Introdução às Curvas Elípticas e Aplicações

Publicações Matemáticas

Introdução às Curvas Elípticas e Aplicações

Parham Salehyan
UNESP

30º Colóquio Brasileiro de Matemática

Impresso no Brasil / Printed in Brazil
Capa: Noni Geiger / Sérgio R. Vaz

30º Colóquio Brasileiro de Matemática

- Aplicações Matemáticas em Engenharia de Produção - Leonardo J. Lustosa e Fernanda M. P. Raupp
- Boltzmann-type Equations and their Applications - Ricardo Alonso
- Dissipative Forces in Celestial Mechanics - Sylvio Ferraz-Mello, Clodoaldo Grotta-Ragazzo e Lucas Ruiz dos Santos
- Economic Models and Mean-Field Games Theory - Diogo A. Gomes, Levon Nurbekyan and Edgard A. Pimentel
- Generic Linear Recurrent Sequences and Related Topics - Letterio Gatto
- Geração de Malhas por Refinamento de Delaunay - Marcelo Siqueira, Afonso Paiva e Paulo Pagliosa
- Global and Local Aspects of Levi-flat Hypersurfaces - Arturo Fernández Pérez e Jiří Lebl
- **Introdução às Curvas Elípticas e Aplicações - Parham Salehyan**
- Métodos de Descida em Otimização Multiobjetivo - B. F. Svaiter e L. M. Graña Drummond
- Modern Theory of Nonlinear Elliptic PDE - Boyan Slavchev Sirakov
- Novel Regularization Methods for Ill-posed Problems in Hilbert and Banach Spaces - Ismael R. Bleyer e Antonio Leitão
- Probabilistic and Statistical Tools for Modeling Time Series - Paul Doukhan
- Tópicos da Teoria dos Jogos em Computação - O. Lee, F. K. Miyazawa, R. C. S. Schouery e E. C. Xavier
- Topics in Spectral Theory - Carlos Tomei

Distribuição: IMPA
Estrada Dona Castorina, 110
22460-320 Rio de Janeiro, RJ
E-mail: ddic@impa.br
http://www.impa.br

ISBN: 978-85-244-0408-5

Conteúdo

Capítulo 0

Introdução

As curvas elípticas, além de terem uma história longa, possuem diversos métodos utilizados no seu estudo e aparecem naturalmente em diversas áreas de matemática, de teoria dos números à análise, e de criptografia à física matemática. A demonstração do último teorema de Fermat, integrais e funções elípticas, formas modulares e resolução da equação de pêndulo são exemplos dessa presença. Isso tudo e a facilidade de serem definidas, sem necessidade de muitos pré-requisitos, as torna objetos muito interessantes a serem apresentados aos alunos de graduação.

O foco principal é fazer uma introdução à teoria de curvas elípticas com destaque a alguns dos resultados mais importantes como teorema de Mordell-Weil, Nagell-Lutz, Mazur; e, como aplicação, apresentar um algoritmo para fatorar números inteiros. O teorema fundamental da aritmética garante a existência e a unicidade de fatoração de números inteiros em números primos. O problema computacional, ou seja, fatorar um determinado número inteiro, pode não ser uma tarefa fácil, principalmente se o número for muito grande. Esse problema, além de ser um problema do interesse dos matemáticos, é de grande importância prática. Existem diversos métodos e algoritmos para fatorar números inteiros, um deles é o algoritmo de Lenstra que utiliza curvas elípticas.

Os tópicos e seus conteúdos estão elaborados de forma acessível para os alunos de graduação. Por isso várias demosntrações não são apresentadas, até porque empregam métodos e técnicas mais avançados.

Com o objetivo de estudar os pré-requisitos necessários, inicialmente faremos uma rápida revisão sobre os polinômios de duas e três variáveis, polinômios homogêneos e zeros de equações polinomiais. Em seguida definiremos o espaço projetivo e estudaremos a relação dos objetos geométricos nos espaços afim e projetivo. Essa relação será exemplificada por retas e cônicas. Neste momento teremos os pré-requisitos necessários para definir curvas algébricas planas e estudar sua teoria elementar. A pretensão não é fazer uma introdução completa ao assunto. Pretendemos estudar alguns tópicos e resultados que serão utilizados no estudo de cúbias, ou seja, curvas de grau três.

Para explorar a teoria elementar de cúbias planas projetivas, após a definição e apresentação de exemplos, falaremos da classificação de cúbicas e finalmente definiremos as curvas elípticas. Em seguida definiremos uma operação entre os pontos de uma curva elíptica e observaremos que o conjunto desses pontos munido desta operação se torna um grupo abeliano. O resultado principal dessa parte é o teorema de Mordell-Weil: dada uma curva elíptica racional, existe um conjunto finito de seus pontos tal que todos os outros podem ser obtidos a partir destes por meio da operação definida anteriormente, ou seja, o grupo dos pontos racionais de uma curva elíptica racional é finitamente gerado. Outros resultados importantes como teorema de Mazur e Nagell-Lutz também serão apresentados. Esses teoremas nos fornecem informações valiosas sobre pontos de ordem finita e pontos inteiros de uma cúbica racional.

Por dois motivos dedicaremos um capítulo ao estudo de cúbicas sobre corpos finitos: uma técnica chamada de redução módulo números primos que é utilizada para verificar a existência de pontos de ordem finita sobre uma curva elíptica; e pelo algoritmo de Lenstra.

Por último, apresentaremos os algoritmos de Pollard e de Lenstra para fatorar números inteiros. O segundo utiliza curvas elípticas. Após explicar os fundamentos e a parte teórica, trataremos alguns exemplos para ilustrar o funcionamento destes algoritmos.

Este livro foi preparado num curto prazo de tempo e pode conter incorreções. Correções e sugestões poderão ser enviadas ao endereço parham @ibilce.unesp.br, ficarei muito satisfeito em recebê-las!

Agradecimentos. Gostaria de registar meus agradecimentos ao Comitê Organizador do 30° Colóquio Brasileiro de Matemática por ter dado oportunidade de ministrar este minicurso, e também à Divisão de Divulgação e Informação Científica por todo apoio durante a preparação deste livro.

Parham
maio de 2015

Capítulo 1

Preliminares

Neste capítulo reunimos alguns resultados básicos que serão utilizados nos próximos capítulos. As demonstrações dos resultados poderão ser consultadas na bibliografia apresentada.

1.1 Polinômios

Seja K um corpo. Chamamos os elementos de K de *constantes*. Dado um conjunto finito $\{a_0, a_1, \ldots, a_n\} \subset K$, formamos uma expressão $p := a_0x^0 + a_1x^1 + \cdots + a_nx^n$ e a chamamos de um *polinômio* em x sobre K. O símbolo x, chamado de um *indeterminado* ou uma *variável* é introduzido para facilitar as contas e não é um elemento de K. O conjunto de todos os polinômios em x sobre K é denotado por $K[x]$. Se $a_n \neq 0$, diremos que p possui grau n e escrevemos $\deg p = n$. O grau do polinômio zero, $p = 0$, é definido como $-\infty$. Por convenção, para todo $n \in \mathbb{Z}$,

$$-\infty < n, -\infty + n = -\infty, -\infty + (-\infty) = -\infty.$$

Nenhuma outra operação é definida com $-\infty$.

Dois polinômios $a_0x^0 + a_1x^1 + \cdots + a_nx^n$ e $b_0x^0 + b_1x^1 + \cdots b_mx^m$ são considerados iguais, se $n = m$ e $a_i = b_i$ pata todo $i = 1, \ldots, n$. Os polinômios são somados e multiplicados segundo as seguintes regras:

$$(a_0x^0 + a_1x^1 + \cdots + a_nx^n) + (b_0x^0 + b_1x^1 + \cdots b_nx^n) := \\ (a_0 + b_0)x^0 + (a_1 + b_1)x^1 + \cdots + (a_n + b_n)x^n;$$

e

$$(a_0x^0 + a_1x^1 + \cdots + a_nx^n) \cdot (b_0x^0 + b_1x^1 + \cdots + b_mx^m) := \\ a_0b_0x^0 + (a_1b_0 + a_0b_1)x^1 + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \cdots + a_nb_mx^{n+m}.$$

Observe que coeficientes zeros são acrescentados para que os polinômios tenham gruas iguais. Em relação aos graus, temos

$$\deg(f + g) \leq \max\{\deg f, \deg g\}, \quad \deg fg = \deg f + \deg g.$$

É fácil verificar que $K[x]$ munido dessas operações forma um domínio cujos zero e unidade são $0x^0$ e $1x^0$. Além disso $\{ax^0 \mid a \in K\}$ forma um corpo isomorfo a K, então podemos considerar $K \subset K[x]$. Para facilitar, substituiremos x^0 pela unidade de K e escreveremos x em lugar de x^1.

Da forma análoga, os polinômios em duas variáveis x e y são definidos como elementos de $K[x, y] := K[x][y]$, e por indução

$$K[x_1, \ldots, x_r] := K[x_1, \ldots, x_{r-1}][x_r].$$

Ou seja, um polinômio em r variáveis é uma soma finita $\sum p_i x_r^i$, onde cada p_i é um polinômio em $r - 1$ variáveis. Embora seja muito útil considerar um polinômio em r variáveis desta forma, é mais comum considerar sua forma geral como uma soma finita

$$p = \sum a_{i_1 \cdots i_r} x_1^{i_1} \cdots x_r^{i_r}, \quad a_{i_1 \cdots i_r} \in K, \ i_1, \ldots, i_r \in \mathbb{N}.$$

Cada termo $a_{i_1 \cdots i_r} x_1^{i_1} \cdots x_r^{i_r}$ é chamado de um *monômio* e seu grau é definido como $\sum_j i_j$. O grau do polinômio é definido como sendo o maior grau de seus monômios. Se todos os monômios tiverem o mesmo grau, ou seja, se existe $d \in \mathbb{N}$ tal que $\sum i_j = d$ para todo $i_1, \ldots, i_j$, então p é chamado de um *polinômio homogêneo* ou uma *forma*.

As operações entre polinômios são generalizadas naturalmente assumindo as regras de comutatividade e distribuição de multiplicação em relação à adição e $x_1^{i_1} \cdots x_r^{i_r} \cdot x_1^{j_1} \cdots x_r^{j_r} := x_1^{i_1 + j_1} \cdots x_r^{i_r + j_r}$. É um

exercício simples verificar que $K[x_1, \ldots, x_r]$ munido destas operações se torna um anel comutativo com unidade.

A maioria das propriedades de $K[x_1, \ldots, x_r]$ é obtida considerando esse domínio como $D[x_r]$, onde $D := K[x_1, \ldots, x_{r-1}]$. O corpo das frações de $K[x_1, \ldots, x_r]$ é denotado por $K(x_1, \ldots, x_r)$ e é chamado de corpo das *funções racionais* de $x_1, \ldots, x_r$ sobre K. Um dos resultados mais importantes é o seguinte teorema.

Teorema 1.1. *O anel dos polinômios definidos sobre um domínio de fatoração única também é domínio de fatoração única.*

A demonstração é feita por indução sobre o número das variáveis e pode ser encontrada em [VW] página 91. Em particular se K é um corpo, então $K[x_1, \ldots, x_r]$ é um domínio de fatoração única.

Vale destacar algumas propriedades dos polinômios homogêneos.

Proposição 1.2.

- *Todo polinômio de grau d em n variáveis pode ser escrito unicamente como uma soma $p_d + p_{d-1} + \cdots + p_0$, onde p_i é um polinômio homogêneo de grau i para todo $i = 0, \ldots, d$.*
- *$p \neq 0$ é homogêneo de grau d, se, e somente se, para todo $\lambda \in K$, $p(\lambda x_1, \ldots, \lambda x_r) = \lambda^d p(x_1, \ldots, x_r)$.*
- *Identidade de Euler: seja p homogêneo de grau d, então*

$$\sum_i x_i \frac{\partial p}{\partial x_i} = dp.$$

- *Os fatores de um polinômio homogêneo são homogêneos.*
- *A soma de dois polinômios homogêneos em pelo menos duas variáveis de graus consecutivos é irredutível.*
- *Um polinômio homogêneo em duas variáveis com coeficientes em $\mathbb{C}$ pode ser escrito como produto de polinômios homogêneos lineares, ou seja, polinômios homogêneos do tipo $ax + by$, onde $a, b \in \mathbb{C}$ são determinados unicamente a menos de $\frac{a}{b}$ ou $\frac{b}{a}$.*

Demonstração. As demonstrações são simples e deixadas como exercício. Vale observar que a última é de fato o teorema fundamental de álgebra para polinômios homogêneos em duas variáveis. □

Exercícios

1. Faça a demonstração da proposição 1.2.

2. Estenda a identidade de Euler para as derivadas parciais de ordem dois:
$$\sum_{i,j} x_i x_j \frac{\partial p}{\partial x_i \partial x_j} = d(d-1)p.$$
Generalize!

