Construções Geométricas

Owen Brison
Departamento de Matemática da Faculdade de Ciências da Universidade de Lisboa

1. Introdução

Os matemáticos da Antiga Grécia procuraram exaustivamente construções geométricas, apenas com régua não graduada e compasso, para a **trissecção do ângulo**, a **duplicação do cubo**[1] e a **quadratura do círculo**[2]. Não as encontraram, apesar de terem descoberto outras maneiras de as realizar. Ao longo de dois mil anos sucederam-se tentativas infrutíferas de muitos matemáticos e, finalmente no século XIX, foi demonstrado que nenhuma dessas três construções é possível; a demonstração é um exemplo muito bem sucedido de "transferência de tecnologia": os problemas são transformados, através da Geometria Analítica, em problemas sobre números reais ou números complexos, sendo estes problemas resolvidos recorrendo à Álgebra e à Análise Matemática.

O facto de um problema ter resistido durante tanto tempo e vir a ser resolvido com instrumentos de uma área aparentemente fora do contexto em que foi posto parece-nos uma lição importante sobre a maneira como a Matemática funciona.

Não é nosso propósito tratar aqui a Geometria Euclidiana ou a história destes problemas com todo o rigor, mas tão só sublinhar a maneira como a Álgebra "abstracta" do Século XIX, ajudou a resolver problemas que tinham ficado em aberto desde os dias de Euclides. Assim, no que respeita a demonstrações, remetemos o leitor para a bibliografia excepto em alguns casos que nos parecem menos técnicos e facilmente acessíveis a eventuais leitores pré-universitários.

Na secção 2 esboçamos a parte principal do que convencionámos designar por "transferência de tecnologia"; nas secções 3 e 4 tratamos os dois primeiros problemas: os teoremas 3.1 e 4.1 são frequentemente atribuídos a P.L. Wantzel; na secção 6 esboçamos o estudo da construtibilidade de polígonos regulares destacando a do heptadecágono; para esta secção pressupomos que o leitor está familiarizado com a notação exponencial para a forma polar dos números complexos.

Um tratamento completo e cuidado do tema deste artigo pode encontrar-se no elegante livro de Hadlock [HC], no qual nos inspirámos fortemente.

2. Algebrização

Como Conway e Guy observam no Capítulo 7 de [CG], a Geometria Euclidiana pode ser encarada como um passatempo com regras fixas; passemos a identificar as que nos interessam. A tese [FR] dá uma visão muito interessante de vários sistemas alternativos de regras.

Supomos conhecidos os termos da geometria euclidiana elementar, como "ponto", "recta", "circunferência", "ân-

[1] i.e., a construção da aresta de um cubo com volume duplo de um cubo dado.

[2] i.e., a construção da aresta de um quadrado com área igual à de um círculo dado.

gulo", etc. referentes a entidades do plano euclidiano, designado por $\mathbb{E}$.

2.1 Construções primitivas

Qualquer construção se inicia com, pelo menos, dois pontos distintos, a uma distância que se fixa como unidade.

Seja *P* um conjunto com pelo menos dois pontos distintos em $\mathbb{E}$. Consideremos as construções seguintes:

Construção R. (Régua) Dados pontos distintos *A* e *B* em *P*, construir uma recta que passe por A e B.

Construção C. (Compasso) Dados pontos distintos *C* e *A* em *P*, construir uma circunferência com centro *C* que passe por *A*.

Qualquer recta fica construída quando construímos dois quaisquer pontos distintos que lhe pertençam. O ponto *P* está construído quando construímos duas rectas distintas cuja intersecção é *P*, ou uma recta e uma circunferência ou duas circunferências distintas cuja intersecção contém *P*.

Resulta das Proposições 2 e 3, do Livro I dos Elementos de Euclides, que a construção seguinte pode ser realizada utilizando as Operações R e C:

Construção C´. (Compasso) Construir uma circunferência com centro em *P* cujo raio seja igual à distância entre dois pontos distintos de *P*.

Essencialmente, a construção **C´** permite a utilização do compasso para "transferir" uma distância já definida.

Daqui em diante, suporemos que as *construções primitivas* são **R** e **C´**.

2.2 Outras construções

Como se sabe, sequências convenientes das construções primitivas permitem realizar as seguintes:

(1) Dada uma recta *l* e um ponto *P* de *l*, construir uma recta perpendicular a *l* que passe por *P*; em particular, construir ângulos rectos.

