qx + rxx + sx^3 + tx^4 + ux^5$ etc. $= 0$; suntque et minuantur utriusque aequationis radices successive unitate, binario, ternario etc. resultantumque aequationum ut ex propositarum ultimi termini sibi invicem subscribantur hoc modo:

$P + 30 + 9R + 27S + 81T + 243V + 729W$	$p + 3q + 9r + 27s + 81t + 243u$
$P + 2Q + 4R + 8S + 16T + 32V + 64W$	$p + 2q + 4r + 8s + 16t + 32u$
$P + Q + R + S + T + V + W$	$p + q + r + s + t + u$
P	p
$P - Q + R - S + T - V + W$	$p - q + r - s + t - u$
$P - 2Q + 4R - 8S + 16T - 32V + 64W$	$p - 2q + 4r - 8s + 16t - 32u$
$P - 3Q + 9R - 27S + 81T - 243V + 729W$	$p - 3q + 9r - 27s + 81t - 243u$

Quia igitur $P + Qx + Rxx$ etc. ponitur esse divisibilis per $p + qx + rxx$ etc. oportet p esse partem aliquotam ipsius P, et $p + q + r + s + t + u$ partem aliquotam ipsius $P + Q + R + S + T + V + W$, et $p - q + r - s + t - u$ partem aliquotam ipsius $P - Q + R - S + T - V + W$, et $p - 2q + 4r - 8s + 16t - 32u$ partem aliquotam ipsius $P - 2Q + 4R - 8S + 16T - 32V + 64W$ etc. cuius quando radices datae et quaesitae aequationis utrobique eadem quantitate minuuntur vel augentur, aequatio ex illa resultans adhuc divisibilis est per aequationem, quae ex hac resurgit, adeoque ultimus terminus hujus divisor ultimum terminum illius aequationis; oportet enim $p + qx + rxx$ etc. esse partem aliquotam ipsius $P + Qx + Rxx$ etc. quicunque demum valor pro x substituatur, sive 1.2.3 etc. sive 0, sive —1.—2.—3 etc. unde patet inter divisores ultimorum terminorum semper debere esse aliquos, scilicet hos $p + 3q + 9r$ etc. $p + 2q + 4r$ etc. $p + q + r$ etc. etc. qui ita progrediuntur, ut supra dictum est, quemadmodum videre est ex hac tabella:

	differentiae primae	3tiae per 2 div.
$p+3q+9r+27s+81t+243u$	$q+5r+19s+65s+211u$	
$p+2q+4r+8s+16t+32u$		$r+8s+25t+90u$
$p+q+r+s+t+u$	$q+3r+7s+15s+31u$	$r+3s+7t+18u$
p		$r+3s+\quad t+\quad 6u$
$p-q+r-s+t-u$	$q-3r+7s-15s+31u$	$r-3s+7t-15u$
$p-2q+4r-8s+16t-32u$		$r-5s+22t-80u$
$p-3q+9r-27s+81t-243u$	$q-5r+19s-65s+211u$	

diff. 2de per 1 divisae	diff. 4tae per 4 divisae	diff. 5tae per 5 divisae
$s-8t+32u$		
$s+2t+6u$	$t-5u$	
$s-2t+6u$	$t-9u$	u
$s-8t+32u$	$t-5u$	u

Quod autem in qualibet serie differentiarum medius terminus aut primus ex duobus mediis sit summa omnium possibilium valorum, qui hac expressione continentur $\frac{m^n}{1.2.3\ldots M}$ etc. X N ac patet:

Finge radices aequationis minui successive his quantitatibus a, b, c, d, e, f, g etc. quae denotent numeros progressionis Arithmeticae

[Nicolas (I) Bernoulli 1708, pp. 832–833.

	differentiae primae	diff 2^{ae} per 2 div
$p+3q+9r+27s+81t+243u$		
	$q+5r+19s+65t+211u$	
$p+2q+4r+8s+16t+32u$		$r+6s+25t+90u$
	$q+3r+7s+15t+31u$	
$p+q+r+t+u$		$r+3s+7t+15u$
	$q+r+s+t+u$	
p		$r+0s+t+0u$
	$q-r+s-t+u$	
$p-q+r-s+t-u$		$r-3s+7t-15u$
	$q-3r+7s-15t-31u$	
$p-2q+4r-8s+16t-32u$		$r-6s+25t-90u$
	$q-5r+19s-65t-211u$	
$p-3q+9r-27s+81t-243u$		

diff 3^{ae} per 3 divisae	diff 4^{ae} per 4 divisae	diff 5^{ae} per 5 divisae
$s+6t+25u$		
	$t+5u$	
$s+2t+5u$		u
	$t+0u$	
$s-2t+5u$		u
	$t-5u$	
$s-6t+25u$		

et donne des conditions pour obtenir des progressions arithmétiques dans les colonnes de ce tableau, ce qui permet de reconnaître un diviseur[10].