Substituição em Polinômios

Uma das operações bastante comuns com polinômios é *substituição* de um constante em lugar do indeterminado: dados $a \in K$ e

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x],$$

definimos $f(a) = a_0 + a_1 a + \cdots + a_n a^n \in K$. Pelas definições de adição e multiplicação, concluímos

$$(f+g)(a) = f(a) + g(a) \quad \text{e } (f \cdot g)(a) = f(a) \cdot g(a).$$

Em outras palavras, a substituição por constante define um homomorfismo de anéis entre $K[x]$ e K.

Um constante $a \in K$ é chamado de um *zero* ou *raiz* do polinômio f, se $f(a) = 0$. A seguir apresentaremos alguns resultados sobre os zeros das equações polinomiais.

Teorema 1.3. *Seja $a \in K$. Então o resto da divisão de f por $x - a$ é $f(a)$.*

Demonstração. Pelo algoritmo da divisão, $f(x) = (x-a)q(x) + r$, onde $r \in K$. Ao substituir $x = a$, concluímos $r = f(a)$. □

Uma consequência direta do teorema 1.3 é que se $a \in K$ é um zero de f, então $x - a$ é um fator de f. Outra consequência importante é obter uma cota superior para o número dos zeros de um polinômio.

Teorema 1.4. *O números dos zeros de um polinômio $f \neq 0$ é no máximo* $\deg f$.

Demonstração. A demonstração é feita por indução sobre $\deg f$ e é deixada como exercício. □

Naturalmente o processo de substituição e a definição de zero podem ser estendidos ao anel de polinômios em várias variáveis, bem como a seus corpos de frações.

1.2 Espaço Projetivo

Nos cursos elementares de geometria analítica, quando estudamos o problema de interseção de retas no plano cartesiano, observamos que retas paralelas não possuem ponto em comum. Em outras palavras, o sistema dado pelas equações de retas paralelas não possui solução. Este problema se repete se estudarmos a interseção da reta dada pela equação $x = 0$ e a hipérbole dada pela equação $xy = 1$. Essa falha do plano cartesiano pode ser resolvida se estudarmos estes problemas no plano projetivo construído a seguir.

Seja K um corpo. O *espaço projetivo* de dimensão n, $\mathbb{P}^n_K$, é o conjunto de todas as retas em K^{n+1} que passam pela origem. Lembrando que cada reta que passa pela origem é identificada por um de seus pontos diferente da origem, podemos interpretar $\mathbb{P}^n_K$ como o quociente

$$\frac{K^{n+1} \setminus \{\mathbf{0}\}}{\sim},$$

onde $\sim$ denota a relação de equivalência dos pontos que estão na mesma reta que passa pela origem:

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \Leftrightarrow$$

$$\exists \lambda \in K \setminus \{0\} \text{ tal que } (x_0, \ldots, x_n) = (\lambda y_0, \ldots, \lambda y_n).$$

Ou seja, um ponto em $\mathbb{P}^n_K$ é a classe de equivalência

$$(x_0 : \cdots : x_n) = \{(\lambda x_0, \ldots, \lambda x_n) \mid \lambda \in K \setminus \{0\}\}.$$

A seguir explicaremos como plano projetivo resolve as *falhas* do plano cartesiano. Primeiro observamos a aplicação

$$\begin{cases} \iota & : & K^n & \longrightarrow & \mathbb{P}^n_K \\ & & (a_0, \ldots, a_{n-1}) & \longmapsto & (a_0 : \cdots : a_{n-1} : 1) \end{cases}.$$

Claramente ι é injetiva, então ao identificar K^n com sua imagem em $\mathbb{P}^n_K$, podemos considerá-lo como um subconjunto do espaço projetivo, em outras palavras, $\mathbb{P}^n_K$ possui uma cópia de K^n. Lembrando a definição da relação de equivalência,

$$\iota(K^n) = \{(a_0 : \cdots : a_n) | a_n \neq 0\}.$$

Defina *pontos no infinito* como sendo $H_\infty := \mathbb{P}^n_K \setminus \iota(K^n)$. Então $\mathbb{P}^n_K = \iota(K^n) \cup H_\infty$. Existe também a aplicação

$$\begin{cases} \widetilde{\iota} & : & \iota(K^n) & \longrightarrow & K^n \\ & & (a_0 : \cdots : a_n) & \longmapsto & (\frac{a_0}{a_n}, \ldots, \frac{a_{n-1}}{a_n}) \end{cases}.$$

Observamos que $\iota \circ \widetilde{\iota} = \mathrm{id}_{\iota(K^n)}$ e $\widetilde{\iota} \circ \iota = \mathrm{id}_{K^n}$. Utilizando ι e $\widetilde{\iota}$ podemos visualizar os *objetos* de K^n em $\mathbb{P}^n_K$ e também olhar para os objetos no espaço projetivo como união de seus pontos no infinito e o complementar desses pontos que é chamado de sua parte *afim*. Nos exemplos a seguir veremos como podemos caminhar entre os espaços afim e projetivo e sanar as falhas do espaço afim.

Exemplo 1.5. *Seja l a reta dada ela equação $ax+by+c=0$ em K^2. Para obter $\iota(l)$ devemos fazer as mudanças $x \to \frac{x}{z}$ e $y \to \frac{y}{z}$. Então $\iota(l)$ é dada pela equação $ax+by+cz=0$ e seu único ponto no infinito é $(b : -a : 0)$. Portanto as retas paralelas afins $ax + by + c = 0$ e $ax + by + c' = 0$ possuem um ponto no infinito em comum, ou seja, se cruzam no espaço projetivo.*

Exemplo 1.6. *A hipérbole e a reta dadas pelas equações $xy = 1$ e $x = 0$ não se interceptam em K^2. A hipérbole em $\mathbb{P}^2_K$ é dada pela equação $xy = z^2$ e a reta por $x = 0$. A primeira possui dois pontos no infinito: $(1 : 0 : 0)$ e $(0 : 1 : 0)$, e a segunda apenas um: $(0 : 1 : 0)$. Portanto $(0 : 1 : 0)$ é o ponto de interseção da hipérbole e a reta.*

1.3 Curvas Algébricas Planas

Nesta seção apresentaremos alguns aspectos gerais e básicos da teoria de curvas algébricas planas. O objetivo é fazer uma breve introdução e estudar alguns conceitos e resultados que serão necessários no estudo de curvas elípticas. O corpo dos números complexos é denotado por $\mathbb{C}$, e o conjunto dos zeros de um polinômio f por $V(f)$.

Definição 1.7. *Um subconjunto $C \subseteq \mathbb{C}^2$ é chamado de uma curva algébrica afim, se existe $f \in \mathbb{C}[x,y] \setminus \mathbb{C}$ tal que*

$$C = V(f) = \{(a,b) \in \mathbb{C}^2 \mid f(a,b) = 0\}.$$

Nesse caso diremos que $f = 0$ é uma equação para a curva C.

Claramente para todo $\lambda \in \mathbb{C}$ e $k \in \mathbb{N}$, $V(f) = V(\lambda f) = V(f^k)$, ou seja, o polinômio f para uma curva dada C não é unicamente determinado. Vale observar que a situação no caso real é bem pior: por exemplo os polinômios $x^2 + y^2$ e $2x^2 + y^2$ possuem o mesmo conjunto de zeros em $\mathbb{R}^2$, no caso apenas $\{(0,0)\}$. A seguir veremos como podemos resolver o problema da escolha do polinômio. De fato observamos que trabalhar em $\mathbb{C}$ oferece mais *vantagens*. Lembramos que $\mathbb{C}$ é um corpo algebricamente fechado, ou seja, qualquer equação polinomial definida sobre $\mathbb{C}$ possui solução. Usando esse fato provaremos a seguinte proposição.

Proposição 1.8. *Se $C \subseteq \mathbb{C}^2$ é uma curva algébrica afim, então C e seu complementar, $\mathbb{C}^2 \setminus C$, possuem infinitos pontos.*

Demonstração. Seja $C = V(f)$. Escreva $f = a_0 + a_1 x + \cdots + a_n x^n$, onde $a_0, \ldots, a_n \in \mathbb{C}[y]$ e $a_n \neq 0$. Se $n = 0$, então pelo fato que $\mathbb{C}$ é algebricamente fechado $f = a_0$ possui raízes e

$$C = \{(a,b) \mid a \in \mathbb{C}, b \text{ é raiz de } f\}$$

possui infinitos pontos. Pelo fato que $f = a_0 \in \mathbb{C}[y]$ possui um número finito de raízes, $\mathbb{C}^2 \setminus C$ também possui infinitos pontos. Se $n > 0$, pelo fato que a_n possui apenas um número finito de raízes, existem infinitos $\alpha \in \mathbb{C}$ tais que $a_n(\alpha) \neq 0$, ou seja,

$$f(x,\alpha) = a_0 + a_1(\alpha) + \cdots + a_n(\alpha)x^n \in \mathbb{C}[x]$$

é de grau $n > 0$, logo possui raízes. Então

$$\{(\beta, \alpha) \mid a_n(\alpha) \neq 0, f(\beta, \alpha) = 0\} \subset C,$$

logo C possui infinitos pontos. Por outro lado como $f(x, \alpha)$ possui um número finito de raízes, $\{(\gamma, \alpha) \mid a_n(\alpha) \neq 0, f(\gamma, \alpha) \neq 0\}$ é infinito, portanto o complementar de C também é infinito. □

O próximo lema é a chave para fazer a *melhor* escolha para a equação de uma curva.

Lema 1.9. *(Study) Sejam $p, f \in \mathbb{C}[x, y]$, p irredutível e $V(p) \subset V(f)$. Então p é um divisor de f.*

Demonstração. Veja [F], p. 15. □

Observem que esse lema não vale para curvas em $\mathbb{R}^2$, basta lembrar do exemplo citado anteriormente: $V(x^2 + y^2) = V(2x^2 + y^2)$, mas nenhum é fator do outro. Uma consequência imediata do lema acima é o próximo corolário

Corolário 1.10. *Sejam $f, g \in \mathbb{C}[x, y]$ tais que $V(f) = V(g)$. Então f e g possuem os mesmos fatores irredutíveis.*

Demonstração. Dado um fator irredutível p de f, claramente $V(p) \subset V(f)$. Pela hipótese $V(p) \subset V(g)$, logo pelo lema 1.9, p é fator de g. Da forma análoga, todo fator de g será um fator de f. Então f e g possuem os mesmos fatores irredutíveis. □

Agora temos tudo para fazer a *melhor* escolha para a equação de uma curva algébrica. Seja $C \subseteq \mathbb{C}^2$ uma curva. Então existe $f \in \mathbb{C}[x, y]$ tal que $C = V(f)$. Pelo fato que $\mathbb{C}[x, y]$ é um domínio de fatoração única, existem únicos $f_1, \ldots, f_k \in \mathbb{C}[x, y]$ irredutíveis e $n_1, \ldots, n_k \in \mathbb{N}$ tais que $f = f_1^{n_1} \cdots f_k^{n_k}$. Claramente

$$V(f) = V(f_1 \cdots f_k) = V(\lambda \cdot f_1 \cdots f_k),$$

para todo $\lambda \in \mathbb{C}^*$. Observe que a relação

$$f \sim g \iff \exists \lambda \in \mathbb{C}^*, \quad f = \lambda \cdot g,$$

é uma relação de equivalência em $\mathbb{C}[x, y]$. Pela unicidade dos fatores irredutíveis de f, o polinômio $f_1 \cdots f_k$ é o de menor grau que define a curva C módulo a relação de equivalência definida acima.

Então para definir uma curva, basta tomarmos o polinômio de menor grau (polinômio minimal) módulo a relação de equivalência acima. Pelos argumentos feitos, esse polinômio é de fato o produto dos fatores irredutíveis de qualquer polinômio que define a curva. Claramente $V(f) = V(f_1) \cup \cdots \cup V(f_k)$. As curvas $V(f_i), i = 1, \ldots, n$, são chamadas de *componentes* de $V(f)$. Se $k = 1$, diremos que a curva é *irredutível*. Tomando o polinômio minimal para definir uma curva, podemos definir um dos mais importantes *invariantes* de uma curva algébrica afim:

Definição 1.11. *Seja $C = V(f) \subset \mathbb{C}^2$, onde f é o polinômio minimal. Então o grau de C é definido por* $\deg C := \deg f$.

