BULLETIN DE LA S. M. F.

D. SELIVANOFF

Sur la recherche des diviseurs des fonctions entières

Bulletin de la S. M. F., tome 13 (1885), p. 119-131

<http://www.numdam.org/item?id=BSMF_1885__13__119_1>

Sur la recherche des diviseurs des fonctions entières; par D. Sélivanoff.

(Séance du 2 avril 1885.)

Soit

$$f(x) = x^n + c_1 x^{n-1} + c_2 x^{n-2} + \ldots + c_{n-1} x + c_n$$

un polynôme quelconque à coefficients entiers.

Nous nous proposons de trouver les diviseurs de $f(x)$ à coefficients entiers.

La recherche des diviseurs du premier degré est bien connue. Il est souvent utile dans cette recherche d'avoir en vue la remarque suivante, due à Gauss.

Si

$$f(x) = (x - a)\psi(x),$$

on a de même

$$f(x) \equiv (x - a)\psi(x) \pmod{n},$$

n désignant un nombre entier quelconque.

En posant $x = a$, on obtient

$$f(a) \equiv 0 \pmod{n}.$$

Si la dernière congruence a lieu, on a

$$f(x) \equiv f(x) - f(a) \pmod{n}$$

ou

$$f(x) \equiv x^n - a^n + c_1(x^{n-1} - a^{n-1}) + \ldots + c_{n-1}(x - a) \pmod{n}.$$

Chaque différence étant algébriquement divisible par $x - a$, on aura

$$f(x) \equiv (x - a)\psi(x) \pmod{n},$$

$$\psi(x) = \frac{x^n - a^n}{x - a} + c_1 \frac{x^{n-1} - a^{n-1}}{x - a} + \ldots + c_{n-1}.$$

Les deux congruences considérées sont donc identiques.

Si aucun des nombres

$$f(0),\ f(1),\ f(2),\ \ldots,\ f(n-1)$$

n'est multiple de n, il est impossible que

$$f(a) \equiv 0 \pmod{n},$$

car

$$f(a) \equiv f(b), \quad \text{si} \quad a \equiv b \pmod{n}.$$

Dans ce cas la fonction $f(x)$ ne peut avoir des diviseurs du premier degré.

Si, parmi les nombres nommés, $f(1)$ est le seul divisible par n, on conclut

$$f(x) \equiv (x-1)\psi(x) \pmod{n}.$$

La fonction $f(x)$ peut admettre un diviseur $x - a$, mais il est nécessaire, dans ce cas, que

$$a \equiv 1 \pmod{n}.$$

Passons maintenant à la recherche des diviseurs de second degré de la forme

$$\varphi(x) = x^2 + ax + b.$$

On peut suivre la méthode dont quelques points importants m'ont été indiqués par mon ami M. Runge.

On détermine d'abord la limite supérieure des modules des racines de l'équation $f(x) = 0$. Soit ρ cette limite.

Ce nombre peut être déterminé par les conditions

$$\mathfrak{F}(\rho) > 0, \quad \mathfrak{F}(\rho - 1) < 0,$$

où

$$\mathfrak{F}(x) = x^n - |c_1|x^{n-1} - |c_2|x^{n-2} - \ldots - |c_{n-1}|x - |c_n|,$$

ρ étant un nombre entier et le signe $|a|$ désignant le module de a.

Supposons que

$$f(x) = \varphi(x)\psi(x), \quad \varphi(x) = x^2 + ax + b;$$

on doit avoir

$$|a| < 2\rho, \quad |b| < \rho^2,$$

car a est la somme de deux certaines racines de l'équation $f(x) = 0$, b leur produit.

En posant $x = 0$, on trouve

$$c_n = b\psi(0);$$

donc b est nécessairement diviseur de c_n.

En prenant pour x un nombre entier g, nous obtiendrons

$$f(g) = \varphi(g)\psi(g).$$

Le nombre

$$\varphi(g) = g^2 + ag + b$$

est donc diviseur du nombre $f(g)$.

Pour résoudre le problème, on représente les diviseurs de $f(g)$ sous la forme

$$g^2 + ag + b$$

de toutes les manières possibles, les coefficients a et b devant remplir les conditions indiquées.

En remplaçant g par x, on obtient des fonctions parmi lesquelles sont nécessairement contenus les diviseurs quadratiques de $f(x)$, s'il en existe de tels.