D. Bernoulli

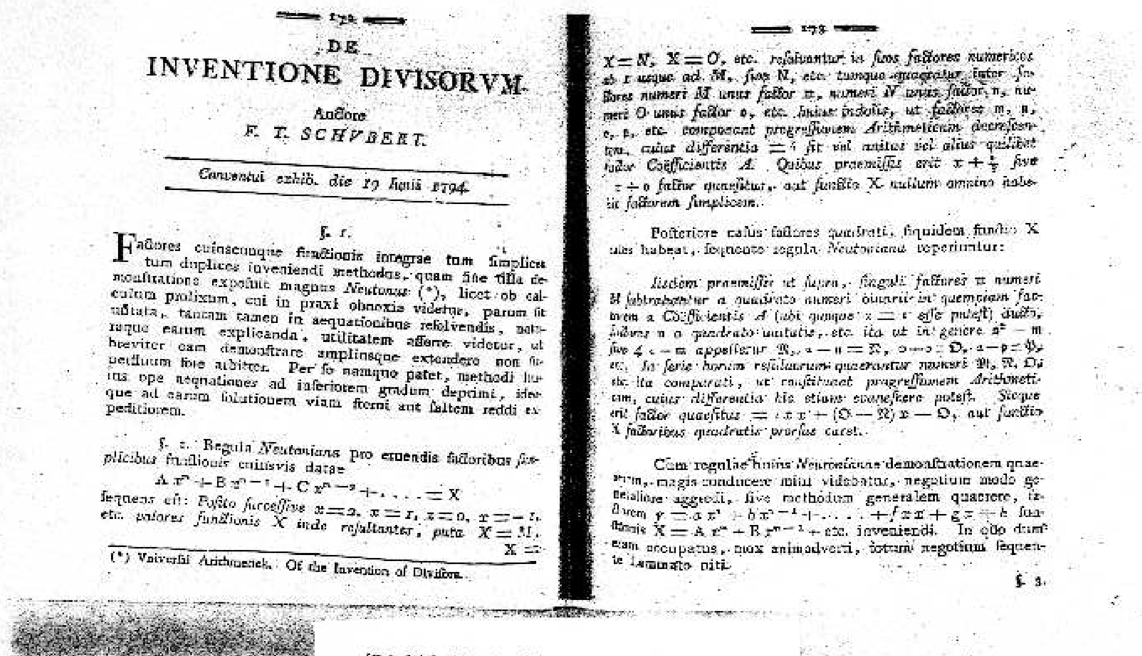
Daniel Bernoulli (1700–1782) donne des explications supplémentaires sur la méthode de Newton dans une note de bas de page insérée dans l'édition latine d'*Arithmetica Universalis*[11] de 1761. Il étudie le cas particulier des diviseurs linéaires $mx+n$ des polynômes cubiques $2x^3+xx+g$. Il considère les valeurs -2, 1, 0 et -1 et étudie ensuite les tableaux de différences finies de leurs diviseurs.

Friedrich Theodor Schubert (1758–1825)

Né le 30 octobre 1758 à Helmstädt (Braunschweig), mort le 21 octobre 1825 à St-Pétersbourg (Russie). Il a étudié à Greisswald et Göttingen.

Il a été précepteur entre 1780 et 1783. Ensuite, en 1783, il s'établit en Russie où il est successivement *réviseur* du département Hapsal d'Estonie (1783–1785), géographe (1785), membre correspondant de l'Académie de St-Pétersbourg (1786),

[10] V. la motivation plus loin.
[11] V.[Isaac Newton, 1761] p. 63–64.



DE

INVENTIONE DIVISORVM.

Auctore

F. T. SCHVBERT.

Conventui exhib. die 19 Junii 1794.

§. 1.

Factores cuiuscunque functionis integrae tum simplices tum duplices inveniendi methodos, quam sine ulla demonstratione exposuit magnus *Newtonus* (*), licet ob calculum prolixum, cui in praxi obnoxia videtur, parum sit usitata, tantam tamen in aequationibus resolvendis, nostraque earum explicanda, utilitatem afferre videtur, ut breviter eam demonstrare ampliusque extendere non superfluum fore arbitror. Per se namque patet, methodi huius ope aequationes ad inferiorem gradum deprimi, ideoque ad earum solutionem viam sterni aut saltem reddi expeditiorem.

§. 2. Regula *Newtoniana* pro eruendis factoribus *simplicibus* functionis cuiusvis datae

$$A x^n + B x^{n-1} + C x^{n-2} + \ldots = X$$

sequens est: *Posito successive* $x = 2$, $x = 1$, $x = 0$, $x = -1$, etc. *valores functionis X inde resultantes, puta* $X = M$, $X =$

(*) Universal Arithmetick. Of the Invention of Divisors.

$X = N$, $X = O$, etc. *resolvantur in suos factores numericos ab 1 usque ad M, sive N, etc. tumque quaeratur, inter factores numeri M unus factor m, numeri N unus factor n, numeri O unus factor o, etc. huius indolis, ut factores m, n, o, p, etc. componant progressionem Arithmeticam decrescentem, cuius differentia* = 1 *sit vel unitas vel alius quilibet divisor Coëfficientis A. Quibus praemissis erit* $x + \frac{n}{1}$ *sive* $x + o$ *factor quaesitus, aut functio X nullum omnino habebit factorem simplicem.*

Posteriore casu factores quadrati, siquidem functio X tales habeat, sequente regula *Newtoniana* reperiuntur:

Iisdem praemissis ut supra, singuli factores m numeri M subtrahantur a quadrato numeri binarii in quempiam factorem a Coëfficientis A (ubi quoque x = 1 esse potest) ducti, factores n a quadrato unitatis, etc. ita ut in genere $4^2 - m$ *sive* $4 - m$ *appelletur* $\mathfrak{M}$, $1 - n = \mathfrak{N}$, $o - o = \mathfrak{O}$, $1 - p = \mathfrak{P}$, *etc. In serie horum residuorum quaerantur numeri* $\mathfrak{M}$, $\mathfrak{N}$, $\mathfrak{O}$, *etc. ita comparati, ut constituant progressionem Arithmeticam, cuius differentia hic etiam evanescere potest. Sicque erit factor quaesitus* $= \iota x x + (\mathfrak{O} - \mathfrak{N}) x - \mathfrak{O}$, *aut functio X factoribus quadratis prorsus caret.*

Cum regulae huius *Newtonianae* demonstrationem quaererem, magis conducere mihi videbatur, negotium modo generaliore aggredi, sive methodum generalem quaerere, functionem $y = a x^r + b x^{r-1} + \ldots + f x x + g x + h$ functionis $X = A x^n + B x^{n-1} +$ etc. inveniendi. In quo dum eram occupatus, mox animadverti, totum negotium sequenti Lemmate niti.

§. 3.