Curvas de grau um, dois, três,... são chamadas de retas, cônicas, cúbicas, ...

Como observamos anteriormente, o espaço projetivo é um ambiente mais rico do que espaço afim, por esse motivo estenderemos o conceito de curvas algébricas ao espaço projetivo.

Pelo primeiro item da proposição 1.2, todo $f \in \mathbb{C}[x, y]$ pode ser escrito como $f = \sum_{i=0}^{d} f_i$, onde $d = \deg f$ e cada f_i é um polinômio homogêneo de grau i. A *homogeneização* de f é o polinômio homogêneo, também de grau d,

$$f^*(x, y, z) := \sum_{i=0}^{d} z^{d-i} f_i(x, y).$$

Claramente $f^*(x, y, 1) = f(x, y)$. Reciprocamente, dado um polinômio homogêneo F, definimos sua desomogeneização com respeito a z por

$$F_*(x, y) := F(x, y, 1).$$

Observe que $\deg F_* \leq \deg F$. Por exemplo no caso de $F = xy + z^2$, os graus permanecem iguais; mas no caso de $F = xyz$, $\deg F_* = 2 < \deg F = 3$.

Proposição 1.12. *Sejam $f, g \in \mathbb{C}[x,y]$, e $F, G \in \mathbb{C}[x,y,z]$ homogêneos. Então*

1. $(fg)^* = f^* g^*$.
2. $(FG)_* = F_* G_*$.
3. $(f^*)_* = f$.
4. $z^n (F_*)^* = F$, *onde* $n = \deg F - \deg F_*$.

Demonstração. Exercício! □

Usando os dois primeiros itens da proposição acima, concluímos:

Corolário 1.13. *Seja $f \in \mathbb{C}[x,y]$. Então f é irredutível, se, e somente se f^* é irredutível.*

Dada uma curva algébrica afim $C = V(f)$, seja $F = f^*$. O conjunto $\overline{C} = V(F) \subset \mathbb{P}^2_{\mathbb{C}}$ é chamado de *fecho projetivo* de C. Claramente $C = \overline{C} \cap \mathbb{C}^2$. Como veremos na próxima definição, $\overline{C}$ é de fato uma curva *projetiva*.

Definição 1.14. *Um conjunto $X \subset \mathbb{P}^2_{\mathbb{C}}$ é chamado de uma curva plana projetiva se existe $F \in \mathbb{C}[x,y,z] \setminus \mathbb{C}$ homogêneo tal que $X = V(F)$.*

Igual ao caso afim, no caso projetivo também escolheremos o polinômio minimal módulo da relação de equivalência que identifica dois polinômios se um for múltiplo constante não nulo do outro. Dessa forma podemos definir a grau da curva como sendo o grau do polinômio minimal que a define. Então de fato um fecho projetivo de uma curva afim define uma curva projetiva(de mesmo grau), e reciprocamente dada uma curva projetiva $V(F)$, o conjunto $V(F_*)$, se F_* não for constante, define uma curva afim. Pelo item 4 da proposição 1.12, F_* é constante, se, e somente se, o F define a reta no infinito. O conjunto $V(F_*)$ é chamado de *parte afim* ou *pontos a distância finita* de $V(F)$. Os *pontos no infinito* da curva são dados pelas soluções da equação $F(x,y,0) = 0$. Lembrando a definição do espaço projetivo e a aplicação $\iota : \mathbb{C}^2 \to \mathbb{P}^2_{\mathbb{C}}$, podemos dizer que cada curva projetiva pode ser escrita como a união de sua parte afim com seus pontos no infinito. Vale observar que o conjunto dos pontos no infinito é finito.

Exemplo 1.15. *Todas as cúbicas:* $y^2z = x^3$, $y^2z = x^2(x+z)$ *e* $y^2z = x(x-z)(x-2z)$ *possuem um único ponto no infinito:* $(0:1:0)$. *Suas partes afins, ou seja, as cúbicas afins correspondentes são:* $y^2 = x^3$, $y^2 = x^2(x+1)$ *e* $y^2 = x(x-1)(x-2)$.

Exercício

Sejam C uma curva plana projetiva. Então o conjunto dos pontos no infinito de uma curva plana projetiva é finito.

Nesse momento não podemos deixar de pelo menos citar um dos resultados mais importantes da teoria das curvas planas projetivas. Esse resultado, conhecido por teorema de Bézout, é de fato a generalização da primeira parte do exercício acima no caso de curvas planas projetivas. Esse teorema afirma que sob certas condições o número de pontos de interseção de duas curvas planas projetivas é igual ao produtos de seus graus. Mas alguns casos particulares, como interseção de uma reta ou uma cônica com uma curva de grau d, podem ser demonstrados facilmente.

Teorema 1.16. *(Bézout) Seja* $C \subset \mathbb{P}^2_{\mathbb{C}}$ *uma curva de grau* d. *Uma reta (respectivamente uma cônica) que não for componente de* C, *possui* d *(respectivamente* $2d$*) pontos em comum com* C.

Demonstração. Seja $C = V(F)$, onde F é um polinômio homogêneo de grau d. Uma reta é dada por uma equação do tipo $ax+by+cz = 0$. Sem perda de generalidade, podemos supor $c \neq 0$. Para determinar os pontos de interseção da reta com C, fazemos a substituição $z = -\frac{a}{c}x - \frac{b}{c}y$ na equação de C. Dessa forma obtemos um polinômio homogêneo de grau d em duas variáveis x e y. As raízes dessa equação determinam os pontos de interseção da reta com a curva C. Pelo último item da proposição 1.2 sabemos que esse polinômio possui d raízes, portanto a reta e C possuem d pontos em comum.
Dada uma cônica C, sabemos que C é projetivamente equivalente à cônica dada pela equação $y^2 = xz$, que por sua vez pode ser parametrizada por $x = u^2, y = uv, z = v^2$. Fazendo essas substituições na equação da curva obtemos um polinômio homogêneo em duas variáveis u e v de grau $2d$. Novamente pela proposição 1.2, esse

polinômio possui $2d$ raízes, portanto a cônica e C possui $2d$ pontos em comum.
Observem que em ambos os casos o polinômio obtido após as substituições não é polinômio nulo pois a reta e a cônica não são componentes de C.

□

1.4 Pontos Singulares e Suaves

Sejam $C = V(f)$ uma curva afim e $P(a,b) \in C$. Sabemos que a equação da reta tangente a C no ponto P é dada por

$$\frac{\partial}{\partial x}f(P)(x-a) + \frac{\partial}{\partial y}f(P)(y-b) = 0.$$

Da forma análoga, no caso de curvas projetivas, a equação da reta tangente num ponto $P(a:b:c)$ é dada por

$$\frac{\partial}{\partial x}F(P)(x-a) + \frac{\partial}{\partial y}F(P)(y-b) + \frac{\partial}{\partial z}F(P)(z-c) = 0,$$

onde F é a equação da curva. Claramente essas equações representam de fato retas, se as derivadas parciais não se anulam ao mesmo tempo. O que não é impossível. Por exemplo no caso da cúbica $y^2 = x^3$ as derivadas parciais se anulam na origem.

Definição 1.17. *Um ponto $(a:b:c) \in C = V(F)$ é dito um ponto singular se $\frac{\partial}{\partial x}F(a:b:c) = \frac{\partial}{\partial y}F(a:b:c) = \frac{\partial}{\partial z}F(a:b:c) = 0$. Se C tiver pelo menos um ponto singular, será chamada de uma curva singular, caso contrário será uma curva suave ou não singular.*

Vale observar que o conjunto dos pontos singulares de uma curva plana projetiva é finito. De fato cotas superiores para o número dos pontos singulares em termos do grau da curva podem ser obtidos facilmente. Por exemplo pelo teorema de Bézout é fácil obter a cota superior $d(d-1)$, onde d é o grau da curva, para o número dos pontos singulares. Uma cota melhor é $\frac{d(d-1)}{2}$. Para ver resultados nesse sentido e uma discussão mais *geométrica* sobre pontos singulares, recomendamos fortemente que o leitor veja [V] ou [F].

Exercícios

1. Determine o(s) ponto(s) singular(es) das cúbicas $V(z(x^2 - y^2))$ e $V(xyz)$.

2. Sejam $f \in \mathbb{C}[x]$, $m \in \mathbb{N}$ e $C_m = V(y^m - f(x))$. Mostre que:

   - C_1 é suave.
   - $C_m, m \geq 2$ é singular, se, e somente se, f possui raízes múltiplas. Em particular, se $\deg f = 3$, então C_m possui no máximo um ponto singular. Conclua que existem curvas suaves e singulares de qualquer grau.

3. - Seja $F = G \cdot H$ um polinômio redutível. Mostre que os pontos de $V(G) \cap V(H)$ são pontos singulares de $V(F)$.
   - Sejam C e D curvas planas projetivas sem componentes em comum. Mostre

     $$\mathrm{Sing}(C \cup D) = \mathrm{Sing}(C) \cup \mathrm{Sing}(D) \cup (C \cap D),$$

     onde $\mathrm{Sing}(\cdot)$ representa o conjunto dos pontos singulares.
   - Sabemos que uma curva plana projetiva irredutível de grau d possui no máximo $\frac{d(d-1)}{2}$ pontos singulares. Use esse fato para obter essa cota em geral.

4. Seja $f = F+G$, onde $F, G \in \mathbb{C}[x, y]$ são polinômios homogêneos não lineares de graus distintos. Mostre que os pontos singulares de $V(f)$ são dados por $F = G = 0$. Além disso, se F e G não tiverem fatores em comum, então $(0, 0)$ é o único ponto singular de $V(f)$. (Dica: Use a fórmula de Euler)

5. Mostre que as cúbicas de Steiner dadas pelos polinômios

   $$F_{\mu,\lambda} = \mu(x^3 + y^3 + z^3) + \lambda xyz$$

   são singulares, se, e somente se, $\mu = 0$ ou $\lambda^3 = -1$.

6. Mostre que as cúbicas

   $$xy^2 + yz^2 + zx^2 + yx^2 + zy^2 + xz^2 + kxyz = 0$$

   são suaves, exceto nos casos em que $k = 2, 3, 6$.

Capítulo 2

Cúbicas

Este capítulo é dedicado a fazer uma introdução breve às cúbicas planas projetivas. O foco principal é o caso de cúbicas irredutíveis. Veremos que seus pontos possuem a estrutura de um grupo abeliano, e que no caso suave esse grupo é finitamente gerado. Comentaremos vários resultados sobre esse grupo. A maioria das demonstrações precisa de estudos um pouco mais avançados e por isso elas não serão apresentadas. Mas suas importância e utilidade são esclarecidas por meio dos exemplos. No caso singular mostraremos que o grupo não é finitamente gerado.

Lembramos que, por definição, uma cúbica plana projetiva é uma curva de grau três, ou seja, uma curva definida por um $f \in \mathbb{C}[x, y, z]$ homogêneo de grau três. Como um polinômio homogêneo de grau três possui 9 coeficientes, vale a pena pensarmos se há uma maneira de *simplificá-lo*, ou seja, obter formas mais simples de f por meio de mudanças de coordenadas. Lembre-se que uma mudança de coordenadas (projetiva) em $\mathbb{P}^2_{\mathbb{C}}$ é uma aplicação $\mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^2_{\mathbb{C}}$ induzida por uma matriz invertível de ordem 3. Diremos que $X_1, X_2 \subset \mathbb{P}^2_{\mathbb{C}}$ são projetivamente equivalentes, se existe uma mudaça de coordenadas projetiva T tal que $T(X_1) = X_2$.

Exemplo 2.1. *As cônicas projetivas dadas pelas equações* $x^2+y^2+z^2=0$ *e* $y^2=xz$ *são projetivamente equivalentes por meio da mudança de coordenadas dada por* $\begin{pmatrix} i & 0 & -1 \\ 0 & 1 & 0 \\ i & 0 & 1 \end{pmatrix}$, *isto é:*

$$(x:y:z)\mapsto(ix-z:y:ix+z).$$

2.1 Classificação de Cúbicas

Para a classificação das cúbicas, separaremos os casos redutível e irredutível. Se f for redutível, dependendo de números dos fatores, teremos os seguintes casos para uma cúbica redutível : união de uma reta com uma cônica e união de três retas. Cada um desses casos possui várias configurações, como veremos na figura 2.1. Pelo exercício 3 da seção 1.4, todas as cúbicas redutíveis são singulares.