M. Hermite, à qui j'ai communiqué les principes de cette méthode, a bien voulu me faire l'observation suivante :

On peut se demander si, à d'autres points de vue, par exemple au moyen des congruences, en prenant hardiment pour modules divers nombres premiers, on n'arriverait point plus vite au but.

En étudiant la théorie des fonctions irréductibles suivant un module premier, j'ai reconnu tout l'avantage qu'offre la considération des congruences dans la recherche des diviseurs. On connaît le nombre de ces fonctions (Serret, *Algèbre supérieure,* § 349), et il est facile de les former pour les degrés peu élevés.

Par rapport au module 2, il n'y a qu'une seule fonction irréductible du second degré

$$x^2 + x + 1,$$

et deux fonctions du troisième degré

$$x^3 + x^2 + 1, \quad x^3 + x + 1.$$

Pour le module 3, on a trois fonctions du second degré

$$x^2 + 1, \quad x^2 - x - 1, \quad x^2 + x - 1$$

et huit fonctions du troisième degré

$$x^3 - x - 1,\quad x^3 - x + 1,\quad x^3 + x^2 - 1,\quad x^3 - x^2 + 1,$$
$$x^3 - x^2 + x + 1,\quad x^3 + x^2 - x + 1,\quad x^3 - x^2 - x - 1,\quad x^3 + x^2 + x - 1.$$

En divisant la fonction proposée $f(x)$ par ces fonctions, on reconnaît quels sont les diviseurs de $f(x)$ du second et du troisième degré par rapport aux modules 2 et 3.

Si, par exemple,

$$f(x) \equiv (x^2 - x - 1)\psi(x) \pmod{3}$$

et si $f(x)$ n'admet pas d'autres diviseurs suivant le module 3, on conclut que, parmi les fonctions

$$x^2 + ax + b,$$

obtenues par la méthode précédente, on ne doit retenir que celles où

$$a \equiv -1,\quad b \equiv -1 \pmod{3}.$$

Prenons quelques exemples :

1. On recherche les diviseurs de la fonction

$$f(x) = x^5 - 10x^4 - 32x^3 + 7x^2 - 500x - 120.$$

Cette fonction se trouve dans l'Ouvrage de M. Laguerre (*Note sur la résolution des équations numériques,* p. 7; 1880).

En réduisant les coefficients par rapport au module 2, on obtient

$$f(x) \equiv x^2(x^3 + 1) \pmod{2}.$$

La fonction $f(x)$ est modulo 2 divisible par $x + 1$, car

$$f(1) \equiv 0 \pmod{2},$$

d'où

$$f(x) \equiv x^2(x + 1)(x^2 + x + 1) \pmod{2}.$$

Passons au module 3. Les coefficients peuvent être réduits à 0, 1 et -1. On obtient

$$f(x) \equiv x^5 - x^4 + x^2 + x^2 + x \pmod{3}.$$

En remarquant que

$$f(0) \equiv 0,\quad f(1) \equiv 0,\quad f(-1) \equiv 0 \pmod{3},$$

on trouve

$$f(x) \equiv x(x-1)(x+1)(x^2-x-1) \pmod{3}.$$

Prenons encore 5 pour module,

$$\left.\begin{array}{c} f(x) \equiv x^5 - 2x^3 + 2x^2, \\ f(0) \equiv 0, \quad f(1) \equiv 1, \quad f(-1) \equiv -2, \quad f(2) \equiv -2, \quad f(-2) \equiv 2 \end{array}\right\} \pmod{5}.$$

La fonction $f(x)$ n'admet aucun diviseur du premier degré, excepté x suivant le module 5.

On obtient la décomposition en facteurs irréductibles

$$f(x) \equiv x^2(x^3 - 2x + 2) \pmod{5}.$$

Supposons qu'on ait

$$f(x) = \varphi(x)\psi(x), \quad \varphi(x) = x - a,$$

il est nécessaire que

$$a \equiv 0 \pmod{5}.$$

Pour $x = 1$, on trouve

$$f(1) = -2.3.109.$$

Le module des racines de l'équation $f(x) = 0$ étant inférieur à 13,

$$|\varphi(1)| < 14.$$

De la congruence

$$\varphi(x) \equiv x \pmod{5}$$

résulte

$$\varphi(1) \equiv 1 \pmod{5}.$$

On doit avoir

$$\varphi(1) = 1,$$

car $\varphi(1)$ est diviseur de $f(1)$.