[Friedrich Theodor Schubert, 1798], pp. 172 173

membre de cette Académie (1789), surveillant de la bibliothèque et du cabinet des monnaies de l'Académie (1800-1819) etc. [12]

F. T. Schubert a publié plusieurs livres sur l'astronomie, y inclus un traité d'astronomie théorique en trois volumes (trois éditions, dont une en français, 1791) et une histoire de l'astronomie (1804). Il est l'auteur de plusieurs articles publiés dans *Nov. Act. Acad. Petrop.*, *Bode's Jahr.* et *Zach's Mon. Corr.* entre 1788 et 1830. Ses recherches ne portent pas seulement sur l'astronomie mais aussi sur la géométrie, l'analyse et l'algèbre. En plus de son mémoire sur la factorisation des polynômes de 1798 il a aussi publié un autre article sur l'algèbre, *Demonstratio theoremati algebraici*, en 1810, toujours dans *Nov. Act. Acad. Petrop.*. En analyse, par exemple, il s'est penché sur les séries de Taylor, les extrema, le dévelopement des séries en fractions continues et les fonctions implicites en deux variables. Cela prouve qu'il avait des préoccupations encyclopédiques, comme la plupart des mathématiciens du siècle des lumières. Formé en Allemagne, en particulier comme étudiant à Göttingen, Schubert a eu l'occasion de consulter les œuvres de Leibniz et de Newton, d'où son intérêt pour le calcul des diviseurs linéaires et quadratiques des polynômes à coefficients entiers.

N. Bernoulli et F. T. Schubert sont des pionniers. Avant eux il y avait, à notre connaissance, seulement des études particulières – pas de traitement du cas général. Même si leurs techniques de rédaction (usage des tableaux, présentation des méthodes par des exemples) remontent au moins à Newton, leurs techniques pour la factorisation était en avance de plus de cent ans.

La source de F. T. Schubert

Dès le début de son ouvrage Schubert précise que sa méthode repose sur des résultats de I. Newton pour trouver des facteurs de degré un ou deux des polynômes à coefficients entiers [Isaac Newton, 1707].

F. T. Schubert cite au début de son mémoire, p. 172, l'ouvrage *Vniversal Arithmetick. Of the Invention of Divisors.* Il ne donne ni l'année, ni l'éditeur. Puisqu'il s'agit d'une version anglaise c'est très probable qu'il a utilisé la traduction de Ralphson de 1710 ou de 1728 [Isaac Newton, 1710]. Rien n'indique que Schubert connaissait l'ouvrage de N. Bernoulli [Nicolas (I) Bernoulli, 1708].

Même si son ouvrage est contemporain aux œuvres de Lagrange, pour donner seulement un exemple, le style de Schubert est très proche de celui de Newton, Leibniz et Bernoulli. Il énonce une règle générale, ensuite il donne la justification par des exemples.

On ignore la raison immédiate pour laquelle il s'est occupé de la méthode de Newton. Tandis que pour Bernoulli l'ouvrage de Newton était récent et avait attiré l'intérêt des contemporains, chez Schubert le mémoire sur la factorisation semble être passé quasiment inaperçu.

[12] Notons que F. T. Schubert est l'arrière grand père maternel de la célèbre mathématicienne Sophie Kovalewskaya (1850–1891).

L'ouvrage de Schubert

Décrivons ce que F. T. Schubert a exposé dans son mémoire. Nous conservons pour le moment ses notations, ensuite nous adopterons des conventions plus modernes.

Schubert considère un polynôme à coefficients entiers[13], qu'il note X,

$$X = Ax^m + Bx^{m-1} + Cx^{m-2} + \dots$$

et il se propose de trouver un facteur, noté y, de degré $n \geq 1$ à coefficients entiers,

$$y = ax^n + bx^{n-1} + cx^{n-2} + \dots + fxx + gx + h.$$

Il écrit (p. 177) qu'on a $X = yY$, avec

$$Y = (kx^\mu + lx^{\mu-1} + \dots)(px^\tau + qx^{\tau-1} + \dots)$$

et il en déduit

$$m = n + \mu + \tau \quad \text{et} \quad A = akp,$$

même s'il n'utilise pas cette décomposition. Puis il considère le polynôme

$$ax^n - y = -bx^{n-1} - cx^{n-2} - \dots - fxx - gx - h,$$

et calcule les valeurs des polynômes X et $ax^n - y$ aux points 0, ± 1, ± 2, ... et construit le tableau suivant (page 178):

x	***Factor*** y	ax^n	***Residua***
$+2$	$2^n a + 2^{n-1}b + \dots + 4f + 2g + h$	$+2^n a$	$-2^{n-1}b - 2^{n-2}c - \dots - 4f - 2g - h = \mathcal{M}$
$+1$	$a + b + c + \dots + f + g + h$	$+a$	$-b - c - \dots - f - g - h = \mathcal{N}$
0	$+h$	0	$-h = \mathcal{O}$
-1	$\pm a \pm b \pm c \dots + f - g + h$	$\pm a$	$\mp b \pm c \dots - f + h - h = \mathcal{P}$
-2	$\pm 2^n a \pm 2^{n-1}b \dots + 4f - 2g + h$	$\pm 2^n a$	$\mp 2^{n-1}b \pm 2^{n-1}c \dots - 4f + 2g - h = \mathcal{Q}$

Ensuite Schubert calcule les différences $\Delta^j(ax^n - y)$ et s'aperçoit que la suite des valeurs de $\Delta^{n-2}(ax^n - y)$ est une progression arithmétique de nombres entiers.

La méthode de Bernoulli–Schubert repose sur la propriété suivante:

Soit F un polynôme à coefficients rationnels de degré d plus petit que n. On considère $y_i = F(x_i)$, où $x_1 = x_0 + a$, ..., $x_n = x_0 + na$, avec x_0 et a des entiers. Alors la suite $\Delta^{d-1}(y_0, \dots, y_n)$ est en progression arithmétique.