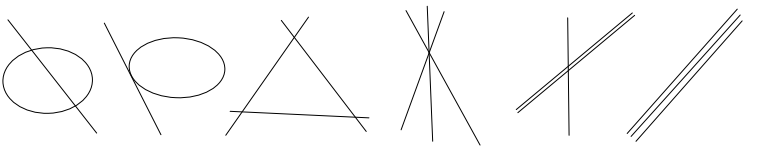

Figura 2.1: Cúbicas Redutíveis

No caso irredutível a situação é um pouco diferente. Como veremos nos próximos resultados, a menos de mudanças de coordenadas projetivas, existem apenas uma cúbica no caso suave e duas no caso singular. A classificação obtida vale para qualquer subcorpo $L\subseteq\mathbb{C}$.

Teorema 2.2. *Sejam $L \subseteq \mathbb{C}$ um corpo e $F \in L[x, y, z]$ irredutível de grau 3 tal que $C = V(F)$ é suave. Então C é projetivamente equivalente à cúbica $C_\lambda : y^2z = G(x, z)$, onde $G \in \mathbb{C}[x, z]$ é homogêneo de grau três sem fatores múltiplos.*

Em particular, se $L = \mathbb{C}$, pelo fato que $\mathbb{C}$ é algebricamente fechado, $G = x(x - z)(x - \lambda z)$, onde $\lambda \in \mathbb{C} \setminus \{0, 1\}$.

A demonstração desse teorema, mesmo nos casos mais gerais em que a característica do corpo é positiva, pode ser encontrada em [G] ou [H]. De fato o teorema 2.2 vale quando char$L \neq 2$. No caso de char$L = 2$, conseguimos chegar apenas a seguinte forma: $G = xz^2 + ay^2z + bxyz + y^3 + cxz^2$. O único ponto no infinito de uma cúbica projetiva suave dada no teorema 2.2 é $\mathcal{O} = (0 : 1 : 0)$, e sua parte afim é dada pela equação $y^2 = f(x)$, onde f é um polinômio de grau 3 em uma variável com raízes distintas. Esta forma de apresentar uma cúbica afim suave é conhecida por sua *forma de Weierstrass*. A forma apresentada no teorema 2.2 é conhecida como *forma de Legendre*. Vale observar que nesse caso a cúbica poderá ter uma ou duas componentes reais, ou seja, ao esboçar o gráfico da cúbica no plano cartesiano ocorrerá um dos casos mostrados na Figura 2.2. Esses casos acontecem quando f possui apenas uma raiz real(como C_1) ou três raízes reais distintas (como C_2), caso contrário, teremos as cúbicas singulares (lembre-se do exercício 2 da seção 1.4).

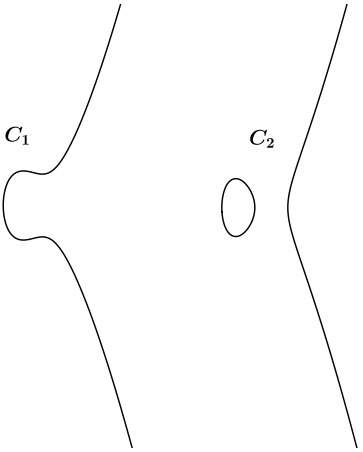

Figura 2.2: Cúbicas com uma ou duas componentes reais

Naturalmente podemos perguntar quando as cúbicas suaves C_λ, $\lambda \in L \setminus \{0,1\}$ são projetivamente equivalentes. A resposta é dada no seguinte teorema.

Teorema 2.3. *C_λ e $C_{\lambda'}$ são projetivamente equivalentes, se, e somente se, $\lambda' \in M_\lambda := \{\lambda, \lambda^{-1}, 1-\lambda, (1-\lambda)^{-1}, \lambda(\lambda-1)^{-1}, \lambda^{-1}(\lambda-1)\}$.*

A função j definida por $j(\lambda) := 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$ é invariante em relação às substituições de λ por valores em M_λ. Portanto é um invariante da classe das curvas projetivamente equivalentes a C_λ. O fator 2^8 é apenas um fator normalizador. Em geral escrevemos $j(C) = j(\lambda)$ para todas as cúbicas da classe C_λ. Esse número é chamado de *invariante* j da cúbica (suave) C. Pela invariância de j na classe das cúbicas suaves projetivamente equivalentes, o mapa

$$j : \{_{\text{classe das cúbicas suaves projetivamente equivalentes}}\} \to L$$

definido por $C \mapsto j(C)$ está bem definido e é injetivo. A seguir verificamos a sobrejetividade.
Seja $l \in L$. A equação de grau 6,

$$2^8(\lambda^2 - \lambda + 1)^3 - l\lambda^2(\lambda - 1)^2 = 0$$

possui uma solução $\lambda_0 \neq 0, 1$, e todos os elementos de M_{λ_0} também são soluções. Se $\#M_{\lambda_0} = 6$, obtivemos todas as soluções da equação acima. Caso contrário teremos as seguintes possibilidades:

$$M_{-1} = M_{\frac{1}{2}} = M_2 = \left\{-1, \frac{1}{2}, 2\right\}; \;\; M_\rho = M_{\rho^{-1}} = \{\rho, \rho^{-1}\}, \;\; \rho = \frac{1+\sqrt{-3}}{2}.$$

No primeiro caso, $l = 2^6 3^3$; e no segundo, $l = 0$. Em todos os casos M_{λ_0} é o conjunto de todas as soluções da equação.

A bijetividade de j resolve o problema de classificação de cúbicas suaves no sentido de que, para cada elemento de L, a menos de equivalência projetiva, existe uma única cúbica suave. No caso singular temos *bem menos* casos, como veremos no seguinte teorema.

Teorema 2.4. *Sejam $L \subseteq \mathbb{C}$ um corpo. Uma cúbica singular definida sobre L é projetivamente equivalente à cúbica $y^2z = x^3$ ou $y^2z = x^2(x+z)$.*

Veja [G] ou [H] para sua demonstração. Observamos que em cada um dos casos no teorema 2.4, existe apenas um ponto singular: o ponto singular no caso de $C_1 : y^2z = x^3$ é chamado de *cúspide*; e no caso de $C_2 : y^2z = x^2(x+z)$ é chamado de *nó*, veja as cúbicas C_1 e C_2 na Figura 2.3.

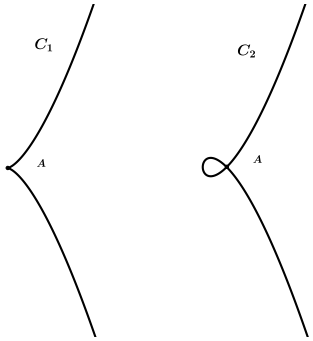

Figura 2.3: Cúbicas Cuspidal e Nodal

Cúbicas suaves aparecem em diversas áreas de matemática e ciência como teoria dos números, análise complexa, criptografia e física clássica

e moderna. Foram utilizadas para demonstrar o último teorema de Fermat. Para ver um pouco de ubiquidade das cúbicas suaves, veja [S2]. Um dos problemas onde estas curvas aparecem é calcular comprimento de uma elipse. Este problema envolve integrais definidas de funções do tipo $\sqrt{g(x)}$, onde g é um polinômio de grau 3 ou 4. Essas integrais, chamadas de *integrais elípticas*, em geral não podem ser calculadas em termo de funções conhecidas. Pela relação próxima entre as integrais elípticas e cúbicas suaves, estas cúbicas são chamadas de curvas elípticas.

Definição 2.5. *Uma cúbica suave definida sobre o corpo K é chamada de uma curva elíptica (sobre o corpo K).*

Nosso foco principal é estudar curvas elípticas sobre $\mathbb{Q}$. Pelo teorema 2.2, uma curva elíptica sobre $\mathbb{Q}$ é

$$E(\mathbb{Q}) := \{(x : y : z) \in \mathbb{P}^2_{\mathbb{Q}} | y^2 z = x(x - z)(x - \lambda z), \lambda \in \mathbb{Q} \setminus \{0, 1\}\}.$$

Lembrando que $\mathcal{O} = (0 : 1 : 0)$ é seu único ponto no infinito, escrevemos $E(\mathbb{Q}) = C_f(\mathbb{Q}) \cup \{\mathcal{O}\}$, onde $C_f(\mathbb{Q})$ é sua parte afim dada por $f \in \mathbb{Q}[x]$ de grau 3 com raízes distintas.

2.2 Operação entre os Pontos

Nesta seção definiremos uma operação entre os pontos não singulares, $\mathcal{S}_\mathcal{C}$, de uma cúbica irredutível $\mathcal{C}$ em $\mathbb{P}^2_{\mathbb{C}}$ e mostraremos que esse conjunto munido dessa operação possui estrutura de um grupo abeliano. A defnição é baseada no fato de que uma reta e uma cúbica possuem três pontos em comum (exercício da seção 1.3).

Sejam $P, Q \in \mathcal{S}_\mathcal{C}$. Considere a reta que passa por P e Q e obtenha o terceiro ponto de interseção dessa reta com a cúbica, denotado por $R := P * Q$. É fácil verificar[1] que $R \in \mathcal{S}_\mathcal{C}$. A operação $*$ possui as seguintes propriedades:

Lema 2.6. *Sejam $P, Q, R, S \in \mathcal{S}_\mathcal{C}$. Então*

1. $P * Q = Q * P$;

[1] Para isso tem de aprender um pouco sobre multiplicidade de interseção.

2. $(P * Q) * P = Q$*;*

3. $((P * Q) * R) * S = P * ((Q * S) * R)$.

Demonstração. As duas primeiras são consequências diretas da definição. Para demonstrar *3*, devemos usar o seguinte teorema, conhecido por *teorema de nove pontos associados*[2]: *sejam* C_1 *e* C_2 *duas cúbicas sem componentes em comum e* $P_1, \ldots, P_9$ *seus pontos de interseção. Então qualquer outra cúbica que passe por* $P_1, \ldots, P_8$*, passa também por* P_9.

Sejam X o lado esquerdo de *3*; e Y o lado direito. Veja a Figura 2.4. As cúbicas $L_1L_2L_3$ e $M_1M_2M_3$ passam pelos nove pontos acima e $\mathcal{C}$ passa por oito desses nove, portanto passa pelo nono ponto, ou seja, $X = Y$. □

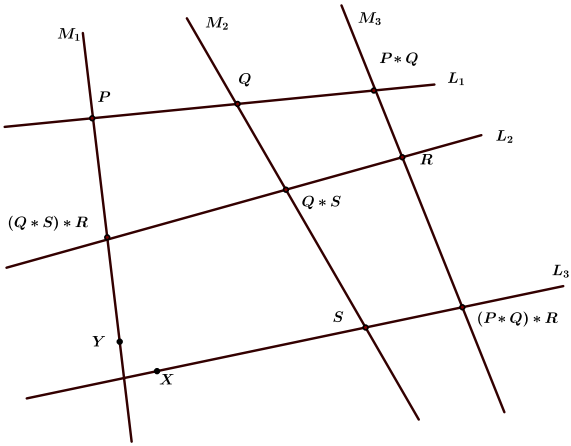

Figura 2.4: Propriedade 3

Agora escolha um ponto não singular de $\mathcal{C}$ como O e defina

$$P + Q := (P * Q) * O.$$

Usando o lema 2.6 podemos verificar facilmente que

[2]Para o caso geral desse teorema, veja [ST, p. 240].

Proposição 2.7. *$(\mathcal{S}_\mathcal{C}, +)$ é um grupo abeliano cujo elemento neutro é O e o inverso de P é $-P := P * (O * O)$.*

Pela classificação das cúbicas irredutíveis, o ponto no infinito é não singular, então podemos escolher esse ponto para definir a operação acima. Claramente a definição da operação depende da escolha do ponto O, mas os grupos obtidos são isomorfos.

