João Filipe Queiró
Universidade de Coimbra
jfqueiro@mat.uc.pt

DO ALGORITMO DE EUCLIDES AO TEOREMA DE QUILLEN-SUSLIN

Uma viagem iniciada no Livro VII dos *Elementos* de Euclides que vai até ao final do século XX.

1. INTRODUÇÃO

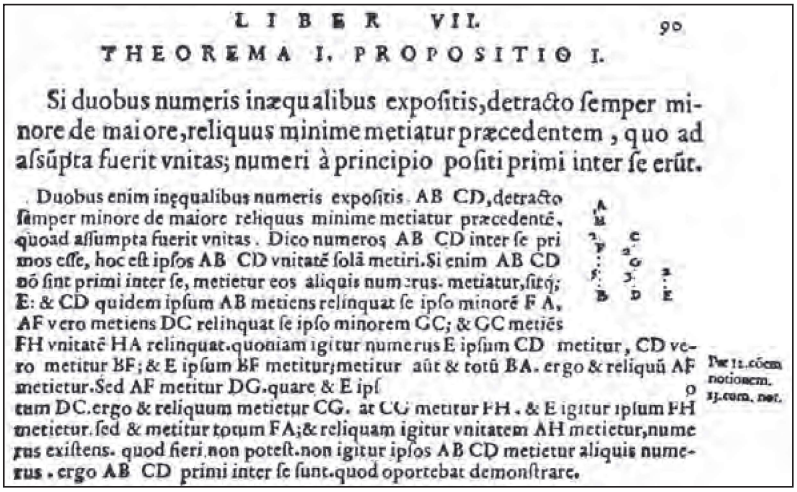
O 7.º Livro dos *Elementos* de Euclides, o primeiro dos livros aritméticos da obra, trata das questões de divisibilidade para números naturais. Depois de 22 definições básicas (incluindo número divisor de outro e múltiplo de outro, número primo e números primos entre si), a 1.ª Proposição afirma o seguinte:

> Dados dois números diferentes, sendo subtraído o menor do maior e sucessivamente repetido esse processo, se o número que resta nunca dividir o anterior até que reste 1, os números originais são primos entre si.

O que isto quer dizer, em símbolos dos nossos dias, é o seguinte: sejam a e b dois números naturais diferentes. Sem perda de generalidade, podemos supor $a > b$. Proceda-se à seguinte sequência de divisões inteiras:

$$\begin{aligned} a &= q_1 b + r_1\,, \quad 0 < r_1 < b \\ b &= q_2 r_1 + r_2\,, \quad 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3\,, \quad 0 < r_3 < r_2 \\ &\vdots \\ r_{k-2} &= q_k r_{k-1} + 1\,. \end{aligned}$$

Então a e b são primos entre si.



LIBER VII. 90

THEOREMA I. PROPOSITIO I.

Si duobus numeris inæqualibus expoſitis, detracto ſemper minore de maiore, reliquus minime metiatur præcedentem, quo ad aſſũpta fuerit vnitas; numeri à principio poſiti primi inter ſe erũt.

Duobus enim inæqualibus numeris expoſitis AB CD, detracto ſemper minore de maiore reliquus minime metiatur præcedentẽ, quoad aſſumpta fuerit vnitas. Dico numeros AB CD inter ſe primos eſſe, hoc eſt ipſos AB CD vnitatẽ ſolã metiri. Si enim AB CD nõ ſint primi inter ſe, metietur eos aliquis numerus. metiatur, ſitq; E: & CD quidem ipſum AB metiens relinquat ſe ipſo minorẽ FA, AF vero metiens DC relinquat ſe ipſo minorem GC; & GC metiẽs FH vnitatẽ HA relinquat. quoniam igitur numerus E ipſum CD metitur, CD vero metitur BF; & E ipſum BF metitur; metitur aũt & totũ BA. ergo & reliquũ AF metietur. Sed AF metitur DG. quare & E ipſum DC. ergo & reliquum metietur CG. at CG metitur FH. & E igitur ipſum FH metietur. ſed & metitur totum FA; & reliquam igitur vnitatem AH metietur, numerus exiſtens. quod fieri non poteſt. non igitur ipſos AB CD metietur aliquis numerus. ergo AB CD primi inter ſe ſunt. quod oportebat demonſtrare.

