# Formas Quadráticas e Leis de Reciprocidade

André Macedo - 2º ano, FCUP

sob orientação do prof. António Machiavelo

10 de Junho de 2014

# Introdução

- Uma forma quadrática (inteira) binária é um polinómio homogéneo de grau 2 a duas variáveis da forma $f(x, y) = ax^2 + bxy + cy^2$. Escrevemos $f = (a, b, c)$ para denotar esta forma.
- Define-se o **discriminante** de $f$ como $\Delta = b^2 - 4ac$.
- $f$ diz-se definida se $\Delta < 0$, semi-definida se $\Delta = 0$ e indefinida caso $\Delta > 0$.

**Exemplo**

$f(x, y) = 7x^2 + 3xy + 5y^2$ é definida com $\Delta = -131$.

# Início de uma classificação

## Proposição

1. *Se $f$ é indefinida, então assume valores positivos e negativos.*
2. *Se $f$ é definida, então $a \neq 0$ e*
   - *$f(x,y) \geq 0$ caso $a > 0$ (e dizemos que $f$ é definida positiva).*
   - *$f(x,y) \leq 0$ caso $a < 0$ (e dizemos que $f$ é definida negativa).*
3. *Se $f$ é semi-definida, então $f(x,y) \geq 0$ se $a > 0$, $f(x,y) \leq 0$ se $a < 0$ e $f(x,y) = cy^2$ caso contrário.*

# Representações de inteiros

## Definição

Dizemos que uma forma quadrática $f$ representa um inteiro $n$ se existem inteiros $x_0, y_0$ tais que $f(x_0, y_0) = n$. Dizemos ainda que $f$ representa $n$ de forma própria se $(x_0, y_0) = 1$.

## Nota

Se $f(x_0, y_0) = n$ e $(x_0, y_0) = d$, então $d^2 | n$, $(\frac{x_0}{d}, \frac{y_0}{d}) = 1$ e $f(\frac{x_0}{d}, \frac{y_0}{d}) = \frac{n}{d^2}$. Desta forma, as representações de $n$ por $f$ reduzem-se às representações próprias de $\frac{n}{d^2}$.

Assim, estudamos apenas (sem perda de generalidade) as representações próprias de um dado inteiro por $f$.

# Representações de inteiros

**Teorema**

*Sejam $n$ e $d$ inteiros com $n \neq 0$. Então existe uma forma quadrática $f$ com $\Delta = d$ que representa $n$ de forma própria se e só se a congruência $x^2 \equiv d \pmod{4|n|}$ tiver solução.*

**Corolário**

*Seja $d \equiv 0$ ou $1 \pmod 4$. Se $p$ é um primo ímpar, então existe uma forma quadrática de discriminante $d$ que representa $p$ se e só se a equação $x^2 \equiv d \pmod p$ tiver solução.*

# Símbolo de Legendre

## Definição

Seja $a \in \mathbb{Z}$ e $p$ um primo ímpar. Define-se o símbolo de Legendre por:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se a é um resíduo quadrático módulo p.} \\ 0, & \text{se p divide a.} \\ -1, & \text{se a não é um resíduo quadrático módulo p.} \end{cases}$$

## Proposição

*O símbolo de Legendre tem as seguintes propriedades:*

- $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$ *(Critério de Euler).*
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
- *Se* $a \equiv b \pmod{p}$, *então* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

# Equivalência e Redução de formas

## Definição

Duas formas quadráticas $f, g$ dizem equivalentes (e escreve-se $f \sim g$) se existem $p, q, r, s \in \mathbb{Z}$ tais que $g(x, y) = f(px + qy, rx + sy)$ e $ps - qr = 1$.

- $\sim$ é uma relação de equivalência no conjunto das formas quadráticas.
- Se $f \sim g$, então os seus discriminantes são iguais e representam os mesmos inteiros.
- $h(d) :=$ número de classes de equivalência das formas com $\Delta = d$.

Será que existe um representante natural de cada classe de equivalência?

# Equivalência e Redução de Formas

**Teorema**

*Seja $f = (a, b, c)$ uma forma quadrática definida ($\Delta < 0$) positiva ($a > 0$). Então, é sempre possível encontrar uma única forma $g = (A, B, C)$ equivalente a $f$, dita a forma* **reduzida**, *com as seguintes propriedades:*

- $|B| \leq A \leq C$
- $B \geq 0$ *(se alguma das desigualdades acima não é estrita)*

Repare-se que, se $f = (a, b, c)$ é reduzida, então é válida a desigualdade $|b| \leq \sqrt{\frac{-\Delta}{3}}$, uma vez que $4b^2 \leq 4ac = b^2 - \Delta$, logo $3b^2 \leq -\Delta$. Assim o número de formas reduzidas com um discriminante $\Delta$ fixo é finito.