Teorema 2.8. *(Poincaré) Sejam $\mathcal{C}$ uma cúbica irredutível, $\mathcal{O}$ seu ponto no infinito e $\mathcal{P} \in \mathcal{S}_\mathcal{C}$. Denote por $+'$ a operação definida em $\mathcal{S}_\mathcal{C}$ tomando $\mathcal{P}'$ como o ponto fixo. Então $A +' B = A + B - \mathcal{P}'$, para todo $A, B \in \mathcal{S}_\mathcal{C}$. Em particular $A \overset{\Phi}{\mapsto} A - \mathcal{P}'$ define um isomorfismo entre $(\mathcal{S}_\mathcal{C}, +')$ e $(\mathcal{S}_\mathcal{C}, +)$.*

Demonstração. A igualdade é obtida usando o item *3* do lema 2.6:

$$\begin{aligned} A + B - \mathcal{P}' &= (((A * B) * \mathcal{P}) * (-\mathcal{P}')) * \mathcal{P} \\ &= (A * B) * ((\mathcal{P} * \mathcal{P}) * (-\mathcal{P}')) \\ &= (A * B) * ((-\mathcal{P}') * (\mathcal{P} * \mathcal{P})) \\ &= (A * B) * \mathcal{P}' \\ &= A +' B. \end{aligned}$$

Claramente Φ é uma bijeção. Utilizando a igualdade entre as operações:

$$\begin{aligned} \Phi(A +' B) &= \Phi(A + B - \mathcal{P}') \\ &= A + B - \mathcal{P}' - \mathcal{P}' \\ &= A - \mathcal{P}' + B - \mathcal{P}' \\ &= \Phi(A) + \Phi(B). \end{aligned}$$

□

Tomando o ponto no infinito como o ponto fixo obteremos algumas vantagens, por exemplo fica mais simples determinar o inverso de um ponto. Nesse caso $\mathcal{O} * \mathcal{O} = \mathcal{O}$, portanto $-P = P * \mathcal{O}$.

Proposição 2.9. *Tome o ponto no infinito, $\mathcal{O}$, como o ponto fixo. Sejam $P, Q, R \in \mathcal{S}_\mathcal{C}$. Então*

1. *$P + Q + R = \mathcal{O}$, se, e somente se, P, Q, R são colineares;*

2. *$P \neq \mathcal{O}$ é de ordem dois, i.e, $2P = \mathcal{O}$, se, e somente se, a reta tangente no ponto P passa por $\mathcal{O}$.*

Demonstração. Para o primeiro item, observem

$$\begin{aligned} P+Q+R=\mathcal{O} \quad &\iff \quad P+Q=-R \\ &\iff \quad (P*Q)*\mathcal{O}=R*\mathcal{O} \\ &\iff \quad ((P*Q)*\mathcal{O})*\mathcal{O}=(R*\mathcal{O})*\mathcal{O} \\ &\overset{\text{lema 2.6}}{\iff} \quad P*((Q*\mathcal{O})*\mathcal{O})=-(R*\mathcal{O}) \\ &\iff \quad P*(-(Q*\mathcal{O}))=-(-R) \\ &\iff \quad P*Q=R, \end{aligned}$$

ou seja, P, Q, R são colineares.
O segundo item é de fato um caso particular do primeiro. Observem que a reta tangente no ponto P passa por $\mathcal{O}$, se, e somente se, $P, P, \mathcal{O}$ são colineares. Isso por sua vez é equivalente a $P + P + \mathcal{O} = \mathcal{O}$, ou, $2P = \mathcal{O}$. □

Outro fato que deve ser observado é sobre grupos associados às cúbicas projetivamente equivalentes.

Proposição 2.10. *Duas cúbicas irredutíveis são projetivamente equivalentes, se, e somente se, seus grupos associados são isomorfos.*

Demonstração. Veja [G]. □

Exercício

- Prove o teorema de nove pontos associados:
  - Sejam l uma reta projetiva e F uma forma de grau d. Se $F_{|_l} \equiv 0$, então F é divisível por l.
  - Demonstre a afirmação anterior, substituindo a reta por uma cônica.
  - Agora demonstre o teorema.

2.3 Fórmulas Explícitas

Nesta seção obteremos fórmulas explícitas para a operação definida em $\mathcal{S}_{\mathcal{C}}$. Pelos teorema 2.8 e proposição 2.10, podemos considerar a cúbica dada pela equação $y^2z = F(x,z) \in \mathbb{C}[x,z]$, onde F é uma forma de grau 3 e o ponto fixo como seu único ponto no infinito, $\mathcal{O}(0:1:0)$. Nesse caso a parte afim é dada por

$$C_f := \{(x,y)|y^2 = f(x) = x^3 + ax^2 + bx + c\}.$$

Como $\mathcal{O}$ é um ponto não singular e além disso é o elemento neutro de $\mathcal{S}_{\mathcal{C}}$, para obter as fórmulas basta considerar $P_1(x_1,y_1), P_2(x_2,y_2) \in C_f$.

Sejam L a reta que passa por P_1 e P_2 e x_3, y_3 as coordenadas de $P_1 * P_2$.

Se $x_1 \neq x_2$, escrevemos $L : y = mx + n$. Neste caso as primeiras coordenadas dos pontos de $L \cap C_f$ satisfazem a equação $(mx+n)^2 = f(x)$ que é uma equação polinomial de grau 3. Utilizando a relação entre a soma das raízes da equação

$$x^3 + (a - m^2)x^2 + (b - 2mn)x + (c - n^2) = 0,$$

concluímos $x_1 + x_2 + x_3 = m^2 - a$, ou, $x_3 = m^2 - a - x_1 - x_2$ e portanto $y_3 = mx_3 + n$. Seguindo o segundo passo para obter $P_1 + P_2$, concluímos $P_1 + P_2 = (x_3, -y_3)$.

No caso em que $x_1 = x_2$, devemos considerar os casos $P_1 = P_2$ e $P_1 \neq P_2$. No primeiro caso L é a reta tangente a C_f. Se $y_1 \neq 0$, então $m = \frac{3x_1^2 + 2ax_1 + b}{2y_1}$ e $n = y_1 - mx_1$. Neste caso $x_3 = m^2 - a - 2x_1$, logo $y_3 = mx_3 + n$ e $P_1 + P_1 = (x_3, -y_3)$. Se $y_1 = 0$, então $P_1 * P_1 = \mathcal{O}$, portanto $P_1 + P_1 = \mathcal{O}$. Quando $P_1 \neq P_2$, a equação de L é $x = x_1$, portanto $P_1 * P_2 = \mathcal{O}$ e $P_1 + P_2 = \mathcal{O}$.

Usando essas fórmulas podemos verificar a associatividade sem utilizar o teorema de nove pontos associados. Outra consequência é o seguinte.

Proposição 2.11. *Sejam $K \subseteq \mathbb{C}$ um corpo e $C_f(K) := \{(x,y) \in C_f | x,y \in K\}$. Então $(C_f(K) \cup \{\mathcal{O}\}, +)$ é um subgrupo de $(\mathcal{S}_{\mathcal{C}}, +)$. Em particular $(E(\mathbb{Q}), +)$ é um grupo abeliano.*

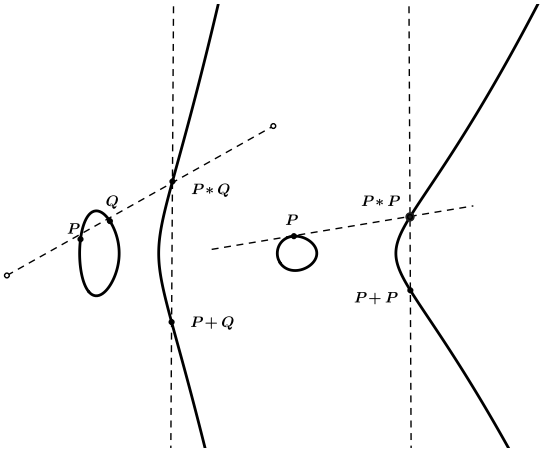

Figura 2.5: Operação

A seguir faremos alguns exemplos os quais nos darão motivação para estudar os resultados apresentados na próxima seção. Os dois primeiros envolvem o último teorema de Fermat: a equação $u^n + v^n = w^n, n \geq 3$, possui apenas soluções inteiras triviais, ou seja, $(u, v, w) \in \mathbb{Z}^3$ tal que $uvw = 0$.

Exemplo 2.12. *Por meio de uma série de mudança de variáveis, podemos transformar a equação* $u^3 + v^3 = w^3$ *na cúbica* $y^2z = x^3 - \frac{27}{4}z$, *chamada de* cúbica de Fermat, *veja [KA, Cap. III]. As soluções triviais de* $u^3 + v^3 = w^3$ *correspondem a* $\mathcal{O}$, $P_1(3, \frac{9}{2})$ *e* $P_2(3, -\frac{9}{2})$. *Isto é o grupo dos pontos racionais de* $y^2z = x^3 - \frac{27}{4}z$ *possui apenas* 3 *elementos, portanto é isomorfo a* $\mathbb{Z}_3$. *Claramente* $P_1 + P_2 = \mathcal{O}$ *e* $P_1 * P_1 = P_1$, *portanto* $P_1 + P_1 = P_2$, *ou,* $3P_1 = \mathcal{O}$.

Exemplo 2.13. *O caso quártica do último teorema de Fermat se transforma em* $y^2 = x^3 - 4x$. *Neste caso as soluções triviais correspondem a* $\{\mathcal{O}, (0,0), (2,0), (-2,0)\}$. *Como todos estes pontos possuem ordem no máximo dois,* $E(\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. *Isto acontece para todas as curvas elípticas* $y^2 = x^3 - n^2x$, *onde* n *é um inteiro livre de quadrados, veja [KA, p. 110].*

Exemplo 2.14. *Considere* $y^2 = x^3 - x + \frac{1}{4}$ *e* $P = (0, \frac{1}{2})$. *Então* $2P = (1, -\frac{1}{2})$, $3P = (1, \frac{1}{2})$, $6P = (2, -\frac{5}{2}) \neq \mathcal{O}$, $8P \neq \mathcal{O}$ *e* $12P = (\frac{21}{25}, -\frac{13}{250}) \neq \mathcal{O}$. *Pelo teorema 2.16, P possui ordem infinita, portanto neste caso* $E(\mathbb{Q})$ *é um grupo infinito.*

Exercício

- Considere a cúbica $y^2 = x^3 - x$. Sejam $P_1(0,0)$ e $P_2(1,0)$. Determine $P_1 + P_2$.

2.4 Teoremas de Mordell-Weil, Nagell-Lutz e Mazur

O objetivo desta seção é estudar, $E(\mathbb{Q})$, o grupo dos pontos racionais de uma curva elíptica. Nos exemplos no final da seção anterior vimos que $E(\mathbb{Q})$ pode ser finito ou infinito. Nesta seção apresentaremos alguns resultados gerais sobre $E(\mathbb{Q})$. O primeiro é o teorema de Mordell-Weil que afirma $(E(\mathbb{Q}), +)$ é um grupo (abeliano) finitamente gerado. Esse resultado foi apresentado por Poincaré como uma conjectura por volta de 1900 e somente cerca de duas décadas depois foi demonstrado por Mordell. Infelizmente não podemos apresentar os pré-requisitos necessários para demonstrar esse teorema. Em [ST] podemos encontrar uma demosntração com uma hipótese adicional: *assumir que existe um ponto de ordem dois.* Em seguida apresentaremos os teoremas de Mazur e Nagell-Lutz. Esses teoremas fornecem informações mais precisas sobre a estrutura de $E(\mathbb{Q})$.

Teorema 2.15. *(Mordell-Weil) O grupo dos pontos racionais de uma curva elíptica é um grupo abeliano finitamente gerado.*

Ou seja, existe $\{P_1, \ldots, P_r\} \subset E(\mathbb{Q})$ tal que todo $P \in E(\mathbb{Q})$ pode ser escrito como $n_1P_1 + \cdots + n_rP_r$, para únicos $n_1, \ldots, n_r \in \mathbb{Z}$. Pelo teorema de estrutura de grupos abelianos finitamente gerados (veja, por exemplo [L, p. 46]),

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r,$$

onde $E(\mathbb{Q})_{\text{tor}}$ representa o subgrupo dos pontos de ordem finita, chamado de *grupo de torção* e r é chamado do *posto de* $E(\mathbb{Q})$. Pelo fato de que $E(\mathbb{Q})$ é abeliano e finitamente gerado, $E(\mathbb{Q})_{\text{tor}}$ é finito. Cada uma dessas partes pode ser trivial. Por exemplo no caso de cúbica de Fermat o posto é zero; e no caso de $y^2z = x^3 + 2z^3$ não existe nenhum ponto de ordem finita além de $\mathcal{O}(0 : 1 : 0)$. Esses exemplos fazem pensar quais são os grupos finitos que podem aparecer como $E(\mathbb{Q})_{\text{tor}}$, bem como são as possibilidades do posto e se há técnicas para determiná-los explicitamente. No caso de $E(\mathbb{Q})_{\text{tor}}$ um resultado de Mazur determina todas as possibilidades, em particular fornece uma cota para $\#E(\mathbb{Q})_{\text{tor}}$.