Dans leurs mémoires Bernoulli et Schubert supposent implicitement cette proprieté. Mais il connaissaient parfaitement les résultats de Newton[14] et c'est très probablement l'utilisation des diffèrences finies qui les avaient conduits à construire les tableaux de leurs ouvrages.

[13] Comme Jakob Hermann, v [Gottfried Wilhelm Leibniz, 1859], p. 329.

[14] Schubert rappelle au début de son ouvrage les recherches de Newton sur les différences finies ainsi que sur les facteurs de degré un ou deux des polynômes [Isaac Newton, 1707].

Schubert ne donne aucune référence aux travaux antérieurs de Nicolas Bernoulli. Il ne cherche pas à determiner le polynôme y mais $x^n - y$, réduisant ainsi le degré d'une unité. Grâce aux tableaux des différences il évite de considérer les opérations avec des rationnels qui ne soient pas des entiers, ce que pourrait arriver si on cherchait les facteurs par interpolation. Ces artifices permettent de minimiser les calculs et élargissent un peu la famille des polynômes pour lesquels sa méthode aboutit à la factorisation.

Poursuivons la lecture du mémoire de Schubert. Dans les paragraphes 7–12 (pages 180–185) il considère les valeurs que prend X aux points 0, ± 1, ± 2, ± 3, ... et il regarde les diviseurs de ces valeurs. Il donne des formules pour les possibles diviseurs linéaires, quadratiques, cubiques et biquadratiques. Ensuite il affirme que $\ll$*Regulam nostram uno exemplo illustrasse sufficiet* $\gg$, c'est à dire "il suffira d'un exemple pour illustrer notre règle". Cette façon d'argumenter un résultat, même si elle n'est plus acceptée pour les mathématiciens contemporains, était largement utilisée avant le XIX$^{\text{e}}$ siècle. On va voir plus loin que sa méthode est correcte.

Comme exemple il choisit

$$X = x^6 - 2x^5 + 3x^4 - 3x^3 + 3x^2 - 2x + 1$$

et il cherche un facteur de degré quatre, soit

$$y = ax^4 + bx^3 + cx^2 + dx + e\,.$$

Il considère d'abord les valeurs de X aux points 3, 2, 1, 0, -1, -2 et construit un tableau contenant ces valeurs ainsi que les entiers positifs qui sont des diviseurs de ces valeurs. La colonne de ces diviseurs est appelé *factores speciales* (facteurs spéciaux).

x	X	*Factores speciales* y
+3	+427	1. 7. (61). 427.
+2	+33	1. 3. (11). 33.
+1	+1	(1).
0	+1	(1).
−1	+15	1. 3. (5). 15.
−2	+217	1. 7. (31). 217.

La signification des diviseurs entre parenthèses va être expliquée un peu plus tard.

Schubert choisit $a = 1$ et construit le tableau de différences suivant:

x^4	*Residua* $x^4 - y$	$\Delta(x^4 - y)$	$\Delta^2(x^4 - y)$
+81	+80. 74. (+20). etc.		
		+65. +61. (+15).	
+16	+15. +13. (+5). −17		+50. +48. (+10).
		+15. +13. (+5).	
+1	().		+14. +12. (+4).
		+1. +1. (+1).	
0	(−1).		+2. 0. (−2).
		−1. +1. (+3).	
+1	0. −2. (−4). −14.		+14. +12. (−8).
		−15. −11. (+11).	
+16	+15. +9. (−15). −201.		

Le tableau précédent est construit selon la règle suivante: Chacune des colonnes $\Delta(x^4 - y)$ et $\Delta^2(x^4 - y)$ est la suite formée par les différences des termes des deux suites successives de la colonne précédente.

Choisissant dans la colonne des valeurs de $x^4 - y$ les nombres entre parenthèses, on obtient dans les colonnes $\Delta(x^4 - y)$ et $\Delta^2(x^4 - y)$ les nombres entre parenthèses. La dernière suite, celle de la colonne $\Delta^2(x^4 - y)$, est une progression arithmétique de raison 6.

Il cherche alors le polynôme $x^4 - y$ qui prend les valeurs entre parenthèses dans la colonne des valeurs de $x^4 - y$. Il résout le système d'équations linéaires correspondant et trouve

$$x^4 - y = x^3 - x^2 + x - 1$$

donc

$$y = x^4 - x^3 + x^2 - x + 1\,.$$

Ensuite il observe que y est un vrai facteur du polynôme X et obtient l'autre facteur

$$X/y \;=\; x^2 - x + 1\,,$$

d'où la factorisation de X:

$$x^6 - 2x^5 + 3x^4 - 3x^3 + 3x^2 - 2x + 1 \;=\; (x^4 - x^3 + x^2 - x + 1)\cdot(x^2 - x + 1)\,.$$

Analyse de la méthode de Bernoulli–Schubert

Le procédé de Bernoulli–Schubert repose sur l'interpolation des facteurs possibles du polynôme de départ, en utilisant la méthode des différences finies comme déjà chez Newton et Leibniz.

Ces deux auteurs ont le mérite de détailler la méthode de Newton, de fournir des explications nouvelles et de rendre ainsi cette méthode plus accessible.

Notons que Schubert affirme (paragraphe 9, p. 182) que par cette méthode il ne peut pas découvrir des facteurs multiples [15]. Son argumentation repose sur

[15] Facile denique perspicitur, methodo hac factores multiplices reperiri non posse.

la remarque que d'une égalité $X(d) = 0 \cdot y(d)$, avec d une racine entière de X, on ne peut rien déduire sur la valeur de $y(d)$. Cependant on peut éviter les racines entières du polynôme en choisissant les valeurs pour lesquelles le polynôme ne s'annule pas. Par exemple, si on considère le polynôme

$$X = x^4 - 2x^3 + 2x^2 - 2x + 1$$

on va voir qu'il a de facteurs multiples. Ce polynôme s'annule en 1, mais si on choisit pour noeuds du tableau des différences les points 2, 3, 4, 5 et 6 on trouve par son algorithme les diviseurs $x^2 + 1$ et $x^2 - 2x + 1$, ensuite la factorisation

$$x^4 - 2x^3 + 2x^2 - 2x + 1 \; = \; (x-1)^2(x^2+1)\,.$$

Par ailleurs, puisqu'on cherche une factorisation du polynôme, dès qu'on trouve un entier d tel que $X(d) = 0$ on peut diviser le polynôme par le facteur linéaire $x - d$ avant d'appliquer la méthode de Bernoulli–Schubert.