Figura 1. A 1.ª Proposição do 7.º Livro dos *Elementos* de Euclides, na famosa edição latina de Commandino [3].

Para provar esta afirmação, Euclides argumenta assim: se a e b não fossem primos entre si, existiria um divisor comum de a e b, digamos d, maior do que 1. Da primeira das igualdades acima concluímos que d divide o primeiro resto r_1. Da segunda concluímos então que d divide r_2. E assim sucessivamente, até concluirmos que d divide 1, o que é impossível. Logo, nenhum número maior do que 1 divide a e b e, portanto, estes números são primos entre si.

A 2.ª Proposição tem, como muitas outras nos *Elementos*, a forma de um problema:

> *Dados dois números não primos entre si, encontrar o maior dos seus divisores comuns.*

A resolução usa um procedimento análogo ao utilizado para provar a 1.ª Proposição. Sejam a e b dois números não primos entre si. Se b dividir a, é um divisor comum de ambos e é manifestamente o maior dos divisores comuns. Se b não dividir a, proceda-se à seguinte sequência de divisões inteiras:

$$\begin{aligned} a &= q_1 b + r_1\,, \quad 0 < r_1 < b \\ b &= q_2 r_1 + r_2\,, \quad 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3\,, \quad 0 < r_3 < r_2 \\ &\vdots \end{aligned}$$

Repetindo este processo, chegar-se-á a um número que divide o anterior, isto é, a uma divisão com resto 0:

$$\begin{aligned} &\vdots \\ r_{k-2} &= q_k r_{k-1} + r_k\,, \quad 0 < r_k < r_{k-1} \\ r_{k-1} &= q_{k+1} r_k\,. \end{aligned}$$

Isto porque não se pode chegar a um resto igual a 1, pois nesse caso, pela 1.ª Proposição, a e b seriam primos entre si, contra a hipótese. Por outro lado, os restos não podem permanecer sempre positivos, porque cada um é menor do que o anterior.

Euclides afirma que r_k (o último resto não nulo) é o maior dos divisores comuns de a e b.

Por um lado, r_k é um divisor comum de a e b: da última igualdade vemos que divide r_{k-1}; da penúltima concluímos então que divide r_{k-2}; e assim sucessivamente até às primeiras igualdades, que permitem concluir que r_k divide a e b.

Por outro lado, r_k é o maior dos divisores comuns de a e b: se não fosse, existiria um divisor comum de a e b, digamos g, maior do que r_k. Da primeira igualdade concluímos que g divide r_1; da segunda, que g divide r_2; e assim sucessivamente, até concluirmos que g divide r_k, o que não pode ser, pois g é maior que r_k.

A este procedimento para encontrar o maior divisor comum chama-se "algoritmo de Euclides".

Na 3.ª Proposição, Euclides resolve o mesmo problema para três números, ficando claro que a técnica utilizada permite achar o maior divisor comum de quantos números se quiser.

Deixemos os *Elementos* e venhamos para os nossos dias. É óbvio que a noção de maior divisor comum pode ser apresentada para quaisquer inteiros a e b não ambos nulos. Usamos a notação mdc (a, b), e analogamente para mais do que dois números. Registemos algumas propriedades simples:

- mdc $(a, 0) = |a|$,
- mdc(a, b) = mdc(b, a) = mdc (a, -b),
- mdc $(a_1, a_2, \ldots, a_n)$ = mdc [mdc$(a_1, a_2, \ldots, a_{n-1}), a_n$].