(2) Dada uma recta *l* e um ponto *P* fora de *l*, construir uma paralela e outra perpendicular a *l* que passem por *P*.

(3) Construir um segmento de recta com *n* unidades inteiras de comprimento.

(4) Dados segmentos de recta com *a* e *b* unidades de comprimento, construir segmentos de recta com comprimento $a+b$ ou, se $a \geq b$, $a-b$ unidades.

(5) Dados segmentos de recta com *a* e *b* unidades de comprimento e sendo $b \neq 0$, construir segmentos de recta com comprimentos *ab* e a/b unidades.

(6) Dado um segmento de recta com $a\,(>0)$ unidades de comprimento, construir um segmento de recta com comprimento $\sqrt{a}$ unidades.

(7) Construir ângulos de 60º e 72º; em particular, construir triângulos equiláteros bem como pentágonos regulares.

(8) Dado um ângulo de medida α e números naturais *k* e *n*, construir ângulos de medidas $\alpha/2^k, 2\alpha, \ldots, n\alpha$; em particular, construir ângulos de medida 45º.

Em geral, uma construção será uma sequência conveniente de repetições das construções primitivas **R** e **C´**. A definição seguinte formaliza esta ideia.

Definição 2.1. *Seja S um conjunto de pontos do plano* $\mathbb{E}$.

1. Se duas rectas distintas ou duas circunferências distintas ou uma recta e uma circunferência são construtíveis por R ou C´ a partir de pontos de S, as intersecções correspondentes (quando não vazias) dizem-se ***construtíveis numa etapa a partir de S****.*

2. Se S tiver mais que um ponto, diz-se que um ponto $Q \in \mathbb{E}$ *é* ***construtível a partir de S*** *quando existe um número natural n e uma sequência* $Q_1, \ldots, Q_n$ *de pontos de* $\mathbb{E}$ *tais que*

$$Q_n = Q$$

e, se para cada i=1, ..., n, definindo

$$P_0 = S,$$

$$P_{i-1} = P_0 \cup \{Q_1, \ldots, Q_{i-1}\},$$

o ponto Q_i *é construtível numa etapa a partir de* P_{i-1}.

Podemos iniciar a "transferência de tecnologia".

2.3 O plano Cartesiano

Começamos por identificar o plano **E** com o quadrado cartesiano do conjunto dos números reais, R^2, mediante a fixação de um sistema de dois eixos ortonormais.

Sabemos da geometria elementar que, dados pontos (a,0), (b,0), é possível construir cada um dos pontos (a+b, 0) e (a–b,0), numa etapa, e (ab,0) (ou (a/b,0) se $b \neq 0$) em mais etapas, recorrendo ao teorema de Thales. Em suma,

Seja qual for o número racional q, é possível construir o ponto (q,0), a partir de {(0,0),(1,0)}.

É também possível construir certos pontos cujas coordenadas não são racionais; por exemplo, o ponto $\left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right)$ é um dos pontos de intersecção da circunferência $x^2 + y^2 = 1$ com a recta de equação $x = y$, sendo a circunferência e a recta ambas construtíveis a partir de {(0,0),(1,0)}; em seguida, podemos construir $(\sqrt{2}, 0)$. Em geral,

Dado um ponto (a,0), *sendo a real e positivo, podemos construir o ponto* $(\sqrt{a}, 0)$.

Passamos à segunda fase de "transferência".

2.4 Extensões do corpo dos números racionais

A identificação de **E** com R^2 permite então traduzir os problemas geométricos de que nos estamos a ocupar em termos de números reais[3].

Representamos respectivamente por Q e R os corpos dos números racionais e dos números reais. Um **subcorpo** de R será um seu subconjunto K, diferente de {0} e fechado para a soma, a diferença e o quociente por números não-nulos; escreveremos $K \subseteq L$ para abreviar K é *subcorpo do subcorpo* L, i.e., K e L são subcorpos de IR e $K \subseteq L$. Observe-se que, não só Q é subcorpo de R como também, se $K \subseteq L$, necessariamente $1 \in K$ e, consequentemente, $2 = 1 + 1 \in K$, $3 \in K$, ...; daí também $-2, -3, \ldots \in K$ e $\pm\frac{1}{2}, \pm\frac{1}{3}, \ldots \in K$ e finalmente, $\frac{m}{n} \in K$ sempre que m, n são números inteiros e $n \neq 0$. Assim

$Q \subseteq K$ sempre que $K \subseteq R$.