Teorema 2.16. *(Mazur) Se $E(\mathbb{Q})_{\text{tor}}$ não for trivial, então é isomorfo a um destes 14 grupos: $\mathbb{Z}_n, n = 2, \ldots, 10, 12$; $\mathbb{Z}_2 \times \mathbb{Z}_{2m}; m = 1, 2, 3, 4$. Em particular $\#E(\mathbb{Q})_{\text{tor}} \leq 16$.*

Esse teorema foi apresentado por Mazur nos anos 1970 ([M1], [M2]). Segundo esse teorema a ordem dos pontos de $E(\mathbb{Q})_{\text{tor}}$ é no máximo 12 e não existem pontos de ordem 11, mas podem existir ponto de qualquer ordem de 2 a 12; e por exemplo se existir um ponto de ordem 7, então $E(\mathbb{Q})_{\text{tor}} \simeq \mathbb{Z}_7$, uma vez que esse grupo é o único da lista que pode ter elemento de ordem 7. Para cada um destes grupos apresentados no teorema 2.16 existem exemplos [S1, p. 264]. Isso em particular garante que 16 é a melhor cota para $\#E(\mathbb{Q})_{\text{tor}}$. Além disso existe a forma precisa das curvas elípticas cujo grupo de torção seja isomorfo a cada um dos grupos apresentados no teorema 2.16, a lista completa pode ser encontrada em [KD]. Para determinar os pontos de ordem finita, o teorema de Nagell-Lutz é muito útil [KA, p. 130]. Esse teorema determina condições necessárias para que um ponto racional possa ter ordem finita e pode ser aplicado em cúbicas não singulares definidas por equações do tipo:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}.$$

Teorema 2.17. *(Nagell-Lutz) Sejam C uma curva elíptica definida por uma equação do tipo acima e $P(x, y)$ um ponto racional de ordem finita.*

1. *Então $4x, 8y \in \mathbb{Z}$;*

2. *Se* $a_1 = 0$, *então* $x, y \in \mathbb{Z}$;

3. *Se* $a_1 = a_3 = 0$, *então* $x, y \in \mathbb{Z}$. *Além disso* $y = 0$, *o caso em que* P *possui ordem* 2; *ou* $y^2|d$, *onde* d *é o discriminante*[3] *de* $x^3 + a_2x^2 + a_4x + a_6$.

Exemplo 2.18. *Aplicamos o teorema 2.17 para* $y^2 = x^3 - x^2 + x$. *É fácil verificar que* $P(0,0)$ *é de ordem* 2. *Como* $d = 5$, *se o ponto racional* (x, y) *é de ordem finita, então* $y^2|5$, *portanto* $y = \pm 1$. *Então* $P_1(1,1)$ *e* $P_2(1,-1)$ *podem ter ordem finita. Como* $2P_1 = 2P_2 = P$ *e* P *possui ordem* 2, *concluímos que* P_1 *e* P_2 *são de ordem* 4. *Então* $E(\mathbb{Q})_{\text{tor}} \simeq \mathbb{Z}_4$.

Exercício

- Usando o teorema 2.16, mostre que $(2,1) \in C : x^3 + y^3 = 9$ possui ordem infinita.

O exemplo 2.20 a seguir mostra que a recíproca do teorema 2.17 não é verdadeira.

2.5 Redução Módulo Números Primos

Claramente o teorema 2.17 pode ser muito útil para determinar os pontos de ordem finita, embora não possa ser aplicado em geral, lembrem-se de que há restrição sobre os coeficiente de f. De qualquer forma pode não ser muito eficiente quando o discriminante possui muitos fatores, pois nesse caso teremos de verificar muitas possibilidades.

Outro método que pode ser mais eficiente nesses casos é a redução módulo números primos. Primeiro observamos que naturalmente podemos considerar uma cúbica com coeficientes inteiros sobre corpos finitos $\mathbb{F}_p$, onde p é número primo, por meio de redução de seus coeficientes módulo p. Por exemplo a cúbica $y^2 = x^3 + 3x + 5$ define a cúbica $y^2 = x^3 + x + 1$ sobre $\mathbb{Z}_2$; e $y^2 = x^3 + 2$ sobre $\mathbb{Z}_3$. A partir

[3]Lembramos que no caso de $x^3 + ax^2 + bx + c$, $d = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$.

disso pode considerar seu conjunto dos pontos em $\mathbb{Z}_p$, denotado por $\mathcal{C}(\mathbb{F}_p)$. A pergunta natural é: será que $\mathcal{C}(\mathbb{F}_p)$ munido de operação definida em $\mathcal{S}_\mathcal{C}$ é um grupo? Com um pouco de paciência[4] para fazer as contas, podemos verificar que se $p \nmid 2d$, então a resposta é positiva. Essa hipótese garante também que uma cúbica suave reduzida permanece suave. Dado $P(x, y) \in C_f$ denote sua redução módulo p por $\widetilde{P}(\widetilde{x}, \widetilde{y})$.

Teorema 2.19. *(Redução módulo p) Sejam $\mathcal{C} : y^2 + a_1xy + a_3y = f(x) \in \mathbb{Z}[x]$ uma curva elíptica, d o discriminante de f e p um número primo tal que $p \nmid 2d$. Então a redução módulo p, $E(\mathbb{Q})_{\text{tor}} \to \mathcal{C}(\mathbb{F}_p)$ é um monomorfismo. O mesmo vale para $p = 2$, se $a_1 = 0$ e $p \nmid d$.*

Em particular $E(\mathbb{Q})_{\text{tor}}$ pode ser visto como um subgrupo de $\mathcal{C}(\mathbb{F}_p)$, portanto $\#E(\mathbb{Q})_{\text{tor}} \mid \mathcal{C}(\mathbb{F}_p)$.

Exemplo 2.20. *Seja $\mathcal{C} : y^2 = x^3 + 3$. Então $d = -3^5$. Portanto qualquer primo $p \geq 5$ pode ser tomado para aplicar o teorema 2.19. É fácil verificar que $\#\mathcal{C}(\mathbb{F}_5) = 6$ e $\#\mathcal{C}(\mathbb{F}_7) = 13$. Então $\#E(\mathbb{Q})_{\text{tor}} \mid 6$ e $\#E(\mathbb{Q})_{\text{tor}} \mid 13$, logo $\#E(\mathbb{Q})_{\text{tor}} = 1$, ou seja, $E(\mathbb{Q})_{\text{tor}}$ contém apenas o ponto no infinito de $\mathcal{C}$. Consequentemente $(1, 2) \in E(\mathbb{Q})$ possui ordem infinita e $\mathcal{C}$ infinitos pontos racionais.*
Vale observar que, se aplicássemos o teorema de Nagell-Lutz, deveríamos verificar todas as possibilidades de um ponto de $\mathcal{C}$ ter segunda coordenada em $\{\pm1, \pm3, \pm9, \pm27, \pm81, \pm243\}$.

Pela variedade de resultados sobre $E(\mathbb{Q})_{\text{tor}}$, podemos dizer que esse grupo é bem conhecido. Quanto ao posto, a situação é bem mais complicada. Até agora não existe um método eficiente para determiná-lo em geral. Segundo uma conjectura, existem curvas elípticas de postos arbitrariamente grandes. Em 2006, N. Elkies mostrou que o posto de $y^2 + xy + y = x^3 - x^2 - ax + b$, onde $a = 20067762415575526585033208209338542750930230312178956502$ e $b = 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$, é no mínimo 28.
Em alguns casos é possível obter cotas para o posto. Sejam $E(\mathbb{Q})$ uma curva elíptica dada por $y^2 = f(x)$ e que f possui raízes inteiras,

[4] Ou consultar [ST, p. 122-123].

digamos, α, β e γ. Seja d o discriminante de f. Diremos que um primo p é

$$\begin{cases} \textfrak{bom}, \text{ se } p \nmid d; \\ \textfrak{quase ruim}, \text{ se divide exatamente um de } \alpha-\beta, \beta-\gamma, \alpha-\gamma; \\ \textfrak{muito ruim}, \text{ se divide todos os números } \alpha-\beta, \beta-\gamma, \alpha-\gamma. \end{cases}$$

Sejam n_1 e n_2 os números de primos quase ruins e muito ruins respectivamente. Então o posto de $E(\mathbb{Q})$ é no máximo $n_1 + 2n_2 - 1$ [KA, p. 108]. Existem resultados sobre o posto de algumas cúbicas, por exemplo em alguns casos, as curvas elípticas dadas pela equação $y^2 = x^3 - n^2x, n \in \mathbb{Z}$ possuem posto zero, i.e, nestes casos $E(\mathbb{Q})$ é finito [KA, p. 110].

Outro método bastante eficiente é extraído da demonstração do teorema de Mordell-Weil, veja [ST, p. 89-98]

Exercício

- Determine $E(\mathbb{Q})_{\text{tor}}$ para cada uma das cúbicas a seguir.

1. $y^2 = x^3 + 2$
2. $y^2 = x^3 + x$
3. $y^2 = x^3 + 4$
4. $y^2 = x^3 + 4x$
5. $y^2 + y = x^3 - x^2$
6. $y^2 = x^3 + 1$
7. $y^2 - xy + 2y = x^3 + 2x^2$
8. $y^2 + 7xy - 6y = x^3 - 6x^2$
9. $y^2 + 3xy + 6y = x^3 + 6x^2$
10. $y^2 - 7xy - 36y = x^3 - 18x^2$
11. $y^2 + 43xy - 210y = x^3 - 210x^2$
12. $y^2 = x^3 - x^2$
13. $y^2 = x^3 + 5x^2 + 4x$
14. $y^2 + 5xy - 6y = x^3 - 3x^2$
15. $y^2 = x^3 + 337x^2 + 20736x$

2.6 Comentários sobre o Caso Singular

Embora nosso foco principal seja estudar cúbicas suaves, pelo menos para satisfazer curiosidade compensa ver se o teorema Mordell-Weil vale para cúbicas singulares. A boa notícia é que nos casos singulares determinar esses grupos é bem mais fácil do que no caso não singular. Pelos teoremas 2.4, 2.8 e proposição 2.10, basta apenas olhar para as cúbicas nodal e cuspidal apresentadas no teorema 2.4. Primeiro mostraremos que nesses casos os grupos são infinitos. Isso é feito por meio de parametrizações das cúbicas singulares. Geometricamente as parametrizações são obtidas pela interseção das retas $y = rx, r \in \mathbb{Q}$, com as cúbicas.

No caso da cúbica nodal afim $y^2 = x^3 + x^2$, seja $\mathfrak{N}$ o conjunto dos pontos racionais. Lembre-se de que $S(0,0)$ é seu único ponto singular e tome $P(x,y) \in \mathfrak{N}$ suave. Então a aplicação

$$\nu : \begin{cases} \mathfrak{N} & \longrightarrow & \mathbb{Q} \\ P & \longmapsto & \frac{y}{x} \\ S & \longmapsto & 1 \end{cases},$$

está bem definida. Escrevendo a equação da cúbica da forma $(\frac{y}{x})^2 = x + 1$, a injetividade é verificada facilmente. Para verificar a sobrejetividade, dado $r \in \mathbb{Q} \setminus \{1\}$, devemos determinar $x, y \in \mathbb{Q}$ tais que $(x,y) \in \mathfrak{N}$ seja suave e $\frac{y}{x} = r$. Usando $(\frac{y}{x})^2 = x + 1$, basta tomar $x = r^2 - 1$ e $y = r^3 - r$. Isto de fato define a inversa de ν:

$$\nu^{-1} : \begin{cases} \mathbb{Q} & \longrightarrow & \mathfrak{N} \\ r & \longmapsto & (r^2 - 1, r^3 - r), \ r \neq 1 \\ 1 & \longmapsto & (0,0) \end{cases}.$$

No caso da cúspide $y^2 = x^3$, denote o conjunto dos pontos racionais por $\mathfrak{C}$. Usando a mesma ideia do caso nodal, obteremos as seguintes aplicações:

$$\begin{cases} \mathfrak{C} \setminus \{(0,0)\} & \longrightarrow & \mathbb{Q}^* & \longrightarrow & \mathfrak{C} \setminus \{(0,0)\} \\ (x,y) & \longmapsto & \frac{y}{x} & & \\ & & r & \longmapsto & (r^2, r^3) \end{cases}.$$

A existência destas aplicações apenas garante que os conjuntos dos pontos racionais das cúbicas singulares são infinitos. Mas como não

são homomorfismos entre grupos, não fornecem nenhuma informação quanto a suas estruturas de grupo. Lembramos que $(\mathbb{Q},+)$ e $(\mathbb{Q}^*,\cdot)$ não são grupos finitamente gerados. O próximo teorema de fato afirma que o teorema de Mordell-Weil não vale para as cúbicas singulares.