2 L'algorithme de Kronecker

C'est le mathématicien allemand Leopold Kronecker qui est considéré comme le premier inventeur d'un algorithme général de factorisation des polynômes à coefficients entiers. Dans l'ouvrage [Leopold Kronecker, 1882] de plus de cent pages, il étudie la factorisation des polynômes d'une variable à coefficients entiers sur une seule page [Leopold Kronecker, 1882], p. 10 (v. aussi [Leopold Kronecker, 1897], p. 256–258). Certainement Kronecker était préoccupé par ce problème auparavant. Par exemple, dans ses leçons non publiées sur les équations algébriques du Wintersemester 1880/1881 [Leopold Kronecker, 1880], il présente déjà – et en détail – ce procédé. Il reviendra sur ce sujet dans son cours sur la théorie des nombres [Leopold Kronecker, 1901], p. 178–181.

Kronecker se penche sur le problème de la factorisation des polynômes dans un grand cours[16] sur la théorie algébrique des nombres et également dans un mémoire sur le même sujet.

Il est partisan d'une approche constructive des mathématiques, voir sa remarque sur l'irréductibilité au début de cet article.

Kronecker considère la factorisation des polynômes à coefficients entiers dans un contexte général. Son algorithme s'insère dans un grand projet: la présentation dans une même théorie de la théorie algébrique des nombres et celle des fonctions algébriques d'une variable.

Dans son ouvrage les polynômes à coefficients entiers jouent un rôle fondamental. La plus grande partie de son travail est dédiée à l'étude des "Gattungen", des quantités algébriques sur des "Rationalitätsbereiche", c'est à dire des éléments algébriques sur le corps des fractions d'un anneau de polynômes de plusieurs variables sur les entiers.

[16] Comme Newton.

On peut dire que pour Kronecker, pour vérifier qu'un anneau de polynômes est factoriel, il faut donner une méthode de décomposition. Cela se voit surtout dans sa préoccupation de vérifier que les polynômes à plusieurs variables peuvent être aussi factorisés dans un produit de polynômes irréductibles. Dans son cours, avant de quitter la section sur la factorisation des polynômes, il tient à indiquer aussi un algorithme pour la factorisation des polynômes à plusieurs variables. La transformation qu'il utilise est, de point de vue de la complexité des calculs, assez mauvaise, mais donne quand même une solution effective du problème.

Brièvement le procédé de factorisation de Kronecker est le suivant.

Soit $F(x)$ un polynôme à coefficients entiers de degré $2n$ ou $2n+1$. Pour trouver un diviseur à coefficients entiers il suffit de trouver un diviseur de degré n ou plus petit. Soient alors les entiers distincts r_0, r_1, r_2, ..., r_n et posons

$$g_0(x) = \frac{(x-r_1)(x-r_2)\cdots(x-r_n)}{(r_0-r_1)(r_0-r_2)\cdots(r_0-r_n)},$$

$$g_1(x) = \frac{(x-r_0)(x-r_2)\cdots(x-r_n)}{(r_1-r_0)(r_1-r_2)\cdots(r_1-r_n)},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

alors chaque polynôme à coefficients entiers $f(x)$, dont le degré ne dépasse pas n, est representé comme une combinaison linéaire des polynômes $g(x)$, et on a

$$f(x) = f(r_0)g_0(x) + f(r_1)g_1(x) + \cdots + f(r_n)g_n(x)\,,$$

qui n'est autre que la formule d'interpolation de Lagrange.

Soit $f(x)$ un diviseur du polynôme donné $F(x)$, alors le coefficient de $g_h(x)$ de cette représentation doit être un diviseur de l'entier $F(r_h)$, et alors on doit discuter seulement un nombre fini de systèmes de coefficients, afin d'obtenir tous les diviseurs de $F(x)$ ou de démontrer l'irréducibilité de $F(x)$.

On peut noter que L. Kronecker étudie encore plus brièvement[17] l'utilité de sa méthode pour la factorisation des polynômes à plusieurs variables à coefficients entiers. Si on veut factoriser un polynôme dans les variables qu'il note par x, x', ..., $x^{(n)}$ il propose le changement de variables

$$x' = c_1 x^g, x'' = c_2 x^{g^2}, \ldots, x^{(n)} = c_n x^{g^n}$$

qui conduit à un polynôme d'une variable à coefficients entiers.

[17] Une demi–page [Leopold Kronecker, 1882], p. 11.

Nun ist:

$$\frac{F(x,x_1)}{F'(x_1)} = -\frac{1}{2}(x^3+2x^2-x-2)$$

$$\frac{F(x,x_2)}{F'(x_2)} = \frac{1}{6}(x^3+3x^2+2x)$$

$$\frac{F(x,x_3)}{F'(x_3)} = \frac{1}{2}(x^3+x^2-2x)$$

$$\frac{F(x,x_4)}{F'(x_4)} = \frac{1}{6}(x^3-x)$$

Bezeichnen wir für C_1, C_2, C_3, C_4 resp. $1, 4, -2, -11$, so folgt

$$\Psi(x) = \sum_{\kappa=1}^{4} C_\kappa \frac{F(x,x_\kappa)}{F'(x_\kappa)} = x^3+2x+1.$$