Mais

$$\varphi(1) = 1 - a,$$

d'où

$$a = 0,$$

ce qui est impossible, car $f(10)$ est différent de zéro.

La fonction $f(x)$ ne peut donc avoir des diviseurs du premier degré.

Supposons maintenant qu'on ait

$$f(x) = \varphi(x)\psi(x), \quad \varphi(x) = x^2 + ax + b.$$

Comme les modules des racines de l'équation $f(x) = 0$ sont inférieurs à 13, on a

$$|a| < 26, \quad |b| \leq 120,$$

$$\varphi(13) < 13^2 + 26.13 + 120 \quad \text{ou} \quad \varphi(13) < 627.$$

On a encore

$$\varphi(13) > 0,$$

car les racines positives de $f(x) = 0$ sont inférieures à 13.

Le nombre $\varphi(13)$ est diviseur de

$$f(23) = 2.3.1657,$$

et, par conséquent, il ne peut avoir que les valeurs suivantes :

$$\varphi(13) = 1,\ 2,\ 3,\ 6.$$

Il résulte de la relation

$$f(x) \equiv x^2(x^3 - 2x + 2) \pmod 5$$

que

$$\varphi(x) \equiv x^2 \pmod 5$$

et

$$\varphi(13) \equiv \varphi(-2) \equiv -1) \pmod 5).$$

Les nombres 1, 2, 3, 6 ne sont pas congrus — 1 module 6; d'où il suit que la fonction $f(x)$ est irréductible,

$$(2) \qquad f(x) = x^5 - 5x^4 + 21x^3 - 28x^2 + 29x - 70.$$

En effectuant les mêmes calculs, on trouve

$$f(x) \equiv x(x+1)(x^3 + x + 1) \pmod 2,$$
$$f(x) \equiv (x^2+1)(x^3 + x^2 - x + 1) \pmod 3.$$

La fonction $f(x)$ n'a pas de diviseurs du premier degré. Cherchons les diviseurs du second degré

$$\varphi(x) = x^2 + ax + b,$$
$$\rho = 9,$$
$$f(9) = \varphi(9)\psi(9) = 2^6.619.$$
$$\varphi(9) < 9^2 + 18.9 + 70 = 313,$$
$$\psi(9) < 9^3 + 3.9.9^2 + 3.9^2.9 + 70 = 5173,$$

$$313 > \varphi(9) > \tfrac{5173}{313},$$
$$313 > \varphi(9) > 7.$$
$$\varphi(x) \equiv x^2 + x \pmod 2, \quad \varphi(x) \equiv x^2 + 1 \pmod 3,$$
$$\varphi(9) \equiv 0 \pmod 2, \qquad \varphi(9) \equiv 1 \pmod 3,$$
$$\varphi(9) = 16,\ 64.$$

Il faut représenter maintenant ces valeurs de $\varphi(9)$ sous la forme

$$9^2 + 9a + b,$$

que nous désignerons pour abréger par

$$(1,\ a,\ b).$$

Ayant une représentation

$$(1,\ a',\ b'),$$

on obtient toutes les autres en posant

$$a = a' - t, \quad b = b' + 9t,$$

t désignant un nombre entier quelconque.

Les valeurs de a et b doivent remplir les conditions

$$|a| < 18, \quad a \equiv 1 \pmod 2, \quad a \equiv 0 \pmod 3,$$
$$70 \equiv 0 \pmod 6, \quad b \equiv 0 \pmod 2, \quad b = 1 \pmod 3.$$

Les diviseurs pairs de 70 sont

$$2,\ 10,\ 14,\ 70.$$

b peut avoir les valeurs	-2,	10,	-14,	70
Leurs restes module 9.............	-2,	1,	4,	-2

$$16 = (1,\ -9,\ 16),$$
$$b = 16 + 9t = -2,\ 70, \quad t = -2,\ 6,$$
$$a = -9 - t = -7,\ -15,$$
$$\varphi(1) = 1 + a + b = \text{»},\ 2^3.7, \quad f(1) = 2^2, 11.$$