Uma consequência interessante do algoritmo de Euclides é a seguinte:

Teorema. *Sejam a e b inteiros não ambos nulos e seja d o seu maior divisor comum. Então existem inteiros x e y tais que $d = ax + by$.*

Demonstração. Podemos supor a e b positivos. Olhemos para as igualdades que escrevemos a propósito da 2.ª Proposição dos *Elementos*. Da penúltima tiramos

$$r_k = r_{k-2} - q_k r_{k-1}\,.$$

Da antepenúltima sai então que

$$r_k = -q_k r_{k-3} + (1 + q_k q_{k-1}) r_{k-2}\,.$$

Prosseguindo deste modo, chegamos a uma igualdade da forma $r_k = ax + by$.

Exemplo. Sejam $a = 399$ e $b = 168$. Tem-se

$$\begin{aligned} 399 &= 2 \times 168 + 63 \\ 168 &= 2 \times 63 + 42 \\ 63 &= 1 \times 42 + 21 \\ 42 &= 2 \times 21. \end{aligned}$$

Logo, mdc (399, 168) = 21. Usando os cálculos feitos, tem-se

$$\begin{aligned} 21 &= 63 - 42 \\ &= 63 - (168 - 63 \times 2) \\ &= 63 \times 3 - 168 \\ &= (399 - 168 \times 2) \times 3 - 168 \\ &= 399 \times 3 - 168 \times 7. \end{aligned}$$

É óbvia a generalização deste resultado para mais do que dois inteiros.

O Teorema que acabámos de descrever costuma ser associado ao nome de Étienne Bézout (1730-1783). De facto, Bézout provou-o não para inteiros mas para polinómios numa variável [1], cuja teoria de divisibilidade é totalmente análoga à dos inteiros. Voltaremos a este assunto adiante.

E aqui chegamos ao tema principal deste artigo.

Da Álgebra Linear elementar recordamos que, dada uma matriz quadrada A e sendo adj(A) a sua adjunta, vale a igualdade

$$A \cdot \text{adj}(A) = \det(A) \cdot I,$$

onde I é a matriz identidade. Daqui sai imediatamente que A é invertível se e só se $\det(A) \neq 0$.

Suponhamos agora que só nos interessam matrizes inteiras, isto é, matrizes cujos elementos são números inteiros. A igualdade acima continua a ser verdadeira e, se A for inteira, adj (A) também é e det(A) é obviamente um número inteiro. Mas agora a condição $\det(A) \neq 0$ já não garante a invertibilidade de A, isto é, que A^{-1} seja também inteira. De facto, tem-se:

Teorema. *Uma matriz inteira A é invertível (mantendo-nos dentro dos inteiros) se e só se det(A) for um inteiro invertível, isto é, se e só se* $\det(A) = 1$ *ou* $\det(A) = -1$.

Demonstração. A suficiência é óbvia. Para provar a necessidade, suponhamos que A é invertível. Então A^{-1} é inteira e, portanto, $\det(A^{-1})$ é um número inteiro. Mas $\det(A^{-1}) = \frac{1}{\det(A)}$, que só é inteiro se $\det(A) = 1$ ou $\det(A) = -1$.

Vamos finalmente ao problema que nos interessa. Só trabalhamos com matrizes inteiras. Sejam dados dois inteiros a e b quaisquer. Coloquemo-los na primeira linha de uma matriz 2×2:

$$\begin{bmatrix} a & b \\ * & * \end{bmatrix}.$$

A pergunta é: quando é que podemos encontrar dois inteiros, a colocar nas posições indicadas com *, de forma a obter uma matriz invertível?

A resposta segue de afirmações que já fizemos: tal é possível se e só se a e b forem primos entre si, isto é, se mdc (a, b) = 1. De facto, se a e b forem primos entre si, existem inteiros x e y tais que $ax + by = 1$. Então o determinante da matriz

$$\begin{bmatrix} a & b \\ -y & x \end{bmatrix}$$

é igual a 1 e portanto esta matriz é invertível.