# Processo de Redução de Formas

A ideia base do algoritmo é a seguinte:

- De entre todas as formas equivalentes a uma dada, procuramos $f = (a, b, c)$ com $|b|$ tão pequeno quanto possível, por aplicação da transformação de coordenadas $(x, y) = (x + my, y)$, tornando $f = (a, b, c) \sim (a, 2am + b, c')$. Para essa forma, tem-se já as condições $|b| \leq a$ e $|b| \leq c$.
- Finalmente, se $a > c$, aplicamos a transformação $(x, y) = (-y, x)$, fazendo $f = (a, b, c) \sim (c, -b, a)$. A forma resultante obedece assim a $|b| \leq a \leq c$.
- A condição $b \geq 0$ se $|b| = a \vee a = c$ é satisfeita usando transformações semelhantes.

# Aplicações dos resultados estudados

## Proposição

*Seja $p$ um primo tal que $p|x^2+y^2$, com $x, y$ inteiros tais que $(x,y)=1$. Então $p$ é uma soma de dois quadrados.*

## Demonstração.

$p|x^2+y^2 \implies (\frac{x}{y})^2 \equiv -1 \pmod{p} \implies \left(\frac{-1}{p}\right) = 1$. Assim $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{4}{p}\right) = 1$, logo, pelo Corolário atrás apresentado, $p$ pode ser representado por uma forma de discriminante $\Delta = -4$. Ora, como $|b| \leq \sqrt{\frac{-\Delta}{3}} \implies b = 0$ (pois $b$ é par), logo $a = c = 1$ e a única forma (reduzida) possível é $f = (1,0,1)$, pelo que $p$ é a soma de dois quadrados. □

# Aplicações dos resultados estudados

Argumentos deste género (aliados a resultados de reciprocidade quadrática) podem ainda ser usados para concluir os seguintes resultados:

1. (Teorema de Fermat) para todo o primo $p \equiv 1 \pmod 4$, tem-se $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{4}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1 \implies$ existe uma forma com $\Delta = -4$ que representa $p$. Como qualquer tal forma é equivalente à reduzida $f = (1, 0, 1)$, $p$ é soma de dois quadrados.
2. para $\Delta = -3$, um argumento semelhante ao atrás usado permite-nos concluir que a única forma reduzida é $f = (1, 1, 1)$. Assim, e como, por reciprocidade quadrática $p \equiv 1 \pmod 3 \implies \left(\frac{-3}{p}\right) = 1$, então $p$ pode ser representado por uma forma com $\Delta = -3$. Como qualquer forma nestas condições é equivalente à reduzida $f = (1, 1, 1)$, então conclui-se que qualquer $p \equiv 1 \pmod 3$ é da forma $x^2 + xy + y^2$.

# Lei da Reciprocidade Quadrática

- Note-se que a base destas provas se baseia no conhecimento do valor de $h(d)$ e no cálculo do símbolo de Legendre $\left(\frac{a}{p}\right)$.
- A Lei da Reciprocidade Quadrática dá um algoritmo simples e eficiente de avaliar símbolos de Legendre.

**Teorema (Lei da Reciprocidade Quadrática)**

*Sejam $p$ e $q$ primos ímpares distintos. Então:*

- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
- $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

# Lei da Reciprocidade Quadrática

## Nota

Uma maneira equivalente de escrever a 3ª condição do teorema é: $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{((p-1)/2)((q-1)/2)}$, já que $\left(\frac{q}{p}\right)^2 = 1$.

## Exemplo

Note-se que, com $p = 29 \equiv 1 \pmod 4$, vem $(-1)^{((p-1)/2)((q-1)/2)} = 1$ $\forall q$ primo, logo $\left(\frac{29}{73}\right) = \left(\frac{73}{29}\right) = \left(\frac{15}{29}\right) = \left(\frac{3}{29}\right)\left(\frac{5}{29}\right) = \left(\frac{29}{3}\right)\left(\frac{29}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{-1}{5}\right) = (-1) \times (-1)^{(5-1)/2} = (-1) \times 1 = -1 \implies$ 29 não é resíduo quadrático módulo 73.