$\varphi(1)$ n'étant pas diviseur de $f(1)$, la valeur

$$\varphi(x) = x^2 - 15x + 70$$

est inadmissible :

$$64 = (1,\ -9,\ 64),$$
$$b = 64 + 9t = 10, \quad t = -6,$$
$$a = -9 - t = -3.$$

On obtient une seule fonction

$$\varphi(x) = x^2 - 3x + 10$$

pouvant être diviseur de $f(x)$. Exécutant la division, on trouve

$$f(x) = (x^2 - 3x - 10)(x^3 - 2x^2 + 5x + 5x + 7).$$

La recherche des diviseurs devient plus simple si l'équation $f(x) = 0$ a des racines égales.

L'application du procédé du plus grand commun diviseur est souvent impraticable à cause des grands coefficients qui apparaissent dans les divisions successives.

Quelques exemples suffisent pour faire voir quels bons services rend dans ce cas la considération des congruences.

3. Soit

$$f(x) = x^7 + x^6 - 5x^5 + 24x^4 - 38x^3 + 53x^2 - 36x + 20.$$

Après avoir reconnu que $f(x)$ n'a pas de diviseurs du premier degré, supposons qu'on ait

$$f(x) = \varphi(x)^2 \psi(x), \quad \varphi(x) = x^2 + ax + b.$$

En prenant 2 pour module, on trouve

$$f(x) \equiv x^7 + x^6 + x^5 + x^4 \pmod 2, \quad f'(x) \equiv x^6 + x^4 \pmod 2,$$

$f'(x)$ étant la dérivée de $f(x)$.

En remarquant que

$$\mathfrak{F}(x^2) \equiv \mathfrak{F}(x)^2 \pmod 2,$$

on a

$$f'(x) \equiv x^2(x+1)^4 \pmod 2.$$

La fonction $f(x)$ est modulo 2 divisible par $x + 1$, car

$$f(1) \equiv 0 \pmod 2.$$

Donc

$$\varphi(x) \equiv x^2 + x \pmod 2.$$

En prenant 3 pour module, on trouve

$$f(x) \equiv x^7 + x^6 + x^5 + x^3 - x^2 - 1, \quad f'(x) \equiv x(x^5 - x^3 + 1) \pmod 3.$$

Cherchons le plus grand commun diviseur des fonctions $f(x)$ et $\frac{1}{x} f'(x)$.

Dans les divisions successives, il convient de remplacer les coefficients par o, 1 et —1. On obtient

$$\varphi(x) \equiv x^2 - x - 1 \pmod{3}.$$

Prenons encore pour module le nombre 11,

$$\left.\begin{aligned} f(x) &\equiv x^7 + x^6 - 5x^5 + 2x^4 - 5x^3 - 2x^2 - 3x - 2 \\ f'(x) &\equiv - 4x^6 - 5x^5 - 3x^4 - 3x^3 - 4x^2 - 4x - 3 \end{aligned}\right\} \pmod{11}.$$

Sans altérer le plus grand commun diviseur des fonctions $f(x)$ et $f'(x)$, on peut multiplier $f'(x)$ par (-3) afin de rendre le coefficient de x^6 égal à 1. On trouve

$$-3f'(x) \equiv x^6 + 4x^5 - 2x^4 - 2x^3 + x^2 + x - 2 \pmod{11}.$$

En effectuant les divisions successives, on obtient le résultat suivant :

$$\varphi(x) \equiv x^2 - x + 2 \pmod{11}.$$

La limite supérieure des racines positives de l'équation $f(x) = 0$, que nous désignerons par r, étant égale à 2,

$$\varphi(2) > 0.$$

Les congruences obtenues permettent de conclure que

$$\varphi(2) \equiv 0 \pmod{2}, \quad \varphi(2) \equiv 1 \pmod{3}, \quad \varphi(2) \equiv 4 \pmod{11}.$$

Mais, comme $\varphi(2)^2$ doit être diviseur de

$$f(2) = 2^4.17,$$

on a

$$\varphi(2) = 4.$$

Ayant une représentation

$$4 = 2^2 = (1, 0, 0),$$

on trouvera toutes les autres

$$4 = 2^2 + 2a + b = (1, a, b)$$

au moyen des formules

$$a = -t, \quad b = 2t,$$

t étant un nombre entier quelconque.