Reciprocamente, se for possível completar a linha $[a\ b]$ a uma matriz 2×2 invertível, a e b têm de ser primos entre si: se não fossem, isto é, se tivessem um divisor comum $d > 1$, então essa matriz 2×2 teria o determinante múltiplo de d e portanto não seria invertível.

Exemplo. Como $399 \times 3 - 168 \times 7 = 21$, tem-se $19 \times 3 - 8 \times 7 = 1$ e, portanto, 19 e 8 são primos entre si. A matriz

$$\begin{bmatrix} 19 & 8 \\ 7 & 3 \end{bmatrix}$$

tem determinante 1 e, logo, é invertível. A sua inversa é

$$\begin{bmatrix} 3 & -8 \\ -7 & 19 \end{bmatrix}.$$

Temos assim o Teorema de Bézout – consequência directa do algoritmo de Euclides – reinterpretado como uma afirmação sobre matrizes inteiras: a resposta à questão do completamento a uma matriz invertível de uma linha cujos elementos são primos entre si.

A mesma questão de completamento pode colocar-se para matrizes $n \times n$, com n qualquer, e para linhas arbitrárias. Concretamente, tem-se o seguinte resultado [4]:

Teorema. *Seja n um número natural ≥ 2. Sejam $a_1, a_2, \ldots, a_n$ inteiros quaisquer e seja d o seu maior divisor comum. Então existe uma matriz inteira cuja primeira linha é $[a_1\ a_2\ \ldots\ a_n]$ e cujo determinante é d.*

Demonstração do Teorema. O raciocínio é feito por indução sobre n. O caso $n = 2$ é trivial, sendo consequência imediata da observação feita acima. Suponhamos a afirmação verdadeira para n - 1.

Seja A_1 uma matriz $(n-1) \times (n-1)$ com primeira linha $[a_1\ a_2\ \ldots\ a_{n-1}]$ e determinante $d_1 = \text{mdc}(a_1, a_2, \ldots, a_{n-1})$.

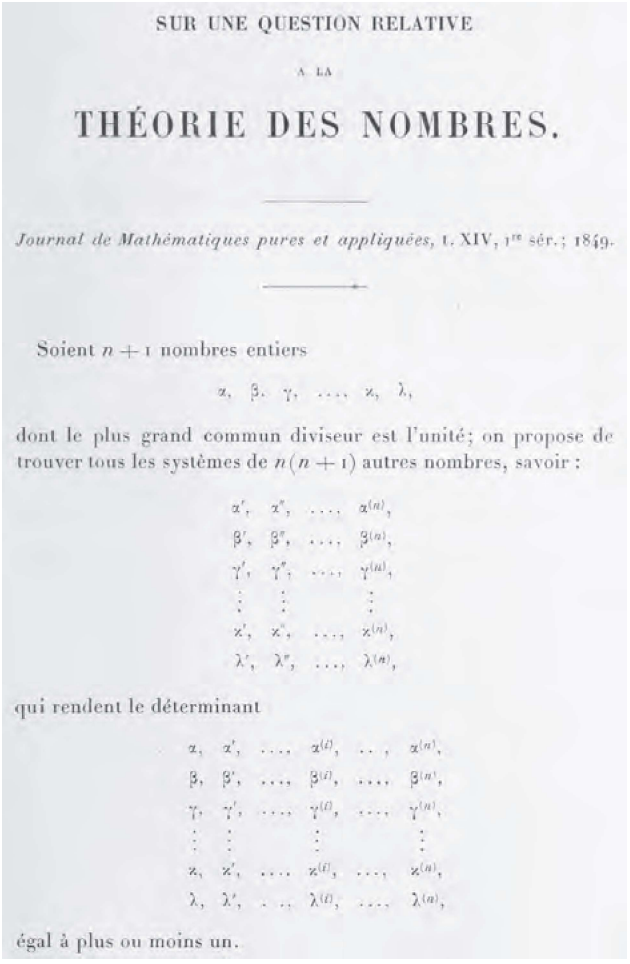
Como $d = \text{mdc}(d_1, a_n)$, existem inteiros x e y tais que $d_1 x + a_n y = d$. Ponhamos

$$A = \begin{bmatrix} & & & a_n \\ & A_1 & & 0 \\ & & & \vdots \\ & & & 0 \\ -\frac{a_1 y}{d_1} & \cdots & -\frac{a_{n-1} y}{d_1} & x \end{bmatrix}.$$