# Somas Quadráticas de Gauss

- Pode-se provar a Lei da Reciprocidade Quadrática usando somas de Gauss e trabalhando no anel dos inteiros algébricos $\Omega := \{w \in \mathbb{C} : w \text{ é raiz de um polinómio mónico com coeficientes inteiros}\}$.
- Neste anel, introduzimos a noção de congruência de maneira natural: Se $\omega_1, \omega_2, \gamma \in \Omega$, dizemos que $\omega_1 \equiv \omega_2 \pmod{\gamma}$ se $\omega_1 - \omega_2 = \gamma\alpha$, com $\alpha \in \Omega$.

**Definição**

Seja $a \in \mathbb{Z}$ e $p$ um primo ímpar. Define-se a soma quadrática de Gauss por $g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{at}$, onde $\zeta = e^{2\pi i/p}$ é uma p-ésima raiz primitiva da unidade.

# Traços Gerais da Prova

- Começa-se por provar que o valor de $g_a$ só depende de $g_1 = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^t$ — mais especificamente, tem-se a igualdade $g_a = \left(\frac{a}{p}\right) g_1$.
- De seguida, estudamos o valor de $g_1$. Avaliando a soma $\sum_{a=0}^{p-1} g_a g_{-a}$ de 2 maneiras distintas, prova-se que $g_1^2 = (-1)^{(p-1)/2} p$, estando o valor de $g_1$ determinado a menos de sinal.
- Finalmente, e denotando $p^* := (-1)^{(p-1)/2} p$, prova-se que $g_1^q \equiv \left(\frac{p^*}{q}\right) g_1 \pmod{q}$. Tem-se também $g_1^q \equiv g_q \pmod{q}$. Daqui, segue que $\left(\frac{p^*}{q}\right) g_1 \equiv g_q = \left(\frac{q}{p}\right) g_1 \implies \left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{(p-1)/2} \left(\frac{p}{q}\right) = (-1)^{((p-1)/2)((q-1)/2)} \left(\frac{p}{q}\right)$.

# Aplicações da Lei da Reciprocidade Quadrática

Esta Lei constitui uma ferramenta poderosa que permite resolver diversos problemas em Teoria dos Números, estabelecendo, por exemplo, a infinitude dos números primos $\equiv 1 \pmod 4$:

- Suponhamos que existem finitos tais primos $p_1, ..., p_k$, constrói-se $N = (2p_1...p_k)^2 + 1$. Seja $p$ um divisor primo de $N$. Note-se que $(2p_1...p_k)^2 \equiv -1 \pmod p \implies \left(\frac{-1}{p}\right) = 1 \implies$ (pela Lei de Reciprocidade Quadrática) $p \equiv 1 \pmod 4$ e $p \neq p_i \ \forall i = 1, ..., k$, contradição.

# Aplicações da Lei da Reciprocidade Quadrática

A Lei da Reciprocidade Quadrática dá-nos também um método de determinar a forma dos divisores primos de algumas classes de números:

- Seja $M_p = 2^p - 1$ um número de Mersenne.
  $q \mid M_p \iff 2^p \equiv 1 \pmod{q} \implies 2 \equiv 2^{p+1} \equiv (2^{(p+1)/2})^2 \pmod{q}$
  $\implies \left(\frac{2}{q}\right) = 1 \implies q \equiv \pm 1 \pmod{8}$.

# Reciprocidade Cúbica

Focamo-nos agora na equação $x^3 \equiv a \pmod{p}$. Infelizmente, se trabalharmos em $\mathbb{Z}_p$, os resultados não são muitos interessantes.

- Se $p \equiv 2 \pmod 3$, então todo o número é resíduo cúbico módulo $p$, já que, se $p = 3n + 2$, então

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

- Se $p \equiv 1 \pmod 3$, então não é fácil decidir se $a$ é ou não resíduo cúbico módulo $p$. De facto, a maior parte dos resultados nesse sentido baseiam-se na escrita de $p$ como soma de múltiplos de quadrados.

# $\mathbb{Z}[\omega]$

Um análogo da Lei da Reciprocidade Quadrática para esta nova equação pode ser obtido trabalhando sobre o anel $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$, onde $\omega = \zeta_3 = \frac{-1+\sqrt{3}i}{2}$ é uma raiz cúbica da unidade.