Se $K \subseteq L \subseteq R$, diremos que L é uma **extensão** de K.

Uma forma bastante simples de obter extensões próprias de um subcorpo K é tomar um número real r que não esteja em K e formar o corpo mínimo que contém $K \cup \{r\}$; por exemplo, tal corpo no caso $Q \cup \{\sqrt{2}\}$ é $\{p + q\sqrt{2},\ p, q \in Q\}$.

De um modo geral, se $C \subseteq R$, o **subcorpo gerado por** C é por definição, um subcorpo de R designado por < C > tal que $C \subseteq < C >$ e, se $K \subseteq R$ e $C \subseteq K$, então $< C > \subseteq K$. Para cada $r \in R$ e cada $K \subseteq R$ põe-se

$$K(r) := < K \cup \{r\} >$$

e, se $r = \sqrt{k}$ para algum $k \in K$, diz-se que K(r), ou seja $K(\sqrt{k})$ é **extensão quadrática** de K.

Se $K \subseteq L$, então L é espaço vectorial sobre K sendo fácil provar o seguinte.

Lema 2.1: *Se* $K \subseteq L$ *e* $k \in K$ *mas* $\sqrt{k} \notin K$, *então*

$$K(\sqrt{k}) = \left\{u + v\sqrt{k} : u, v \in K\right\},$$

$\left\{1, \sqrt{k}\right\}$ *é uma base de* $K(\sqrt{k})$ *sobre K, pelo que a dimensão de* $K(\sqrt{k})$ *sobre K é 2.*

Recorde-se agora que as construções primitivas se tra-

[3] Veremos na secção 6 que, em alguns casos, pode ser preferível utilizar o corpo dos números complexos.

duzem no presente contexto por resoluções de sucessivos sistemas de equações lineares ou polinómios do segundo grau com coeficientes reais e, assim sendo, o mesmo se passa com as outras construções. Interessa-nos um caso particular de extensões:

Definição 2.2. *Se* $\mathbb{Q} \subseteq K \subseteq L \subseteq \mathbb{R}$, *L diz-se uma extensão* ***multi-quadrática*** *de K se, para algum número natural n existe uma cadeia de subcorpos*

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_i \subseteq K_{i+1} \subseteq \ldots \subseteq K_n = L$$

tal que $K_{i+1} = K_i\left(\sqrt{k_i}\right)$ *e* $k_i \in K_i$, *para cada i relevante.*

Não exigimos que $\sqrt{k_i} \notin K_i$; por exemplo, segundo a definição, *K* é uma extensão multi-quadrática de *K*; interessa também observar que, quando $k^2 \in K$, $\sqrt{k}$ é raiz de um polinómio numa variável *t*, com coeficientes em *K*, a saber: $t^2 - k^2$.

O teorema seguinte apresenta uma condição necessária e suficiente para a construtibilidade de um ponto $(x, y) \in \mathbb{R}$ a partir de um conjunto dado de pontos.

Teorema 2.1. *O ponto* $(x, y) \in \mathbb{R}^2$ *é construtível a partir do subconjunto S de* $\mathbb{R}^2$ *se e apenas se x e y pertencem a uma extensão multi-quadrática do subcorpo de* $\mathbb{R}$ *gerado pelo conjunto das coordenadas dos pontos em S.*

Juntando os resultados seguintes, ficamos na posse de instrumentos muito importantes para resolver os problemas referidos na introdução.

Se $\mathbb{Q} \subseteq K \subseteq L$, defina-se a seguinte notação

$|L : K|$ = dimensão de *L* como espaço vectorial sobre *K*.

Teorema 2.2 (da Torre) *Se* $K \subseteq L \subseteq M \subseteq \mathbb{R}$, *então*

$$|M : K| = |M : L| \cdot |L : K|.$$

Este teorema permite estender o lema 2.1 ao caso de uma extensão multi-quadrática e está demonstrado em quase todos os livros que tratam da teoria dos corpos, por exemplo em [BO].

Finalmente, combinando com o lema 2.1 e o teorema 2.1

Corolário 2.1 *Se L for uma extensão multi-quadrática de K, então* $|L:K|$ *é uma potência de 2. Em particular, as coordenadas dos pontos de* $\mathbb{R}^2$ *construtíveis a partir de* $\{(0,0),(0,1)\}$ *estão numa extensão cuja dimensão sobre* $\mathbb{Q}$ *é uma potência de 2.*

3. A trissecção do ângulo

Tal como anunciámos no início, o problema de trissecção do ângulo tem resposta negativa. Esta secção é dedicada a uma demonstração do seguinte teorema:

Teorema 3.1 *É impossível trissectar o ângulo 60º com régua e compasso; mais geralmente, não existe construção para trissectar um ângulo arbitrário.*

A demonstração que vamos apresentar envolve o comportamento de polinómios de grau 3 e utiliza os dois lemas seguintes.