Diese Rolle liefert also eine ganze ganzzahlige Funktion. Es ist in der That eine Theiler von $F(x)$, denn durch Division von x^3+2x+1 in $F(x)$ erhalten:

$$x^5-x^4+x^3-x^2-3x-1 = (x^3+2x+1)(x^2-x-1).$$

§ 11. Nachdem wir uns eine Methode gewonnen haben, die in jedem einzelnen Falle erlaubt, zu entscheiden, ob eine vorgelegte ganze ganzzahlige Function von x ganze ganzzahlige Divisoren hat, sind wir berechtigt, den Begriff der Ungerlegbarkeit oder Irreducibilität aufzustellen. Unter einer ungerlegbaren oder irreducibeln Function von x, verstehen wir eine ganze ganzzahlige Function von x, welche nicht in ganze ganzzahlige Divisoren gerlegt werden kann, also ausschließen Zahlenfactor entfällt. Eine irreducible Function spielt unter den Functionen eine ähnliche Rolle wie die Primzahlen bei den Zahlen. Jede ganze ganzzahlige Function läßt sich also jetzt darstellen in der Form:

$$F(x) = p_1^{k_1} p_2^{k_2} \cdots p_\mu^{k_\mu} f_1^{k_1} f_2^{k_2} \cdots f_\nu^{k_\nu},$$

wo $p_1 \cdots p_\mu$ Primzahlen, $f_1 \cdots f_\nu$ irreducible Functionen und $k_1 \cdots k_\mu$, $k_1 \cdots k_\nu$ ganze positive Zahlen sind. Es gilt nun wie bei der Zerlegung der Zahlen der Satz, daß diese Zerlegung eine eindeutige

Leopold Kronecker, 1880], §40.

Réduction des calculs par Runge

Par interpolation le polynôme $f(x)$ intervenant dans l'algorithme de Kronecker peut être à coefficients rationnels qui ne soient pas des entiers. Si on prend, par exemple,

$$F(x) \;=\; 7x^4 - 6x^3 + 8x^2 - x + 2,$$

on trouve $F(-1) = 24$, $F(0) = 2$, $F(1) = 10$. Si on suppose $f(-1) = 4$, $f(0) = 1$ et $f(1) = 5$ on obtient

$$f(x) \;=\; \tfrac{7}{2}x^2 + \tfrac{1}{2}x + 1$$

qui n'est pas à coefficients entiers.

La méthode de Kronecker suppose le calcul de tous les polynômes d'interpolation $f(x)$, même ceux qui ne sont pas à coefficients entiers. Runge a proposé [Carl Runge, 1886] une méthode qui évite de calculer ces polynômes, ce qui permet de réduire la taille des calculs.

Il utilise les mêmes notations que Kronecker. Il remarque que si $f(x)$ est à coefficients entiers, alors $\dfrac{f(x) - f(r_\alpha)}{x - r_\alpha}$ prend des valeurs entières, donc $f(r_\beta) - f(r_\alpha)$ doit être divisible par $r_\beta - r_\alpha$. Alors parmi les diviseurs entiers Θ_α de $f(r_\alpha)$ il faut examiner seulement ceux assujettis aux conditions du type

$$\Theta_\alpha \;\equiv\; \Theta_\beta \,(\mathrm{mod.}\, \overline{r_\alpha - r_\beta}).$$

Les remarques de Van der Waerden

Dans son célèbre traité Van der Waerden [Bartel L. Van der Waerden, 1937] fait, en particulier, deux remarques sur le mémoire de Kronecker. Il affirme que c'est préférable d'utiliser les différences finies pour l'interpolation plutôt que l'interpolation de Lagrange. C'est aussi le choix de Newton, Leibniz, N. Bernoulli et Schubert, mais pas celui de Kronecker.

Il suggère d'utiliser la décomposition des polynômes modulo un nombre premier pour obtenir des informations sur la factorisation des polynônes sur les entiers ordinaires. On peut considérer que cette remarque anticipe la méthode moderne de Berlekamp–Zassenhaus.

3 L'approche de Hausmann

B. A. Hausmann [Bernard A. Hausmann, 1937] a donné une autre amélioration de l'algorithme de Kronecker. Sa méthode permet d'établir grâce à l'étude d'une liste d'entiers si le polynôme interpolé lui correspondant est vraiment un diviseur d'un polynôme f à coefficients entiers. Elle repose sur des propriétés des polynômes de Hurwitz ainsi que sur l'étude des tableaux de différences. Il faut bien observer que Hausmann, de même que Kronecker, semble avoir complétement ignoré les oeuvres de N. Bernoulli et F. T. Schubert.

Hausmann revient aux différences finies. Il considère un polynôme $f(x)$ de degré n à coefficients entiers qui est *stable*[18], c'est à dire dont toutes les racines sont de partie réelle négative. On notera que l'hypothèse de stabilité des polynômes conduit à une méthode plus efficace que celle de Kronecker, mais voir aussi la remarque plus loin.

Il note qu'un tel polynôme $f(x)$ possède seulement des coefficients strictement positifs et il le suppose factorisé en $f(x) = g_1(x) \cdot g_2(x)$, avec $g_1(x)$ de degré r et $g_2(x)$ de degré s. Il remplace x par 1, 2, ..., $n+1$ et obtient les ensembles de valeurs

$$[a_0, \ldots, a_n] = [b_0, \ldots, b_n] \cdot [c_0, \ldots, c_n],$$

où $a_i = f(i+1)$, $b_i = g_1(i+1)$ et $c_i = g_2(i+1)$.
Il considère alors le tableau des différences

$$\begin{array}{ccccc} a_0 & a_1 & a_2 & \ldots & a_n \\ & a_1 - a_0 & a_2 - a_1 & \ldots & a_n - a_{n-1} \\ & & a_2 - 2a_1 + a_0 & \ldots & a_d - 2a_{n-1} + a_{n-2} \\ & & & \vdots & \vdots \\ & & & & \vdots \end{array}$$

et trouve que la différence d'ordre n est constante. Par ailleurs ce tableau peut être complété à droite, si nécessaire, par les valeurs a_{n+1}, a_{n+2}, ...