Le nombre b est un diviseur de 20 assujetti aux conditions

$$b \equiv 0 \pmod{2}, \quad b \equiv -1 \pmod{3}, \quad b \equiv 2 \pmod{11}.$$

Les diviseurs pairs de 20 sont........	2,	4,	10,	20
Leurs restes modulo 3...............	−1,	1,	1,	−1
Leurs restes modulo 11.............	2,	4,	−1,	−2

b doit avoir la valeur

$$b = 2,$$

et, par conséquent,

$$t = 1, \quad a = -1.$$

Essayant de prendre

$$\varphi(x) = x^2 - x + 2,$$

on trouve

$$f(x) = (x^2 - x + 2)^2(x^3 + 3x - 4x + 5),$$

$$(4) \qquad f(x) = x^7 + x^6 - 14x^5 + 13x^4 + 57x^3 - 149x^2 + 120x - 25.$$

En effectuant les mêmes calculs, on trouve

$$\varphi(x) \equiv x^2 + 1 \pmod{2}, \quad \varphi(x) \equiv x - x^2 + 1 \pmod{3},$$
$$\varphi(x) \equiv x^2 + 2x \pmod{5},$$
$$r = 4,$$
$$f(5) = 2^2.3^3.5^2.23,$$
$$\varphi(5) \equiv 0 \pmod{2}, \quad \varphi(5) \equiv 0 \pmod{3}, \quad \varphi(5) \equiv 0 \pmod{5},$$
$$\varphi(5) = 30,$$
$$30 = (1, \ -5, \ 30).$$

Les diviseurs de 25 multiples de 5 sont..........	5,	25
Leurs restes modulo 2........................	1,	1
Leurs restes modulo 3........................	−1,	1

$$b = 30 + 5t = -5, \ 25; \quad t = -7, \ -1,$$
$$a = -5 - t = 2, \ -4,$$
$$-4 \text{ n'est pas } \equiv 2 \pmod{5},$$
$$\varphi(x) = x^2 + 2x - 5,$$
$$f(x) = (x^2 + 2x - 5)^2(x^3 - 3x^2 + 4x - 1).$$

En dernier lieu, nous ferons voir que la recherche des diviseurs du troisième degré peut être effectuée de la même manière

$$(5) \qquad f(x) = x^7 - x^6 + 3x^5 + 6x^4 + 2x^3 + 48x^2 - 127x + 35,$$

$$f(x) \equiv x^7 + x^6 + x^5 + x + 1, \quad f'(x) \equiv x^6 + x^4 + 1 \equiv (x^3 + x^2 + 1)^2 \pmod{2}.$$

La fonction $f(x)$ n'a pas de diviseurs linéaires, car les valeurs $f(0)$ et $f(1)$ sont impaires.

La fonction x^3+x^2+1 ne divise pas $f(x)$ suivant le module 2 : donc l'équation $f(x)=0$ n'a pas de racines égales.

En exécutant la division de $x^7+x^6+x^5+x+1$ par x^2+x+1, on reconnaît que $f(x)$ n'a pas des diviseurs du second degré, car il n'y en a pas suivant le module 2.

En divisant $f(x)$ par les fonctions irréductibles du troisième degré suivant le module 2 (p. 5), on trouve

$$f(x) \equiv (x^3+x+1)(x^4+x^3+1) \pmod 2.$$

Prenons le nombre 3 pour module

$$f(x) \equiv x^7 - x^6 - x^3 - x - 1 \pmod 3.$$

Cherchons d'abord les diviseurs du premier degré. On trouve

$$f(x) \equiv (x-1)^3(x^4-x^3+x+1) \pmod 3.$$

Mais

$$(x-1)^3 \equiv x^3-1 \pmod 3,$$

d'où il suit

$$f(x) \equiv (x^3-1)(x^4-x^3+x+1).$$

La fonction x^4-x^3+x+1 est irréductible suivant le module 3, comme il est facile de s'en convaincre (p. 5).

