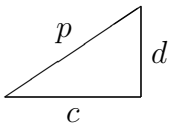
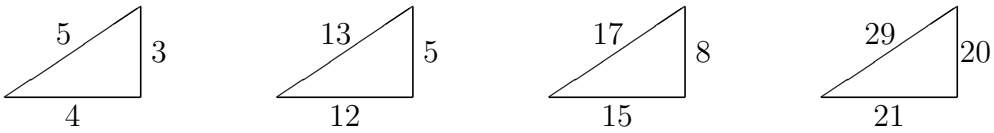
Uma aplicação dos corpos finitos à Teoria dos Números

A seguinte questão constitui um problema clássico da Teoria dos Números:

> Problema: *Seja $p \in \mathbb{N}$, primo. Quando é que p pode ser a hipotenusa de um triângulo rectângulo de catetos c e d inteiros?*



É claro que tal é possível exactamente quando $p^2 = c^2 + d^2$, para algum par c, d de inteiros positivos. Por exemplo, para $p = 5, 13, 17, 29$:



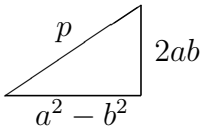
Como ilustração do que se pode fazer com os resultados que vimos até ao momento, vamos agora apresentar uma prova extremamente elegante, retirada dos apontamentos de Álgebra II de A. Machiavelo [DMUP, 1997-99], de um resultado de Fermat que ajuda a resolver este problema.

> Proposição [Fermat]: *Se $p \in \mathbb{N}$ é primo e $p \equiv 1 \pmod 4$ então p é soma de dois quadrados.*

De facto, se p é uma soma $a^2 + b^2$ de dois quadrados então

$$p^2 = (a^2 + b^2)^2 = a^4 + 2a^2b^2 + b^4 = (a^2 - b^2)^2 + (2ab)^2,$$

pelo que, tomando $c = a^2 - b^2$ e $d = 2ab$, obtemos um triângulo nas condições do problema, com hipotenusa p:



Assim, a Proposição de Fermat dá-nos uma condição suficiente para que um primo p seja hipotenusa de um tal triângulo:

$$p \equiv 1 (\mathrm{mod} 4).$$

É o caso de todos os exemplos que apresentámos acima:

$$\begin{aligned}
p=5: \quad 5 &= 2^2+1^2 \Rightarrow 5^2=(2^2-1^2)^2+(2\times 2\times 1)^2=3^2+4^2;\\
p=13: \quad 13 &= 3^2+2^2 \Rightarrow 13^2=(3^2-2^2)^2+(2\times 3\times 2)^2=5^2+12^2;\\
p=17: \quad 17 &= 4^2+1^2 \Rightarrow 17^2=(4^2-1^2)^2+(2\times 4\times 1)^2=15^2+8^2;\\
p=29: \quad 29 &= 5^2+2^2 \Rightarrow 29^2=(5^2-2^2)^2+(2\times 5\times 2)^2=21^2+20^2.
\end{aligned}$$

Demonstremos então a Proposição de Fermat, usando alguns factos sobre corpos finitos provados na aula anterior.

Para isso começamos por determinar todos os primos p para os quais -1 é um quadrado módulo p, ou seja, para os quais $\mathbb{F}_p$ tem uma raiz quadrada de -1.

Quando $p=2$ a resposta é óbvia: $-1=1=1^2$. Suponhamos pois $p\neq 2$. Seja F uma extensão de decomposição sobre $\mathbb{F}_p$ do polinómio $x^2+1\in\mathbb{F}_p[x]$, e denotemos por i uma das duas raízes deste polinómio em F. Como vimos na proposição no início da aula anterior, para cada $a\in F$ tem-se que $a\in\mathbb{F}_p$ se e só se $a^p=a$. Assim, em particular, $i\in\mathbb{F}_p$ se e só se $i^p=i$. Mas

$$i^p=(i^2)^{\frac{p-1}{2}}i=(-1)^{\frac{p-1}{2}}i,$$

que é igual a i quando e só quando $(-1)^{\frac{p-1}{2}}=1$, ou seja, quando e só quando $p-1$ é um múltiplo de 4. Portanto, a equação $x^2\equiv -1 \pmod p$ (p primo) tem solução se e só se $p=2$ ou $p\equiv 1 \pmod 4$.

Seja agora p um primo tal que $p\equiv 1 \pmod 4$. Então, pelo que acabámos de ver, $m^2\equiv -1 \pmod p$, ou seja, $p|(m^2+1)$, para algum inteiro m. Isto implica que, no domínio $\mathbb{Z}[i]$ dos inteiros de Gauss, $p|(m+i)(m-i)$. Como $p\nmid (m+i)$ e $p\nmid (m-i)$, resulta que p não é primo em $\mathbb{Z}[i]$. Mas $\mathbb{Z}[i]$ é um domínio de ideais principais, donde p, não sendo primo, é necessariamente redutível, ou seja, existem inteiros a,b,c,d tais que $p=(a+bi)(a'+b'i)$. Consequentemente, $|p|=|a+bi|\,|a'+b'i|$ e, elevando ao quadrado, $p^2=(a^2+b^2)(a'^2+b'^2)$. Como p é um inteiro primo, é fácil de ver que isto implica $a^2+b^2=a'^2+b'^2=p$. Em conclusão, $p=a^2+b^2$ como afirmou Fermat.

Exercício:

(1) Seja p um primo ímpar e F uma extensão de decomposição sobre $\mathbb{F}_p$ do polinómio x^2+1. Designando por i uma das raízes em F de x^2+1, use a relação $(1+i)^2=2i$ para determinar quais os primos p tais que 2 é um quadrado módulo p.