Lema 3.1 *Sejam K um subcorpo de* $\mathbb{R}$ *e* $f(t) = t^3 + bt + c$ *um polinómio de coeficientes em K* $(b, c \in K)$. *Suponha que f(t) tem uma raiz* $\alpha \in \mathbb{R}$.

1. Se existe $k \in K$ *tal que* $\alpha \in K(\sqrt{k})$, *então f(t) tem uma raiz em K.*

2. Se α *está em alguma extensão multi-quadrática K, então f(t) tem uma raiz em K.*

Demonstração. (1) Se $\sqrt{k} \in K$ então $K\left(\sqrt{k}\right) = K$ e $\alpha \in K$ é raiz de f(t). Logo, podemos supor que $\sqrt{k} \notin K$, pelo que $\{1, \sqrt{k}\}$ é base de $K(\sqrt{k})$ sobre K (lema 2.1). Existem assim $u, v \in K$ tais que $\alpha = u + v\sqrt{k}$. Se $v = 0$, então $\alpha \in K$; logo, podemos supor que $v \neq 0$. Temos

$f(\alpha) = \left(u^3 + 3uv^2k + bu + c\right) \times 1 + \left(3u^2v + v^3k + bv\right) \times \sqrt{k} = 0.$

Como $\{1, \sqrt{k}\}$ é conjunto linearmente independente sobre *K*, e $v \neq 0$, segue-se que

$$u^3 + 3uv^2k + bu + c = 0$$

e $$3u^2 + v^2k + b = 0.$$

Eliminando o termo v^2K concluímos que

$$-8u^3 - 2ub + c = 0.$$

Logo, $-2u \in K$ é raiz de f(t).

(2) Segue-se de (1) por indução.

Com o fim de aplicarmos o lema anterior, convém recordar o

Lema 3.2 *Se o polinómio* $f(t) = a_n t^n + \ldots + a_1 t + a_0$ *tem coeficientes inteiros, u e v são números inteiros primos entre si e* $\frac{u}{v}$ *é raiz de f(t), então u divide* a_0 *e v divide* a_n.

Passemos então à demonstração do teorema 3.1. Recordem-se também as definições 2.1 e 2.2.

Demonstração (do teorema 3.1) Defina-se *O*:=(0,0), X:=(1,0), P_0:={O,X\}, K_0 = Q . É fácil construir um triângulo equilátero sobre a base *OX* a partir de P_0, pelo que podemos construir um ponto A tal que $\angle XOA$ = 60º e |OA| = 1.

Se fosse possível trissectar ângulo *XÔA*, seria possível construir, a partir de P_0, um ponto *B* tal que $\angle$XOB = 20° e |OB|=1; logo, também se poderia construir, a partir de P0, o ponto *D* := (cos(20°),0) de *OX*. Assim, cos(20º) pertenceria a uma extensão multi-quadrática, *K*, de Q, pelo que também 2cos(20º) estaria em K. Seja *r* = 2cos(20º).

Como $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$, tem-se

$$4\cos^3(20°) - 3\cos(20°) = \cos(60°) = \frac{1}{2};$$

mas então, $r^3 - 3r - 1 = 0$, ou seja r seria raiz do polinómio de coeficientes racionais $f(t) := t^3 - 3t - 1$. Uma vez que estamos a supor que *r* estaria numa extensão multi-quadrática de Q, segue-se do lema 3.1 que *f(t)* teria uma raiz racional. Ora, pelo lema 3.2, se *u* e *v* são números inteiros primos entre si e $\frac{u}{v}$ é raiz de *f(t)*, acontece que *u* e *v* dividem 1, i.e., $u = \pm v = \pm 1$; como $f(1) \neq 0 \neq f(-1)$, *f(t)* não tem raízes racionais, uma contradição. Não é portanto possível trisectar XÔA com régua e compasso.