Então A é uma matriz $n \times n$ inteira e a sua primeira linha é $[a_1\ a_2\ \ldots\ a_n]$. Se aplicarmos o Teorema de Laplace à última coluna de A, vemos que $\det(A) = d$, como desejado.

Corolário. *Sejam $a_1, a_2, \ldots, a_n$ inteiros primos entre si. Então existe uma matriz inteira invertível cuja primeira linha é $[a_1\ a_2\ \ldots\ a_n]$.*

Todas as afirmações feitas até aqui sobre números inteiros permanecem válidas, com as adaptações óbvias, para o conjunto $\mathbb{K}[t]$ dos polinómios numa variável t com coeficientes num corpo $\mathbb{K}$. A observação crucial para esse efeito é que existe, para polinómios, um algoritmo de divisão análogo ao dos inteiros, com a adaptação de que, numa divisão de polinómios, o grau do polinómio resto é inferior ao grau do polinómio divisor.[1]



SUR UNE QUESTION RELATIVE

A LA

THÉORIE DES NOMBRES.

Journal de Mathématiques pures et appliquées, t. XIV, 1re sér.; 1849.

Soient $n+1$ nombres entiers

$$\alpha,\ \beta,\ \gamma,\ \ldots,\ \varkappa,\ \lambda,$$

dont le plus grand commun diviseur est l'unité; on propose de trouver tous les systèmes de $n(n+1)$ autres nombres, savoir :

$$\begin{array}{ccccc} \alpha', & \alpha'', & \ldots, & \alpha^{(n)}, \\ \beta', & \beta'', & \ldots, & \beta^{(n)}, \\ \gamma', & \gamma'', & \ldots, & \gamma^{(n)}, \\ \vdots & \vdots & & \vdots \\ \varkappa', & \varkappa'', & \ldots, & \varkappa^{(n)}, \\ \lambda', & \lambda'', & \ldots, & \lambda^{(n)}, \end{array}$$

qui rendent le déterminant

$$\begin{array}{ccccccc} \alpha, & \alpha', & \ldots, & \alpha^{(i)}, & \ldots, & \alpha^{(n)}, \\ \beta, & \beta', & \ldots, & \beta^{(i)}, & \ldots, & \beta^{(n)}, \\ \gamma, & \gamma', & \ldots, & \gamma^{(i)}, & \ldots, & \gamma^{(n)}, \\ \vdots & \vdots & & \vdots & & \vdots \\ \varkappa, & \varkappa', & \ldots, & \varkappa^{(i)}, & \ldots, & \varkappa^{(n)}, \\ \lambda, & \lambda', & \ldots, & \lambda^{(i)}, & \ldots, & \lambda^{(n)}, \end{array}$$

égal à plus ou moins un.

Figura 2. Primeira página de [4].

Quanto à afirmação sobre as matrizes invertíveis, ela muda apenas na identificação dos polinómios que têm inverso multiplicativo, que são obviamente os polinómios não nulos de grau 0 (isto é, constantes).

Mas podemos ir ainda mais longe. Se analisarmos a demonstração do último teorema, vemos que, na realidade, para o provarmos não precisamos directamente do algoritmo de Euclides, mas apenas do Teorema de Bézout, isto é, da possibilidade de exprimir o máximo divisor comum dos elementos $a_1, a_2, \ldots, a_n$ (inteiros ou polinómios) na forma $a_1x_1 + a_2x_2 + \cdots + a_nx_n$.