B. A. Hausmann obtient ensuite le résultat suivant:

Théorème. *Si* $[a_0, \ldots, a_n] = [b_0, \ldots, b_n] \cdot [c_0, \ldots, c_n]$, *où les* a_i *ont été obtenus à partir d'un certain polynôme* $f(x)$, *du type considéré, par substitution de* x *par les* $n+1$ *entiers* 1, 2, ..., $n+1$, *et où les* b_i *et les* c_i *satisfont les relations*

1) $a_i = b_i c_i$;
2) $b_0 \geq 2$ *et* $b_0 < b_1 < \ldots < b_d$;
3) $c_0 \geq 2$ *et* $c_0 < c_1 < \ldots < c_d$;

alors les b_i *définissent un polynôme* $g_1(x)$ *et les* c_i *définissent un polynôme* $g_2(x)$ *tels que* $f(x) = g_1(x) \cdot g_2(x)$ *si et seulement si tableau des différences d'ordre* r *des* b_i *est constant; le tableau des différences d'ordre* s *des* c_i *est constant; et* $r + s = n$.

La méthode de Hausmann traite de la factorisation des polynômes à coefficients entiers qui sont stables, c'est à dire dont les parties réelles des racines sont négatives. Cette méthode peut aussi être utilisée aussi dans le cas des polynômes qui ne sont pas stables grâce à une translation convenable. En effet, si le polynôme $f(x)$ n'est pas stable, soit M un nombre positif tel que

$$|f(z)| \neq 0 \qquad \text{si} \qquad |z| \geq M,$$

[18] On dit aussi polynôme de Hurwitz.

alors le polynôme $S(x) = f(x - \lfloor M \rfloor - 1)$ est stable.

B. A. Hausmann choisit pour M la borne des racines découverte par Cauchy [Augustin–Louis Cauchy, 1829]: Pour le polynôme $P(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n$, la borne supérieure de Cauchy pour les modules des racines est $M = 1 + \max |a_k|/|a_0|$, (k=1, 2, ..., n). On obtient la factorisation de $S(x)$, et ensuite, par translation, celle de $f(x)$. Mais en général les coefficients du polynôme $S(x)$ sont très grands, ce qui rend la méthode inutilisable en pratique pour des polynômes quelconques. En passant, on peut aussi noter que tester si le polynôme $f(x)$ est stable est une tâche lourde dès que le degré n de $f(x)$ atteint cinq.

L'avantage de l'approche de A. Hausmann est qu'au lieu de calculer les polynômes d'interpolation et vérifier par division si un tel polynôme est un diviseur de $f(x)$, on construit des tableaux de différences des suites b_i et c_i. Si leurs ordres sont r, respectivement s, et si on trouve $r+s = n$, alors on a trouvé une factorisation de $f(x)$. Autrement on essaie d'autres valeurs. Il n'y a qu'un nombre fini d'essais nécessaires.

4 Conclusions

Au terme de cette analyse on peut noter que le facteur commun entre les méthodes de Bernoulli–Schubert, Kronecker et Hausmann est la recherche des facteurs possibles par l'intermédiaire de la factorisation des valeurs prises par ces polynômes.

Premier pas:

Il est commun à toutes ces méthodes. Il consiste à calculer les valeurs du polynôme à factoriser $F(x)$ pour un certain nombre d'entiers distincts. Ce nombre d'entiers distincts est au plus $n + 1$, où n est le degré du polynôme. Dans la suite ce nombre sera noté par e.

Deuxième pas:

Partie commune aux trois méthodes: On choisit $b_0, \ldots, b_e$ diviseurs de $a_0, \ldots, a_e$.

a) Bernoulli et Schubert choisissent e égal au degré du polynôme, étudient la tabulation de $(b_0, \ldots, b_n)$ et testent si elle correspond à l'ensemble des valeurs d'un polynôme $f(x)$. Si ce n'est pas le cas l'essai a echoué, sinon on calcule G_1 grâce au théorème d'interpolation par différences finies de Newton.

b) Kronecker se contente de prendre pour e le plus grand entier ne dépassant pas la moitié du degré de $F(x)$, et il construit directement $f(x)$ par la méthode d'interpolation de Lagrange.

c) Hausmann, comme Schubert, prend e égal au degré du polynôme et considère simultanément g_1 défini par $g_1(i+1) = b_i$ et g_2 défini par $g_2(i+1) = a_i/b_i$. Il vérifie ensuite si les tabulations de g_1 et g_2 correspondent à celles d'un couple de polynômes et utilise son théorème.

Troisième pas:

Les deux premiers auteurs doivent enfin tester si le polynôme $f(x)$ est effectivement un diviseur de $F(x)$, si ce n'est pas le cas ils esssaient une autre décomposition, à condition qu'il en reste encore.

Cela n'a pas beaucoup de sens de comparer les efficacités respectives des trois méthodes, en pratique aucune n'est utilisable dès que le degré de F dépasse six. La raison est la suivante: pour chaque valeur a_i de $F(x)$ le nombre de choix des b_i est égal à deux fois le nombre des diviseurs positifs des a_i (sauf pour la méthode de Hausmann), il y a donc un nombre considérable d'essais à effectuer pour n au moins égal à six.

Les méthodes contemporaines diffèrent totalement de celles des pionniers. De plus, elles permettent de factoriser des polynômes de degré de l'ordre de la centaine. Même avec les ordinateurs d'aujourd'hui, les méthodes de Bernoulli–Schubert, Kronecker et Hausmann ne permettraient pas de factoriser des polynômes de degré vingt.