## Nota

- Prova-se que $\mathbb{Z}[\omega]$ é um Dominio Euclideano para a norma $N(\alpha) = \alpha\overline{\alpha}$, onde $\overline{\alpha}$ designa o complexo conjugado de $\alpha$.
- Os elementos invertíveis em $\mathbb{Z}[\omega]$ são $\pm 1, \pm\omega, \pm\omega^2$.
- Seja $p$ um primo em $\mathbb{Z}$. Se $p \equiv 2 \pmod 3$, $p$ é primo em $\mathbb{Z}[\omega]$, se $p \equiv 1 \pmod 3$, $p$ é produto de 2 primos complexos e $p = 3 = -\omega^2(1-\omega)^2$, com $1 - \omega$ primo.

# Reciprocidade Cúbica

- Se $\pi \in D = \mathbb{Z}[\omega]$ é um primo com $N(\pi) \neq 3$, prova-se que $D/\pi D$ é um corpo finito com $N(\pi)$ elementos e que é válida a congruência (para $\alpha$ coprimo com $\pi$) $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$.
- Da factorização
  $\alpha^{N(\pi)-1} - 1 = (\alpha^{(N(\pi)-1)/3} - 1)(\alpha^{(N(\pi)-1)/3} - \omega)(\alpha^{(N(\pi)-1)/3} - \omega^2)$
  e do facto de $\pi$ primo, resulta que existe um único $m = 0, 1, 2$ tal que $\alpha^{(N(\pi)-1)/3} \equiv \omega^m \pmod{\pi}$.

## Definição

Se $N(\pi) \neq 3$, define-se o resíduo cúbico de $\alpha$ módulo $\pi$ por:

- $\left(\frac{\alpha}{\pi}\right)_3 = 0$, se $\pi | \alpha$.
- $\alpha^{(N(\pi)-1)/3} \equiv \left(\frac{\alpha}{\pi}\right)_3 \pmod{\pi}$, com $\left(\frac{\alpha}{\pi}\right)_3 = 1, \omega, \omega^2$.

# Reciprocidade Cúbica

São válidas as seguintes propriedades para os resíduos cúbicos de $\alpha$:

**Proposição**

- $\left(\frac{\alpha}{\pi}\right)_3 = 1$ *se e só se a equação* $x^3 \equiv \alpha \pmod{\pi}$ *tem solução.*
- $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$.
- *Se* $\alpha \equiv \beta \pmod{\pi}$, *então* $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$.

Note-se que como há 6 unidades em $D = \mathbb{Z}[\omega]$, cada elemento não nulo em $D$ tem 6 associados. Para formular a Lei da Reciprocidade Cúbica, precisamos de introduzir a noção de primo primário.

# Lei da Reciprocidade Cúbica

## Definição

Um primo $\pi \in D = \mathbb{Z}[\omega]$ diz-se primário se $\pi \equiv 2 \pmod 3$ em $D$. Se $\pi = a + b\omega$, isto é equivalente a dizer que $a \equiv 2 \pmod 3$ e $b \equiv 0 \pmod 3$ em $\mathbb{Z}$.

Prova-se facilmente que cada primo $\pi \in D$ tem exactamente um primo associado primário.

## Teorema (Lei da Reciprocidade Cúbica)

*Sejam $\pi_1, \pi_2$ primos primários em $\mathbb{Z}[\omega]$ com $N(\pi_1), N(\pi_2) \neq 3$ e $N(\pi_1) \neq N(\pi_2)$. Então* $\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3$.

# Lei da Reciprocidade Cúbica

## Nota

Tal como na Lei da Reciprocidade Quadrática, na Cúbica existem leis suplementares que tratam os casos das unidades e do primo $1-\omega$:

- $\left(\frac{-1}{\pi}\right)_3 = 1$ para todo o primo $\pi$.
- $\left(\frac{1-\omega}{\pi}\right)_3 = \omega^{2m}$, onde $m$ é tal que:
  - Se $\pi = p$ for um primo inteiro, $m = \frac{p+1}{3}$
  - Se $\pi = a + b\omega$ for um primo primário complexo, $m = \frac{a+1}{3}$.

## Nota

A prova desta Lei segue as mesmas ideias da prova da Lei da Reciprocidade Quadrática, usando uma noção mais geral das somas de Gauss e o conceito de somas de Jacobi.

# $\mathbb{Z}[i]$

Para falarmos em Reciprocidade Quártica (ou Biquadrática), temos de trabalhar no anel dos inteiros Gaussianos $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$. O mesmo tratamento feito atrás pode ser realizado neste conjunto.