4. Duplicação do cubo

Em seguida, resolvemos o problema da duplicação do cubo. O problema consistia de facto em construir um cubo cujo volume fosse o dobro do volume de um cubo dado. Ora as nossas construções referem-se a figuras planas e é lícito observar que um cubo é tridimensional, mais precisamente, as diagonais das faces bem como as diagonais não estão todas no mesmo plano. Mas se o cubo tiver arestas de comprimento uma unidade, as diagonais têm comprimentos respectivamente $\sqrt{2}$ e $\sqrt{3}$ unidades, e segmentos de recta de $\sqrt{2}$ ou $\sqrt{3}$ unidades são construtíveis (em E) a partir do segmento de recta com uma unidade de comprimento. Por outras palavras, as diagonais do cubo inicial não trazem segmentos de recta cujos comprimentos não podiam ter sido construídos a partir da aresta do cubo. Logo, e "como manda a tradição" (que temos vindo a estabelecer...), interpretamos este problema como sendo a construção de um segmento de recta de comprimento $\sqrt[3]{2}$ unidades sendo dado um segmento de recta de 1 unidade.

Teorema 4.1 *É impossível duplicar o cubo com régua e compasso.*

Demonstração. Se o ponto ($\sqrt[3]{2}$, 0) fosse construtível a partir de {(0,0),(1,0)}, $\sqrt[3]{2}$ pertenceria a uma extensão multi-quadrática de Q. Mas $\sqrt[3]{2}$ é raiz de $g(t) = t^3 - 2$. Logo, pelo lema 3.1, $t^3 - 2$ tem uma raiz racional. Como, pelo lema 3.2, qualquer raiz racional de *g(t)* admite a forma $\frac{u}{v}$, onde *u* e *v* são números inteiros primos entre si, *u*

divide 2 e *v* divide 1; mas nenhum dos números ±1, ±2 é raiz de *g(t)*; segue-se que $\sqrt[3]{2}$ não está em qualquer extensão multi-quadrática de $\mathbb{Q}$ e o cubo não pode ser duplicado com régua e compasso.

5. A quadratura do círculo

Vimos como se podem resolver, pela negativa, dois dos problemas clássicos. O problema da quadratura do círculo, i.e., de construir com régua e compasso (o lado de) um quadrado com área igual à de um círculo dado com raio não nulo, é bastante mais difícil do que os outros dois por assentar numa distinção mais fina de tipos de números e resultados de Análise Matemática.

Quanto a distinção de números: um número real diz-se **algébrico** se for raiz de um polinómio de coeficientes racionais; caso contrário diz-se **transcendente**. E vale o teorema seguinte:

Teorema 5.1 *Um número real r é algébrico se e apenas se* $|\mathbb{Q}(r):\mathbb{Q}|$ *for finita. Se r é um número algébrico,* $|\mathbb{Q}(r):\mathbb{Q}|$ *é o grau de qualquer polinómio não nulo f(t) de coeficientes racionais e grau mínimo tal que f(r)=0.*

Em 1882, Lindemann demonstrou o

Teorema 5.2 (de Lindemann) *O número* π *é transcendente.*

Uma demonstração deste teorema - que utiliza Análise Matemática - pode encontrar-se em [HC] e [SI]. E mais uma vez ficamos perante uma resposta negativa:

Teorema 5.3 *É impossível quadrar o círculo.*

Demonstração. Dada uma circunferência de raio 1, a construção requerida é a de um quadrado com lado de comprimento $\sqrt{\pi}$ unidades. Se $\sqrt{\pi}$ fosse construtível, pelo teorema 2.1 e corolário 2.1, $|\mathbb{Q}(r):\mathbb{Q}| = 2^m$, para algum número natural *m*. Como $\mathbb{Q} \subseteq \mathbb{Q}(\pi) \subseteq \mathbb{Q}(\sqrt{\pi})$, então $|\mathbb{Q}(\pi):\mathbb{Q}|$ divide 2^m pelo Teorema da Torre (2.2), sendo portanto finita; tal não pode acontecer, pelo teorema 5.1 e o teorema de Lindemann (5.2), portanto $\sqrt{\pi}$ não é construtível e o círculo não é quadrável.

6. Polígonos Regulares

6.1 Preliminares

Um triângulo equilátero admite uma construção (com régua e compasso) fácil e bem conhecida. Um pentágono regular é também construtível: *vide*, por exemplo, [AA]. Gauss, ainda jovem em 1796, descobriu uma construção de um polígono regular de 17 lados, e uma condição suficiente para que um polígono regular de *n* lados seja construtível. Gauss afirmou que o critério era também necessário, embora o artigo de Wantzel [WP] seja o primeiro a publicar uma demonstração deste facto. Para os efeitos da construção de polígonos regulares, convém encarar as construções como sendo feitas no plano complexo, $\mathbb{C}$ (com o eixo real em vez do eixo dos *xx* e o eixo imaginário em vez do eixo dos yy).