Teorema 2.21. • *Seja $\overline{\mathfrak{N}}_{ns}$ o conjunto dos pontos racionais e suaves da cúbica singular $y^2z = x^3 + x^2z$. Então $\phi : \overline{\mathfrak{N}}_{ns} \to \mathbb{Q}^*$ definido por*

$$\phi(P) = \begin{cases} \frac{y-x}{y+x} & \text{se } P = (x,y), \\ 1 & \text{se } P = \mathcal{O}, \end{cases}$$

é um isomorfismo entre grupos.

- *Seja $\overline{\mathfrak{C}}_{ns}$ o conjunto dos pontos racionais e suaves da cúbica singular $y^2z = x^3$. Então $\varphi : \overline{\mathfrak{C}}_{ns} \to \mathbb{Q}$ definido por*

$$\varphi(P) = \begin{cases} \frac{x}{y} & \text{se } P = (x,y), \\ 0 & \text{se } P = \mathcal{O}, \end{cases}$$

é um isomorfismo entre grupos.

Uma vez que o único elemento de ordem finita de $(\mathbb{Q},+)$ é zero, o teorema 2.21 implica que a cúbica cuspidal possui apenas o ponto $\mathcal{O}$ de ordem finita. Como $(\mathbb{Q}^*,\cdot)$ possui apenas um elemento não trivial de ordem finita, a saber -1 de ordem 2, concluímos que a cúbica nodal possui apenas um ponto de ordem finita (exceto $\mathcal{O}$), a saber $(-1,0)$ de ordem 2.

Exercício

1. Mostre que as cúbicas suaves não admitem parametrizações.

2. Mostre que $(\mathbb{Q},+)$ e $(\mathbb{Q}^*,\cdot)$ não são grupos finitamente gerados.

3. Demonstre o teorema 2.21.

2.7 Pontos Inteiros

Vimos que uma curva elíptica suave pode ter infinitos pontos racionais e pelo teorema de Mordell-Weil, o grupo desses pontos é finitamente gerado. Por outro lado, pelo teorema Nagell-Lutz os pontos racionais de ordem finita de fato são *pontos inteiros*, ou seja, possuem coordenadas inteiras. Esses resultados fazem pensar se em geral uma curva elíptica possui pontos inteiros, e se no caso são finitos ou não. O resultado mais geral foi apresentado por Siegel garantindo a finitude do número dos pontos inteiros. Existem outros resultados que fornecem cotas superiores.

Teorema 2.22. *(Siegel) O número dos pontos inteiros de uma curva elíptica definida sobre $\mathbb{Z}$ é finito.*

Existem várias demonstrações para o teorema de Siegel, mas nenhuma é fácil. Apenas em alguns casos particulares podemos demonstrá-lo numa maneira muito elementar. Por exemplo considere a cúbica dada pela equação $x^3 + y^3 = m, m \in \mathbb{Z}$. Então

$$(x + y)(x^2 - xy + y^2) = m,$$

logo $x + y = a$ e $x^2 - xy + y^2 = b$, onde $a, b \in \mathbb{Z}$ tais que $m = ab$. De

$$m \geq |b| = |x^2 - xy + y^2| = \frac{3}{4}x^2 + (\frac{1}{2}x - y)^2 \geq \frac{3}{4}x^2$$

concluímos $|x| \leq 2\sqrt{\frac{m}{3}}$. Da forma análoga, $|y| \leq 2\sqrt{\frac{m}{3}}$. Então acabamos de demonstrar:

Proposição 2.23. *As soluções $(x, y) \in \mathbb{Z}^2$ de $x^3 + y^3 = m, m \in \mathbb{Z}$ satisfazem $\max\{x, y\} \leq 2\sqrt{\frac{m}{3}}$.*

Usando essa proposição podemos verificar que todas as equações da forma acima para $1 \leq m \leq 1728$ possuem apenas uma solução inteira cada, e para $m = 1729$ apenas duas. Observem que $x^3 + y^3$ é uma expressão simétrica, portanto se (x, y) é uma solução, então (y, x) também é; e no caso essas contam apenas uma solução. Esses fatos já tinham sido observados pelo matemático indiano Ramanujan[5]. Um fato muito curioso sobre essa equação é:

[5]Srinivasa Aiyangar Ramanujan, 1887-1902; veja [ST, p. 149]

Proposição 2.24. *Dado o número natural N, existe $m \geq 1$ tal que a cúbica $x^3 + y^3 = m$ possui pelo menos N pontos inteiros.*

Demonstração. Pelo exercício da seção 2.4, a cúbica $x^3 + y^3 = 9$ possui infinitos pontos racionais. Dado um ponto racional $P(\frac{a}{b}, \frac{c}{d})$, sejam $b, d > 0$ e suas coordenadas nas suas formas reduzidas. Então

$$a^3d^3 + c^3b^3 = 9b^3d^3 \Longrightarrow b^3|a^3d^3, \quad d^3|c^3b^3.$$

Portanto $b^3|d^3$ e $d^3|b^3$ e consequentemente $b^3 = d^3$, ou, $b = d$.
Dado N, tomamos N pontos racionais dessa cúbicas. Pelo argumento acima, podemos escrever $P_i(\frac{a_i}{d_i}, \frac{c_i}{d_i}), i = 1, \ldots, N$. Basicamente a escolha de m é de tal forma que possa eliminar os denominadores dos P_is e transformá-los em pontos inteiros. Tome $m = 9(d_1 \cdots d_N)^3$ e

$$P_i'(d_1 \cdots d_{i-1}a_i d_{i+1} \cdots d_N, d_1 \cdots d_{i-1}c_i d_{i+1} \cdots d_N), \quad i = 1, \ldots, N.$$

De $a_i^3 + c_i^3 = 9d_i^3, i = 1, \ldots, N$, concluímos que os P_i's são pontos inteiros da cúbica $x^3 + y^3 = m$. □

Observem que as soluções inteiras dadas pela proposição acima não são relativamente primos. Agora se quisermos acrescentar essa condição às hipóteses da proposição, o problema se tornará bem mais difícil. Mas precisamente queremos saber se dado $N \geq 1$, existe $m \geq 1$ tal que a equação $x^3 + y^3 = m$ tenha uma solução (x, y) tal que x e y sejam relativamente primos e $x > y$? A resposta geral ainda não é conhecida, nem mesmo para valores pequenos de N. Para $N = 3$, o menor m é 3242197:

$$3242197 = 141^3 + 76^3 = 138^3 + 85^3 = 202^3 + (-171)^3.$$

Se ainda quisermos apenas soluções positivas, para $N = 3$, o menor m é

$$15170835645 = 2468^3 + 517^3 = 2456^3 + 709^3 = 2152^3 + 1733^3.$$

Para $N = 4$ ainda não se sabe se existe m com quatro soluções positivas.

Para concluir a discussão sobre o número dos pontos inteiros das cúbicas $C_m : x^3 + y^3 = m$, é interessante mencionar um resultado

de Silverman que relaciona esse número e seus postos. Esse resultado afirma que existe um constante $\kappa > 1$, *independente* de m, tal que o número das soluções inteiras e relativamente primos de C_m é no máximo $\kappa^{1+\text{rank}C_m}$. Em particular enquanto C_m possuir mais pontos inteiros cujas coordenadas sejam relativamente primos, terá posto maior. Esse teorema poderia ser uma maneira para verificar se existem cúbicas cujos postos sejam arbitrariamente grandes: se pudéssemos encontrar uma sequência de $\{m_n\}_n$ tal que o número das soluções inteiras e relativamente primos de C_{m_n} tendesse ao infinito.

Um resultado um pouco mais geral que a proposição 2.23 foi apresentado por A. Thue em 1974. Usando um teorema de aproximação diofantina, demonstrado por ele mesmo, conseguiu mostrar que a equação $ax^3+by^3 = c, a, b, c \in \mathbb{Z}$ possui um número finito de soluções inteiras. Sua longa demostração pode ser encontrada em [ST, Cap. 5].

Para finalizar não podemos deixar de citar um resultado de Baker apresentado em 1966 que fornece uma cota para o número dos pontos inteiros das curvas elípticas. Sua demostração é baseada também num teorema de aproximação diofantina, provado por ele mesmo. Segundo o resultado de Baker, todo ponto inteiro da curva elíptica $y^2 = x^3 + ax^2 + bx + c, a, b, c \in \mathbb{Z}$ satisfaz $\max\{x, y\} \leq \exp((10^6 H)^{10^6})$, onde $H = \max\{|a|, |b|, |c|\}$. No mesmo trabalho ele apresentou um método para determinar todos os pontos inteiros de uma curva elíptica.

Exercícios

1. Mostre que as soluções inteiras de $x^2 - 2y^2 = 1$ são dadas por $(x_0, y_0) = (1, 0)$ e $(x_{i+1}, y_{i+1}) = (3x_i + 4y_i, 2x_i + 3y_i), i \geq 0$.

2. Sejam $a, b, c \in \mathbb{Z} \setminus \{0\}$. Mostre que se (x, y) é uma solução de $ax^3 + bxy^2 = c$, então $\max\{|ax^2|, |by^2|\} \leq 1 + \max\{|a|, |b|\}c^2$.

3. Seja p um número primo. Mostre que a equação $x^3 + y^3 = p$ possui solução inteira somente quando $p = 2$ ou $p = 3u^2+3u+1$ para algum $u \in \mathbb{Z}$.

Capítulo 3

Cúbicas sobre Corpos Finitos

Seja p um número primo e $\mathbb{F}_p$ o corpo finito de p elementos. O objetivo deste capítulo é estudar cúbicas sobre $\mathbb{F}_p$, ou, numa maneira mais geral sobre suas extensões, i.e, corpos finitos $\mathbb{F}_q$, onde $q = p^e$ para algum $e \in \mathbb{N}$. Em todo caso podemos construir o espaço projetivo e falar de pontos no infinito. Dada uma cúbica $\mathcal{C}$ definida sobre um corpo finito $\mathbb{F}$, denotamos seu conjunto de *pontos racionais* por $\mathcal{C}(\mathbb{F})$. Se $\mathcal{C}$ for suave, podemos definir uma operação entre seus pontos e obter um grupo abeliano. Para mais resultados fundamentais, o leitor interessado poderá consultar [GA].

Por exemplo, considere a cúbica $\mathcal{C} : y^2 = f(x) = x^3 + ax^2 + bx + c$, onde $a, b, c \in \mathbb{F}_p$. Essa cúbica é suave, se, e somente se, $p \nmid 2d$, onde d é o discriminante de f. Observem que $\mathcal{O}(0:1:0)$ é o único ponto no infinito de $\mathcal{C}$. Dados pontos $P_1(x_1, y_1), P_2(x_2, y_2) \in \mathcal{C}(\mathbb{F}_p)$, seja $y = \lambda x + \nu$ a equação da reta que passa por eles, então:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{se } x_1 \neq x_2, \\ \frac{3x_1^2 + 2ax_1 + b}{2y_1}, & \text{se } P_1 = P_2, \end{cases}$$

e $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$. Então $P_3(x_3, y_3) = P_1 + P_2$ é dado pelas fórmulas

$$x_3 = \lambda^2 - a - x_1 - x_2, \quad y_3 = -\lambda x_3 - \nu.$$

Observem que se $P_1 = P_2 = \mathcal{O}$, então $P_1 + P_2 = \mathcal{O}$. Claramente tudo isso faz sentido uma vez que todas as contas são feitas com elementos de $\mathbb{F}_p$.

Exemplo 3.1. *Considere $\mathcal{C} : y^2 = x^3 + x + 1$ sobre $\mathbb{F}_5$. É fácil verificar que $\mathcal{C}(\mathbb{F}_5) = \{\mathcal{O}, (0, \pm 1), (\pm 2, \pm 1), (-1, \pm 2)\}$. Então $\mathcal{C}(\mathbb{F}_5)$ é um grupo abeliano de ordem 9, portanto é cíclico ou é produto de dois grupos de ordem 3. Tome $P(0, 1)$. Usando as fórmulas, $3P = (2, 1) \neq \mathcal{O}$. Isso é suficiente para garantir que $\mathcal{C}(\mathbb{F}_5)$ é cíclico, caso contrário todos os pontos, inclusive P, teriam ordem 3.*

3.1 Teorema de Hasse-Weil

Dado um corpo finito $\mathbb{F}$, a pergunta natural é se é possível estimar o número dos elementos de $\mathcal{C}(\mathbb{F})$. Para isso basta consideramos a parte afim da curva, ou seja, tentar estimar o número dos elementos $\{(a, b) \in \mathbb{F} | F(a, b) = 0\}$, onde $F \in \mathbb{F}[x, y]$ é de grau 3. O resultado mais geral no caso de cúbicas não singulares é o teorema de Hasse-Weil:

Teorema 3.2. *(Hasse-Weil) Seja $\mathcal{C}$ uma cúbica não singular definida sobre $\mathbb{F}_q$. Então*

$$|\#\mathcal{C}(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Esse teorema foi apresentado por E. Artin, como uma conjectura, na sua tese de doutorado e foi demonstrado por Hasse em 1933. Em 1948, A. Weil demonstrou esse teorema para curvas não singulares em geral. No caso geral as cotas superior e inferior são $q+1 \pm 2g\sqrt{q}$, onde g é o *gênero* da curva. Por exemplo o gênero da curva de Fermat, $x^n + y^n = 1$, é $\frac{1}{2}(n-1)(n-2)$. Alguns casos particulares de estimar o número de soluções de uma equação de graus 3 foram estudados por Gauss, por exemplo, a curva de Fermat $x^3 + y^3 = 1$ sobre $\mathbb{F}_p$. A equação homogênea associada é $x^3 + y^3 + z^3 = 0$. Observem que consideraremos as soluções no espaço projetivo, portanto não consideraremos a solução trivial $(0, 0, 0)$; e identificaremos a solução (x, y, z) como todos os seus múltiplos não nulos $(ax, ay, az), a \in \mathbb{F}_p$.