## Nota

- Prova-se que $\mathbb{Z}[i]$ é um Dominio Euclideano para a norma $N(\alpha) = \alpha\overline{\alpha}$, onde $\overline{\alpha}$ designa o complexo conjugado de $\alpha$.
- Os elementos invertíveis em $\mathbb{Z}[i]$ são $\pm 1, \pm i$.
- Os primos em $\mathbb{Z}[i]$ são os primos inteiros $p \equiv 3 \pmod 4$ e os elementos $\pi \in \mathbb{Z}[i]$ tais que $N(\pi)$ é um número primo inteiro (note-se que $2 = (1 + i)(1 - i)$ não é primo).

# Reciprocidade Biquadrática

- Se $\pi \in D = \mathbb{Z}[i]$ é um primo com $N(\pi) \neq 2$, prova-se novamente que $D/\pi D$ é um corpo finito com $N(\pi)$ elementos e que é válida a congruência (se $(\alpha, \pi)=1$) $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$. Deste resultado, segue que $\alpha^{\frac{N(\pi)-1}{4}} \equiv 1, -1, i, -i \pmod{\pi}$.

**Definição**

Se $N(\pi) \neq 2$, define-se o resíduo biquadrática de $\alpha$ módulo $\pi$ por:

- $\left(\frac{\alpha}{\pi}\right)_4 = 0$, se $\pi | \alpha$.
- $\alpha^{(N(\pi)-1)/4} \equiv \left(\frac{\alpha}{\pi}\right)_4 \pmod{\pi}$, com $\left(\frac{\alpha}{\pi}\right)_4 = 1, -1, i, -i$.

# Reciprocidade Biquadrática

## Proposição

- $\left(\frac{\alpha}{\pi}\right)_4 = 1$ *se e só se a equação* $x^4 \equiv \alpha \pmod{\pi}$ *tem solução em* $\mathbb{Z}[i]$.
- $\left(\frac{\alpha\beta}{\pi}\right)_4 = \left(\frac{\alpha}{\pi}\right)_4 \left(\frac{\beta}{\pi}\right)_4$.
- *Se* $\alpha \equiv \beta \pmod{\pi}$, *então* $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\beta}{\pi}\right)_4$.

Devido ao facto de cada elemento não-nulo em $\mathbb{Z}[i]$ ter 4 elementos associados, para formular a Lei da Reciprocidade Biquadrática, precisamos novamente de uma a noção de primo primário.

## Teorema (Lei da Reciprocidade Biquadrática)

*Sejam* $\pi, \lambda$ *primos primários em* $\mathbb{Z}[i]$. *Então* $\left(\frac{\pi}{\lambda}\right)_4 = \left(\frac{\lambda}{\pi}\right)_4 (-1)^{\frac{N(\lambda)-1}{4}\frac{N(\pi)-1}{4}}$.

# Primos de Mersenne Generalizados

- Se $p \in \mathbb{Z}$ for um primo, define-se o respectivo número de Mersenne por $G_p = (1+i)^p - 1$ em $\mathbb{Z}[i]$.
- Como $G_p = (1+i)(1+i)^{p-1} - 1 = (1+i)((1+i)^2)^{\frac{p-1}{2}} - 1 = (1+i)(2i)^{\frac{p-1}{2}} - 1 \implies \Im(G_p) \neq 0 \implies$
  $G_p$ é primo $\Leftrightarrow N_p := N(G_p) = 2^p - \left(\frac{2}{p}\right) 2^{\frac{p+1}{2}} + 1$ é primo.
- Usando o Teorema de Lagrange, pode-se provar que se $q | N_p$, então $q = 4pk + 1$, $k \in \mathbb{Z}$.
- Usando a Lei da Reciprocidade Biquadrática, prova-se a condição necessário para a primalidade de $N_p$ (e, portanto, de $G_p$):
  - $5^{\frac{N_p-1}{4}} \equiv -1 \pmod{N_p}$, se $p \equiv 1 \pmod 4$
  - $5^{\frac{N_p-1}{2}} \equiv -1 \pmod{N_p}$, se $p \equiv 3 \pmod 4$

# Referências


- A Classical Introduction to Modern Number Theory, Ireland & Rosen
- An Introduction to the Theory of Numbers, Niven, Zuckerman & Montgomery
- Binary Quadratic Forms, Buell