Supposons maintenant qu'on ait

$$f(x) = \varphi(x)\psi(x), \quad \varphi(x) = x^3+ax^2+bx+c.$$

La limite supérieure des modules des racines étant 4,

$$|a| < 12, \quad |b| < 48.$$

Nous savons encore que

$$\varphi(x) \equiv x^3+x+1 \pmod 2, \quad \varphi(x) \equiv x^3-1 \pmod 3.$$

La limite supérieure des racines positives est égale à 2, d'où il suit

$$\varphi(3) > 0.$$

Il résulte de nos congruences

$$\varphi(3) \equiv 1 \pmod 2, \quad \varphi(3) \equiv -1 \pmod 3.$$

Le nombre $\varphi(3)$ est diviseur de

$$f(3) = 2813 = 29.97,$$
$$\varphi(3) < 3^3 + 12.3^2 + 48.3 + 35 = 314,$$
$$\psi(3) < 3^4 + 4.4.3^3 + 6.4^2.3^2 + 4.4^3 3 + 35 = 1988,$$
$$\varphi(3) > \tfrac{2813}{1988} \text{ ou } \varphi(3) > 1.$$

Donc $\varphi(3)$ doit être un diviseur impair de $f(3)$ compris entre 1 et 314 congru à -1 module 3. On conclut

$$\varphi(3) = 29.$$

Ce nombre doit être mis sous la forme

$$3^3 + 3^2 a + 3b + c = (1, a, b, c).$$

Supposons qu'on ait

$$(1, a, b, c) = (1, a', b', c'),$$

on trouve

$$c = c' + 3t_1, \quad b = b' - t_1 + 3t_2, \quad a = a' - t_2,$$

t_1 et t_2 étant des nombres entiers quelconques.

Le nombre c doit être diviseur de 35 vérifiant les congruences

$$c \equiv 1 \pmod 2), \quad c \equiv -1 \pmod 3).$$

Les diviseurs de 35 sont..............	1,	5,	7,	35
Leurs restes module 3.................	1,	-1,	1,	-1

Le nombre c peut donc avoir les valeurs

$$c = -1,\ 5,\ -7,\ 35.$$

De la représentation

$$29 = (1, -3, 7, 8)$$

on déduit

$$c = 8 + 3t_1 = -1,\ 5,\ -7,\ 35; \quad t_1 = -3,\ -1,\ -5,\ 9,$$
$$b = \quad 7 - t_1 + 3t_2 = 10 + 3t_2, \quad 8 + 3t_2, \quad 12 + 3t_3, \quad -2 + 3t_2,$$
$$a = -3 - t_2.$$

Les valeurs de a et b sont assujetties aux conditions

$$b \equiv 1, \quad a \equiv 0 \pmod 2),$$
$$b \equiv 0, \quad a \equiv 0 \pmod 3),$$

La valeur de b étant multiple de 3, on a

$$b = 12 + 3t_2, \quad c = -7,$$

Pour que b soit impair, il faut que t_2 le soit aussi. Posons

$$t_2 = 2u + 1,$$

on aura

$$b = 15 + 6u, \quad a = -4 - 2u.$$

De la relation

$$a \equiv 0 \pmod 3) \quad \text{ou} \quad -4 - 2u \equiv 0 \pmod 3)$$

résulte

$$u \equiv 1 \pmod 3), \quad u = 1 + 3v,$$
$$b = 21 + 18v, \quad a = -6 - 6v.$$

Pour

$$\begin{array}{lrrrrr}
v = & 0, & 1, & -1, & -2, & -3, \\
a = & -6, & -12, & 0, & 6, & 12, \\
b = & 21, & 39, & 3, & -15, & 33, \\
c = & -7, & -7, & -7, & -7, & -7,
\end{array}$$

$$\begin{array}{lllllll}
\varphi(1) = 1 + a + b + c = & 9, & 21, & -3, & -15, & 38; & f(1) = -3.11 \\
-\varphi(-1) = 1 - a + b - c = & », & », & 11, & », & »; & f(-1) = 11.19
\end{array}$$

On n'obtient qu'une seule fonction

$$\varphi(x) = x^3 + 3x - 7,$$

qui est en réalité diviseur de $f(x)$

$$f(x) = (x^3 + 3x - 7)(x^4 - x^3 + 16x - 5).$$

Pour décomposer les nombres en facteurs premiers, nous nous sommes servi d'une Table contenue dans le Recueil de M. Hoüel (*Tables de logarithmes*, etc., Table VII, p. 116).

Dans les exemples compliqués, il est nécessaire de recourir aux grandes Tables des diviseurs de Burckhard (jusqu'à 3 036 000).