Concretamente, seja *n* um número natural, maior que 3 para evitar trivialidades. O polinómio $t^n - 1$ tem *n* raízes distintas da forma $e^{k2\pi i/n}$ (k = 0, 1, ... , *n*-1) ou, tomando $\zeta = e^{2\pi i/n}$, da forma ζ^k (k = 0, 1, ... , *n*-1); mais: estas *n* raízes são os vértices no plano complexo de um polígono regular inscrito na circunferência de centro 0 e raio 1, com vértice em 1. Temos

$$t^n - 1 = (t-1)(t^{n-1} + t^{n-2} + \ldots + t + 1).$$

Os pontos 0 e 1 ($= \zeta^n$) são dados e interessa construir os pontos $z \in \mathbb{C}$ tais que

$$z^{n-1} + z^{n-2} + \ldots + z + 1 = 0.$$

Por exemplo, no caso do pentágono regular ($n = 5$) há que construir os pontos $z \in \mathbb{C}$ tais que

$$z^4 + z^3 + z^2 + z + 1 = 0.$$

Como um tal z é não-nulo, podemos dividir ambos os membros por z^2 e fazer a substituição $y = z + 1/z$ para obter $y^2 + y - 1 = 0$ ou seja

$$y = (-1 \pm \sqrt{5})/2 \text{ com } z^2 - yz + 1 = 0.$$

Segue-se

$$z = \frac{\left(-1 \pm \sqrt{5}\right)}{4} \pm^* \frac{i\sqrt{10 \pm 2\sqrt{5}}}{4},$$

onde os sinais $\pm$ se correspondem, sendo o sinal $\pm^*$ independente, pelo que temos 4 soluções para z (como deveria acontecer). Basta agora construir o ponto $\frac{-1+\sqrt{5}}{4}$ no eixo real, bem como a circunferência de raio 1, de seguida construir o vértice

$$\frac{-1+\sqrt{5}}{4} + \frac{i\sqrt{10+2\sqrt{5}}}{4},$$

e completar o pentágono.

Citamos o critério de Gauss e Wantzel:

Teorema 6.1 (Gauss-Wantzel). *O polígono regular de n lados é construtível se e só se*

$$n = 2^{\alpha} p_1 \ldots p_s,$$

para certos números inteiros $\alpha \geq 0$ e p_i (i = 1, ..., s), sendo os p_i primos ímpares distintos da forma $p_i = 2^{\left(2^{r_i}\right)} + 1$ com cada r_i inteiro positivo.

Para a demonstração deste resultado consulte-se [HC] ou [BO].

Os números $F_r := 2^{\left(2^r\right)} + 1$, são designados por **números de Fermat**, um **primo de Fermat** é um número F_r que seja primo. Os cinco primeiros números de Fermat, $3 = F_0$, $5 = F_1$, $17 = F_2$, $257 = F_3$, $65537 = F_4$ são primos. Fermat conjecturou que F_r é sempre primo, mas Euler mostrou que $F_5 = 4294967297 = 641 \times 6700417$. Até hoje, não é conhecido qualquer primo de Fermat além dos que descrevemos.

Dado o resultado de Gauss-Wantzel, é de evidente interesse encontrar construções dos polígonos regulares com F_r lados quando $r \leq 4$. Existem vários livros que incluem uma construção do heptadecágono regular (17 lados); *vide*, por exemplo, [BB], [HW], [RS] e [SI]. Outros livros descrevem um algoritmo para o heptadecágono regular sem incluir uma construção concreta; *vide*, por exemplo, [HC] e [GL]. Para informação sobre o polígono regular de 257 lados, *vide* os artigos [BW], [GH] e [TD]; em [TD] constam observações sobre a construção do polígono regular de 65537 lados.