(2) Use (1) para provar o seguinte resultado de Euler:

Se p é um primo tal que $p \equiv 3$ (mod 4) e $2p+1$ é primo, então $(2p+1)|(2^p-1)$.

[Este resultado de Euler mostra, em particular, que o *número de Mersenne* $2^p - 1$ não é primo para $p > 3$ nas condições enunciadas; por exemplo: $23|2^{11}-1$, $47|2^{23}-1$]

[Mais uma vez, note a utilidade da introdução do conceito de polinómio como função definida em $\mathbb{N}_0$ com suporte finito (Aula 5), distinguindo-os assim das respectivas funções polinomiais. De facto, pelo Teorema pequeno de Fermat ("para cada a não divisível pelo primo p, $a^{p-1} \equiv 1 \pmod{p}$"), existe apenas um número finito de funções polinomiais $\mathbb{F}_p \to \mathbb{F}_p$ (por exemplo, a função $x \mapsto x^p$ é igual a $x \mapsto x$), enquanto que os polinómios permitem construir uma infinidade de extensões de $\mathbb{F}_p$, para cada primo p, e tais extensões permitem-nos obter resultados não triviais sobre, por exemplo, os números inteiros, como acabámos de ilustrar]

Teorema. [Critério dos subcorpos]
Seja $\mathbb{F}_q$ o corpo de Galois com $q = p^n$ elementos. Então:

(a) *Todo o subcorpo de $\mathbb{F}_q$ tem ordem p^d, para algum divisor positivo d de n.*

(b) *Reciprocamente, para cada divisor positivo d de n, existe exactamente um subcorpo de $\mathbb{F}_q$ com p^d elementos.*

Demonstração. (a) Seja K um subcorpo de $\mathbb{F}_q$. É evidente que K e $\mathbb{F}_q$ têm o mesmo subcorpo primo P, que é isomorfo a $\mathbb{F}_p$:

$$\mathbb{F}_p \cong P \subseteq K \subseteq \mathbb{F}_q.$$

Então, pelo primeiro teorema da aula anterior, $|K| = p^d$, onde $d = [K : P]$. Mas $n = [\mathbb{F}_q : P] = [\mathbb{F}_q : K]\,[K : P] = [\mathbb{F}_q : K]\,d$, logo $d|n$.

(b) Se $d|n$ (isto é, $n = md$ para algum $m \in \mathbb{N}$) então $p^d - 1|p^n - 1$:

$$p^n - 1 = p^{dm} - 1 = (p^d - 1)(p^{d(m-1)} + p^{d(m-2)} + \cdots + p^d + 1). \qquad (1)$$

Por sua vez, a partir de $p^d - 1 | p^n - 1$, podemos concluir, fazendo o mesmo que em (1) com x no lugar de p, que $x^{p^d-1} - 1 | x^{p^n-1} - 1$. Multiplicando por x obtemos, ainda, $x^{p^d} - x | x^{p^n} - x = x^q - x$. Portanto, qualquer raiz de $x^{p^d} - x$ é raiz de $x^q - x \in \mathbb{F}_q[x]$. Por outro lado,

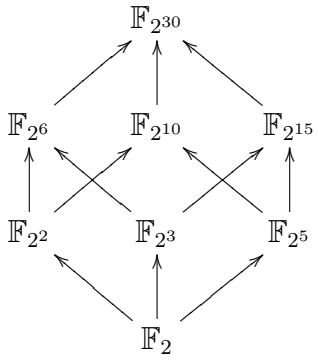
[Recorde da aula anterior: a extensão de decomposição do polinómio $x^{p^n} - x$ sobre $\mathbb{F}_p$ tem exactamente p^n elementos, e é isomorfa a $\mathbb{F}_{p^n}$]

$\mathbb{F}_q$ é a extensão de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. Então $\mathbb{F}_q$ contém todas as raízes de $x^{p^d} - x$, pelo que contém como subcorpo a extensão de decomposição de $x^{p^d} - x$ sobre $\mathbb{F}_p$. Isto mostra que esta extensão, que tem precisamente p^d elementos, é um subcorpo de $\mathbb{F}_q$, e é precisamente o subcorpo que procurávamos.

A unicidade decorre imediatamente do seguinte facto: se houvesse dois subcorpos distintos de ordem p^d em $\mathbb{F}_q$, juntos teriam mais do que p^d elementos (que são raízes em $\mathbb{F}_q$ de $x^{p^d} - x$), uma contradição, pois $x^{p^d} - x$ só pode ter no máximo p^d raízes. Portanto, o único subcorpo de $\mathbb{F}_{p^n}$ de ordem p^d é o corpo das raízes de $x^{p^d} - x \in \mathbb{F}_p[x]$ em $\mathbb{F}_{p^n}$. ∎

Isto significa que a lista de subcorpos de $\mathbb{F}_{p^n}$, a menos de isomorfismo, coincide precisamente com $\{\mathbb{F}_{p^d} : d | n\}$.

Por exemplo, os subcorpos de $\mathbb{F}_{2^{30}}$ podem ser determinados listando todos os divisores positivos de 30: como $30 = 2 \times 3 \times 5$, os únicos divisores positivos de 30 são 1,2,3,5,6,10,15,30, pelo que existem precisamente 8 subcorpos de $\mathbb{F}_{2^30}$:



Neste diagrama indicam-se ainda ainda as relações de inclusão entre os vários subcorpos. Pelo Teorema, estas relações são equivalentes às relações de divisibilidade entre os divisores positivos de 30.

$\mathbb{F}_2$ é o subcorpo primo de $\mathbb{F}_{2^{30}}$.