Esta observação sugere que o teorema de completamento permanece válido se trabalharmos com matrizes cujos elementos pertençam a um anel onde seja válido o Teorema de Bézout. Isso é garantido, por exemplo, na classe dos chamados "domínios de ideais principais". Como o nome indica, trata-se de domínios de integridade onde todos os ideais são principais, isto é, são gerados por um único elemento. Se pensarmos em elementos $a_1, a_2, \ldots, a_n$ não todos nulos num tal anel, o ideal que eles geram é necessariamente principal. É simples ver que um gerador d desse ideal pode escrever-se na forma $a_1x_1 + a_2x_2 + \cdots + a_nx_n$ e é um máximo divisor comum dos elementos $a_1, a_2, \ldots, a_n$. (Notem-se os artigos indefinidos antes de "gerador" e de "máximo divisor comum"; de facto, neste contexto geral, deixa de haver unicidade, o que de resto já acontecia no caso dos polinómios.)

E para anéis mais gerais, em que o Teorema de Bézout pode falhar? Aqui tudo fica mais difícil. Em 1957, Jean-Pierre Serre, medalha Fields em 1954, conjecturou [7], na linguagem dos módulos, que as coisas se mantêm para anéis de polinómios $\mathbb{K}[t_1, t_2, \ldots, t_s]$ em qualquer número s de variáveis[2] com coeficientes num corpo $\mathbb{K}$. A conjectura de Serre era a de que, se tivermos elementos $a_1, a_2, \ldots, a_n$ primos entre si num tal anel, existe uma matriz invertível no anel com primeira linha $[a_1\ a_2\ \ldots\ a_n]$.

A conjectura de Serre veio a ser provada em 1976, independentemente, por Daniel Quillen, medalha Fields em 1978 [6], e Andrei Suslin [8]. Uma demonstração simplificada, cabendo em poucas páginas, pode ser encontrada na 3.ª edição do livro *Algebra*, de Serge Lang [5].

Problemas de completamento a matrizes invertíveis sobre variados tipos de anéis são analisados em [2].

Agradeço a Thomas J. Laffey a indicação da referência [5].

REFERÊNCIAS

[1] Étienne Bézout, *Théorie Générale des Équations Algébriques*, Paris, Ph.-D. Pierres, 1779.

[2] M. Graça Duffner e Fernando C. Silva, "On the Existence of Unimodular Matrices with a Prescribed Submatrix", *Linear Algebra Appl.* 515 (2017), 321-330.

[3] *Euclidis Elementorum libri XV*, tradução latina de Federico Commandino, Pesaro, Jacobus Chriegher, 1572.

[4] Charles Hermite, Sur une Question Relative à la Théorie des Nombres, *Journal de Mathématiques Pures et Appliquées* 14 (1849), 21-30.

[5] Serge Lang, *Algebra*, 3.ª edição, Reading, Addison-Wesley, 1993.

[6] Daniel Quillen, "Projective Modules over Polynomial Rings", *Invent. Math.* 36 (1976), 167-171.

[7] Jean-Pierre Serre, *Modules Projectifs et Espaces Fibrés à Fibre Vectorielle*, Paris, Séminaire P. Dubreil, M.-L. Dubreil-Jacotin et C. Pisot, Fasc. 2, Exposé 23 (1957/58), 18 pp.

[8] Andrei Suslin, "Projective Modules over Polynomial Rings are Free", *Soviet Math. Dokl.* 17 (1976), 1160-1164.

[1] Tendo em vista esta mudança de contexto, é habitual dizer "máximo divisor comum" em vez de "maior", e defini-lo como um divisor comum que é múltiplo de qualquer outro divisor comum.

[2] Para $s > 1$, estes anéis já não são de ideais principais. Por exemplo, em $\mathbb{K}[t_1, t_2]$ o ideal gerado por t_1 e t_2 não é principal e o Teorema de Bézout falha.