6.2 O Heptadecágono regular

Limitamo-nos a um esboço. Temos $n = 17$ e basta construir os pontos $z \in \mathbb{C}$ tais que

$$z^{16} + z^{15} + \ldots + z + 1 = 0.$$

Seja $\zeta = e^{2\pi i/17}$. Tem-se

$$\zeta^{16} + \ldots + \zeta + 1 = 0.$$

Sejam

$$y_1 = \zeta + \zeta^2 + \zeta^4 + \zeta^8 + \frac{1}{\zeta^8} + \frac{1}{\zeta^4} + \frac{1}{\zeta^2} + \frac{1}{\zeta},$$

e

$$y_2 = \zeta^3 + \zeta^5 + \zeta^6 + \zeta^7 + \frac{1}{\zeta^7} + \frac{1}{\zeta^6} + \frac{1}{\zeta^5} + \frac{1}{\zeta^3}.$$

Como $\zeta^{17} = 1$, temos $1/\zeta^m = \zeta^{17-m}$, logo

$$y_1 + y_2 = \zeta^{16} + \ldots + \zeta = -1.$$

Feitas árduas contas, podemos também concluir

$$y_1 y_2 = -4.$$

Os números y_1 e y_2 são assim as raízes de $t^2 + t - 4$, ou seja

$$\{y_1, y_2\} = \left\{\frac{-1+\sqrt{17}}{2}, \frac{-1-\sqrt{17}}{2}\right\}.$$

Portanto, y_1 e y_2 são ambos construtíveis. Subsiste no entanto o problema aqui de identificar cada um dos y_1 e y_2 por si mesmos. Ora, se repararmos que $1/\zeta^m$ é o conjugado complexo de ζ^m, podemos concluir

$$y_1 = 2\left(\cos(\theta) + \cos(2\theta) + \cos(4\theta) + \cos(8\theta)\right),$$

e

$$y_2 = 2\left(\cos(3\theta) + \cos(5\theta) + \cos(6\theta) + \cos(7\theta)\right),$$

sendo $\theta = 2\pi/17$. Mais alguns cálculos mostram que $y_1 > y_2$, logo

$$y_1 = \frac{-1+\sqrt{17}}{2}$$

e

$$y_2 = \frac{-1-\sqrt{17}}{2},$$

onde relembramos que $\sqrt{r}$ designa a raiz quadrada *positiva* do número real positivo *r*. Isto é, y_1 e y_2 são de facto construtíveis um de cada vez.

Em seguida, definem-se

$$y_{1,1} = \zeta + \zeta^4 + \frac{1}{\zeta^4} + \frac{1}{\zeta}$$

$$y_{1,2} = \zeta^2 + \zeta^8 + \frac{1}{\zeta^8} + \frac{1}{\zeta^2}$$

$$y_{2,1} = \zeta^3 + \zeta^5 + \frac{1}{\zeta^5} + \frac{1}{\zeta^3}$$

$$y_{2,2} = \zeta^6 + \zeta^7 + \frac{1}{\zeta^7} + \frac{1}{\zeta^6}.$$

Obtemos facilmente $y_{1,1} + y_{1,2} = y_1$ e, com mais trabalho, $y_{1,1}y_{1,2} = -1$. Segue-se que $y_{1,1}$ e $y_{1,2}$ são as raízes do polinómio $t^2 - y_1 t - 1$ com coeficientes em $Q(y_1)$. Mais uma vez, cálculos com cosenos mostram que $y_{1,1} > y_{1,2}$. Também $y_{2,1}$ e $y_{2,2}$ são as raízes de $t^2 - y_2 t - 1$ e $y_{2,1} > y_{2,2}$. E conseguimos

$$y_{1,1} = \frac{y_1 + \sqrt{y_1^2 + 4}}{2}$$

$$y_{2,1} = \frac{y_2 + \sqrt{y_2^2 + 4}}{2}.$$

Logo, $y_{1,1}$ e $y_{2,1}$ são construtíveis a partir de y_1 e y_2, e daí, construtíveis a partir de Q.

Defina-se

$$y_{1,1,1} = \zeta + \frac{1}{\zeta}$$

$$y_{1,1,2} = \zeta^4 + \frac{1}{\zeta^4}.$$

Analogamente $y_{1,1,1}$ e $y_{1,1,2}$ são raízes de $t^2 - y_{1,1}t + y_{2,1}$ e $y_{1,1,1} > y_{1,1,2}$, pelo que

$$y_{1,1,1} = \frac{y_{1,1} + \sqrt{y_{1,1}^2 - 4y_{2,1}}}{2}.$$

Mais uma vez, $y_{1,1,1}$ é construtível a partir de $y_{1,1}$ e $y_{2,1}$, logo é construtível a partir de Q.