Dans les méthodes modernes de factorisation on utilise deux étapes:

- On choisit d'abord un nombre premier convenable p et on factorise le polynôme modulo p. Cette factorisation est très rapide et on dispose de plusieurs algorithmes efficaces qui reposent essentiellement sur des remarques d'algèbre linéaire sur les corps finis.
- On raffine la factorisation modulo une puissance d'un nombre premier. Cette technique utilise un lemme célèbre de K. Hensel en analyse p–adique [Kurt Hensel, 1918] et des majorations sur les coefficients d'un diviseur possible d'un polynôme. Ces dernières majorations peuvent être démontrées grâce à l'algèbre élémentaire sur les nombres complexes, v. M. Mignotte [Maurice Mignotte, 1974].

Il existe deux méthodes pour achever cette factorisation, une est celle de Zassenhaus–Berlekamp (v. [Elwyn R. Berlekamp, 1967], [Hans Zassenhaus, 1969]), l'autre a été inventée par A. K. Lenstra, H. W. Lenstra and L. Lovász (v. [Arjen K. Lenstra, Hendrik W. Lenstra Jr., László Lovász, 1982]).

Remerciements. Nous sommes extrêmement reconnaissants à Norbert Schappacher qui a fait plusieurs remarques très pertinentes sur une première ébauche de rédaction et qui nous a communiqué les références [Leopold Kronecker, 1880] et [Leopold Kronecker, 1901] sur Kronecker.

Bibliographie

[Elwyn R. Berlekamp, 1967] Factoring polynomials over finite fields, *Bell Systems Tech. J.*, **46**, 1853–1859 (1967).

[Nicolas (I) Bernoulli, 1708] Regula Generalis Inveniendi Aequationes, per quas alia quepiam data, modo reducibilis sit, dividi potest, en Gottfried Wilhelm Leibniz, *Mathematische Schriften*, bd. III, Halle (1856).

[Moritz Cantor, 1908] *Vorlesungen über die Geschichte der Mathematik*, bd. IV, Teubner, Leipzig (1908).

[Augustin–Louis Cauchy, 1829] *Exercises de Mathématiques*, 4$^{\text{ème}}$ année, De Bure Frères, Paris (1829).

[Enc. Sci. Math., 1992] *Encyclopédie des sciences mathématiques pures et appliquées*, t. 1, vol. 2, J. Gabay, Paris (1992).

[Bernard A. Hausmann, 1937] A new simplification of Kronecker's method of factorization of polynomials, *Amer. Math. Monthly*, **44**, 574–576 (1937).

[Kurt Hensel, 1918] Eine neue Theorie der algebraischen Zahlen, *Math. Z.*, **2**, 433–452 (1918).

[Donald E. Knuth, 1981] *The Art of Computer Programming*, Volume 2: Seminumerical Algorithms, Addison–Wesley, Reading Ma (1981).

[Leopold Kronecker, 1880] Theorie der algebraischen Gleichungen, Wintersemester 1880/1881. (manuscrit L 2262, Bibl UFR Math. Strasbourg).

[Leopold Kronecker, 1882] Gründzuge einer arithmetischen Theorie der algebraischen Grössen, *J. reine ang. Math.*, **92**, 1–122 (1882).

[Leopold Kronecker, 1897] *Leopold Kronecker's Werke*, bd. II, 237–387, B. G. Teubner, Leipzig (1897).

[Leopold Kronecker, 1901] *Vorlesungen über algemeine Arithmetik*, B. G. Teubner, Leipzig (1901).

[Gottfried Wilhelm Leibniz, 1856] *Mathematische Schriften*, bd. III, Halle (1856).

[Gottfried Wilhelm Leibniz, 1859] *Mathematische Schriften*, bd. IV, Halle (1859).

[Arjen K. Lenstra, Hendrik W. Lenstra Jr., László Lovász, 1982] Factoring polynomials with rational coefficients, *Math. Ann.*, **261**, 515–534 (1982).

[John Michael McNamee] A bibliography on roots of polynomials, *J. Comput. Appl. Math.*, **47**, p. 391–392 (+diskette) (1993), v. également http://www.elsevier.com/homepage/sac/cam/mcnamee/index.html.

[Maurice Mignotte, 1974] An inequality about factors of polynomials, *Math. Comp.*, **28**, 1153–1157 (1974).

[Isaac Newton, 1707] *Arithmetica Universalis*, Cambridge (1707).

[Isaac Newton, 1710] *Universal Arithmetick*, London (1710).

Reprinted in *Mathematical Works*, vol. 2, Johnson Reprint Corp., (1967).

[Isaac Newton, 1761] *Arithmetica Universalis*, Amsterdam (1761).

[Isaac Newton, 1802] *Arithmétique universelle de Newton*, trad. par Noël Beaudeux, Bernard, Paris, An X (1802).

[Isaac Newton, 1972] *The Mathematical Papers of Isaac Newton*, ed. D. T. Whiteside, vol. 5, Cambridge University Press (1972).

[Johann Christian Poggendorff (ed.)] *Biographisch–literarisches Handwörterbuch zur Geschichte der exacten Wissenschaften*, Bd. 2, p. 850–852, Leipzig (1863).

[Carl Runge, 1886] Ueber die Zerlegung ganzer ganzzahliger Functionen in irreductible Factoren, *J. reine u. angew. Math.*, **99**, 89–97 (1886).

[Friedrich Theodor Schubert, 1798] De Inventione Divisorum, *Nova Acta Scient. imp. Petropolitanae*, t. **XI**, ad annum 1793, Petropoli 1798, 172–182. (1798).

[Bartel L. Van der Waerden, 1937] *Moderne Algebra I*, Springer, Berlin (1937).

[Hans Zassenhaus, 1969] On Hensel factorization, *J. Number Theory*, **1**, 291–311 (1969).

Université Louis Pasteur
UFR de Mathématique
67084 Strasbourg Cedex
France
mignotte@math.u-strasbg.fr

Université de Bucarest
B. P. 39–D5
Bucarest 39, Roumanie
stef@irma.u-strasbg.fr
stef@mat.fizica.unibuc.ro