Finalmente, $\zeta + 1/\zeta = y_{1,1,1}$ enquanto $(\zeta)(1/\zeta) = 1$. Logo, ζ e $1/\zeta$ são as raízes de $t^2 - y_{1,1,1}t + 1$, ou seja

$$\{\zeta, 1/\zeta\} = \{\frac{y_{1,1,1} + \sqrt{y_{1,1,1}^2 - 4}}{2}, \frac{y_{1,1,1} - \sqrt{y_{1,1,1}^2 - 4}}{2}\}.$$

Sabemos que ζ é não-real e está no primeiro quadrante do plano complexo, pelo que

$$\zeta = \frac{y_{1,1,1} + i\sqrt{4 - y_{1,1,1}^2}}{2},$$

e ζ, por sua vez, é construtível a partir de $y_{1,1,1}$ e logo a partir de Q. Já temos os pontos 0,1 e ζ no plano complexo, e podemos completar o polígono de 17 lados.

As definições dos números $y_{a,b,c}$ parecem resultar de actos de magia... De facto, são sugeridas (*vide* [GL]) pela estrutura de um certo grupo (o **Grupo de Galois** da exten-

são $Q(\zeta)$ de Q) que é um grupo cíclico de ordem 16: a última transferência de tecnologia da nossa história.

Agradecimentos

Gostaria de agradecer ao Prof. Doutor Vítor Neves uma revisão profunda deste artigo, e ao Prof. Doutor Jason Gallas as referências [GH] [TD].

Bibliografia

[AA] **Antunes, A.J.:** *Pentágono inscrito numa circunferência*, Gazeta de Matemática nº 138, 47-49, 2000.

[BB] **Bold, Benjamin:** *Famous Problems of Geometry and How to Solve Them*, Dover, New York, 1982.

[BC] **Boyer, Carl B.:** *A History of Mathematics*, John Wiley, New York, 1968.

[BO] **Brison, Owen J.:** *Teoria de Galois*, Dep. de Matemática da Fac. de Ciências da Univ. de Lisboa, Lisboa, 3ª edição, 1999.

[BW] **Bishop, Wayne:** *How to construct a regular polygon*, Amer. Math. Monthly, vol. 85, 186-188, 1978.

[CG] **Conway, John H. & Richard Guy:** *O Livro dos Números*, Univ. de Aveiro, Gradiva, 1999.

[E] **Euclid:** *The Thirteen Books of the Elements*, ~ 300a.C. Tradução com introdução e comentário de Sir Thomas Heath, CUP, 1908. Reimpressão Dover Inc., New York. Vols. I, II, III, 1956.

[FR] Ferre**ira, Rosa Antónia de Oliveira Figueiredo Tomás:** *Geometria Origami*, Tese de Mestrado, Deptº de Matª Pura, Fac. de Ciências da Univ. do Porto, 2000.

[GC] **Gauss, C.F.:** *Disquisitiones Arithmeticae*, Göttingen,1801.

[GH] **Gottlieb, Christian:** *The Simple and Straightforward Construction of the Regular 257-gon*, Math. Intelligencer, vol. 21, No. 1, 31-37, 1999.

[GL] **Gaal, Lisl:** *Classical Galois Theory with Examples*, Markham Publishing Company, Chicago, 1971.

[HC] **Hadlock, Charles Robert:** *Field Theory and its Classical Problems*, The Math. Assoc. of Amer., 1978.

[HW] **Hardy, G.H. & E.M. Wright:** *An Introduction to the Theory of Numbers*, OUP, 5ª edição, 1979.

[RS] **Row, T. Sundara:** *Geometric Exercises in Paper Folding*, Dover, New York, 1966.

[SI] **Stewart, Ian:** *Galois Theory*, Chapman & Hall, London, 2ª edição, 1989.

[TD] **De Temple, D.:** *Carlisle Circles and the Lemoine Simplicity of Polynomial Construction*, Amer. Math. Monthly, vol. 98, 97-108, 1991.

[WP] **Wantzel, P.L.:** *Recherches sur les moyens de reconnaître si un problème de géométrie peut se résoudre avec la règle et le compas*, J. Math. Pures Appl., vol. 2, 77-83, 1837.

Poema de geometria e de silêncio
Ângulos agudos e lisos
Entre duas linhas vive o branco

Sophia de Mello Breyner Andersen, *Coral*, Livraria Simões Lopes, Porto, 1950.
(publicação gentilmente autorizada pela autora)