3.2 Teorema de Gauss

Teorema 3.3. *(Gauss) Seja M_p o número das soluções projetivas de $\mathcal{G} : x^3 + y^3 + z^3 = 0$ em $\mathbb{F}_p$.*

- *Se $3 \nmid p-1$, então $M_p = p+1$.*
- *se $3|p-1$, então existem únicos (a menos de sinal) inteiros a e b tais que $4p = a^2 + 27b^2$. Escolha o sinal de a tal que $3|a-1$, então $M_p = p+1+a$.*

Demonstração. Veja [ST]. □

De fato a demonstração da primeira parte é bem simples: se $3 \nmid p-1$, então $x \mapsto x^3$ define um isomorfismo de $\mathbb{F}_p^*$, portanto resolver essa equação é equivalente a resolver a equação $x + y + z = 0$ que por sua vez é equação de uma reta no plano projetivo, portanto possui exatamente $p+1$ pontos. Quando $3|p-1$, o homomorfismo $x \mapsto x^3$ não é nem injetivo nem sobrejetivo, o que torna a demonstração mais trabalhosa.

Observem que quando $3 \nmid p-1$, M_p é sempre múltiplo de 9. De fato $\mathcal{G}(\mathbb{F}_p)$ possui nove pontos de ordem 3 correspondentes às soluções de $x^3 + y^3 + z^3 = 0$. Esses são aqueles que possuem uma coordenada nula e as outras, raízes cúbicas de 1 e -1. Como $3|p-1$ garante que $\mathbb{F}_p$ tenha 3 raízes cúbicas da unidade, teremos 9 pontos de $\mathcal{G}(\mathbb{F}_p)$ que formam um subgrupo de ordem 9, logo $9|M_p$. Esse fato pode ser demonstrado numa maneira puramente aritmética analisando as possibilidades de congruência de p e a módulo 9.

Exemplo 3.4. *Quando $p = 7$, $a = b = 1$ e $M_7 = 9$. Para $p = 13$, $a = -5$ e $b = 1$, portanto $M_{13} = 9$.*

Exercícios

1. Sejam $p \neq 2$ primo, $a, b, c, d \in \mathbb{F}_p$ tais que $acd \neq 0$ e C a cônica dada pela equação $ax^2 + bxy + cy^2 = dz^2$.

   - Se $b^2 \neq 4ac$, então $\#C(\mathbb{F}_p) = p+1$.
   - Se $b^2 = 4ac$, então $\#C(\mathbb{F}_p) = 1$ ou $2p+1$.

   Dê exemplos nos quais as duas possibilidades ocorram.

2. Determine o grupo $C(\mathbb{F}_p)$ para a curva $C : y^2 = x^3 + x + 1$ e primos $p = 3, 7, 11, 13$.

3. Sejam $p \geq 3$ primo e $m \in \mathbb{N}$ tais que $(m, p-1) = 1$. Mostre que a equação $x^m + y^m + z^m = 0$ possui $p + 1$ soluções projetivas em $\mathbb{F}_p$.

Capítulo 4

Aplicação

O teorema fundamental da aritmética garante a existência e a unicidade de fatoração de números inteiros em números primos. O problema computacional, ou seja, fatorar um determinado número inteiro pode não ser uma tarefa fácil, principalmente para números grandes. Esse problema, além de ser um problema do interesse dos matemáticos, é de grande importância prática. Por exemplo a segurança de alguns sistemas criptográficos depende da dificuldade da fatoração das chaves públicas. Em outras palavras, esses sistemas seriam inseguros se existisse um algoritmo *rápido* para fatoração de inteiros. Existem diversos métodos e algoritmos para fatorar números inteiros, um deles é o algoritmo de Lenstra que utiliza curvas elípticas.

Naturalmente o primeiro passo para fatorar um número inteiro é determinar se o mesmo é primo. Para isto podemos usar um caso particular do pequeno teorema de Fermat[1]: se n é primo ímpar, então $2^{n-1} \overset{n}{\equiv} 1$. Isto é, se $2^{n-1} \not\equiv 1 (\text{mod } n)$, então n não é primo. Outra maneira seria usar o teorema de Wilson: n é primo, se, e somente se, $(n-1)! \overset{n}{\equiv} -1$.

Passando por essa etapa, queremos fatorar o número n. O primeiro e mais natural modo de fazer isso é tomar os números naturais $k < n$ e verificar se estes dividem o número n e quantas vezes. Esse método pode ser otimizado usando o fato que o menor fator de n é menor

[1]Dados $a \in \mathbb{Z}$ e p primo tais que $(a, p) = 1$, então $a^{p-1} \overset{p}{\equiv} 1$.

que $\sqrt{n}$, mas mesmo assim para grandes valores não é muito prático. Antes de apresentar alguns métodos mais eficientes de fatoração, veremos um método para calcular $a^k (\text{mod } n)$ e estimar o número de operações para este cálculo. Além disso faremos uma estimativa para o número de operações necessárias para calcular o maior divisor comum usando o algoritmo de Euclides. Essas estimativas servirão para mostrar o quanto os algoritmos a serem apresentados são eficientes.

4.1 Dois Problemas de Aritmética

Problema 1. Sejam $a, k, n \in \mathbb{N}$. Queremos estimar o número de operações para determinar $a^k (\text{mod } n)$.

Para explicar melhor a ideia, seja $k = 1000$. Escrevemos k como uma soma de potências de 2, ou seja, apresentamos k na base 2:

$$1000 = 2^3 + 2^5 + 2^6 + 2^7 + 2^8 + 2^9,$$

então $a^{1000} = a^{2^3} \cdot a^{2^5} \cdots a^{2^9}$. Calcularemos os números $A_i := a^{2^i} (\text{mod } n)$.

$$\begin{aligned} A_0 &= a (\text{mod } n), \\ A_1 &= A_0 \cdot A_0 = a^2 (\text{mod } n), \\ A_2 &= A_1 \cdot A_1 = a^4 (\text{mod } n), \\ A_3 &= A_2 \cdot A_2 = a^{2^3} (\text{mod } n), \\ &\vdots \\ A_9 &= A_8 \cdot A_8 = a^{2^9} (\text{mod } n). \end{aligned}$$

Então

$$a^{1000} (\text{mod } n) = A_3 \cdot A_5 \cdot A_6 \cdot A_7 \cdot A_8 \cdot A_9 (\text{mod } n).$$

Observem que com apenas 9 operações para obter os A_is e 6 operações para obter $a^{1000} (\text{mod } n)$ faremos o cálculo. Esse é um método que pode ser muito melhor e mais rápido do que calcular a^{1000} e depois determinar o resto da divisão por n. Em geral, considere a expansão binária efetiva de k:

$$k = k_0 + k_1 \cdot 2 + k_2 \cdot 2^2 + k_3 \cdot 2^3 + \cdots + k_{r-1} \cdot 2^{r-1} + 2^r.$$

A seguir calculamos $A_0 = a,\ A_1 = A_0^2,\ A_2 = A_1^2, \ldots, A_r = A_{r-1}^2$. Finalmente obtemos a^k como

$$a^k = (\text{produto dos } A_i\text{s para cada } k_i = 1).$$

São necessárias r operações para calcular os A_is e depois com no máximo (eventualmente $k_i = 0$ para algum i) r operações para calcular a^k, totalizando no máximo $2r$ operações. Observamos

$$k = k_0 + k_1 2 + \cdots + 2^r \geq 2^r \Longrightarrow r \leq \log_2 k.$$

Então provamos

Proposição 4.1. *Dados $a, k, n \in \mathbb{N}$, é possível calcular $a^k \pmod n$ em no máximo $2 \cdot \log_2 k$ operações, onde cada operação consiste em uma multiplicação e uma redução módulo n.*

Esse método para calcular $a^k \pmod n$ é muito prático, uma vez que para os valores grandes de k o número de operações necassárias é *bem menor* que k, isto é garantido pelo fato que

$$\lim_{k \to +\infty} \frac{\log_2 k}{k} = 0.$$

Problema 2. Sejam $a, b \in \mathbb{N}$. O objetivo é fazer uma estimativa do número das operações necessárias para determinar o maior divisor comum de a e b usando o algoritmo de Euclides.

Lembre-se de que o algoritmo de Euclides é baseado em divisões sucessivas:

$$\begin{aligned}
a &= bq_1 + r_2, \quad 0 \leq r_2 < b, \\
b &= r_2 q_2 + r_3, \quad 0 \leq r_3 < r_2, \\
r_2 &= r_3 q_3 + r_4, \quad 0 \leq r_4 < r_3, \\
&\vdots \\
r_{n-1} &= r_n q_n + r_{n+1}, \quad 0 \leq r_{n+1} < r_n, \\
r_n &= r_{n+1} q_{n+1}.
\end{aligned}$$

Como a sequência dos restos é uma sequência decrescente de números inteiros não negativos, $r_{n+2} = 0$ para algum n. Pelo algoritmo $(a, b) = r_{n+1}$. Afirmamos que:

$$\forall i, \quad r_{i+1} \leq \frac{1}{2} r_{i-1}. \qquad (\maltese)$$

Se $r_i \leq \frac{1}{2} r_{i-1}$, então claramente ($\maltese$) é válida pelo fato de que $r_{i+1} < r_i$. Se $r_i > \frac{1}{2} r_{i-1}$, de

$$r_{i-1} = r_i q_i + r_{i+1}, \qquad 0 \leq r_{i+1} < r_i$$

concluímos

$$r_{i+1} = r_{i-1} - r_i q_i < r_{i-1}(1 - \frac{1}{2} q_i).$$

Claramente $q_i \neq 0$, pois caso contrário $r_{i-1} = r_{i+1}$ e isto contradiz o fato de que os r_is são estritamente decrescentes. Então $q_i \geq 1$, logo $r_{i+1} < \frac{1}{2} r_{i-1}$.
Sem perda de generalidade, suponhamos $a \geq b$. Usando as desigualdades $r_2 < b$ e ($\maltese$), por indução finita mostramos

$$r_{2i} < \frac{1}{2^{i-1}} b.$$

Como r_{2i} é um inteiro não negativo, se $2^{i-1} \geq b$, então $r_{2i} < 1$, o que significa que $r_{2i} = 0$. Ou seja,

$$2^{i-1} \geq b \Longrightarrow r_{2i} = 0.$$

Em outras palavras

$$i \geq 1 + \log_2 b = \log_2(2b) \Longrightarrow r_{2i} = 0.$$

Dessa forma acabamos de provar a seguinte proposição

Proposição 4.2. *Usando o algoritmo de Euclides, em no máximo*

$$2 \cdot \log_2 \max\{2a, 2b\}$$

passos, determinaremos o maior divisor comum de a e b.

Agora voltaremos ao problema de fatoração de inteiros em produto de primos. A seguir explicaremos o algoritmo de Pollard.

4.2 Algoritmo de Pollard

Esse algoritmo constitui um protótipo daquilo que iremos estudar posteriormente: a fatoração por curvas elípticas. Infelizmente esse método não funciona para todos os números, mas quando funciona, é muito eficiente. A ideia é a seguinte: suponha que n tenha um fator primo p tal que $p-1$ é um produto de pequenos primos. Pelo pequeno teorema de Fermat, se $p \nmid a$ então $a^{p-1} \equiv 1 (\text{mod } p)$. Assim $p|(a^{p-1}-1, n)$. Não conhecemos p, portanto não podemos calcular $a^{p-1}-1$. Então escolheremos um inteiro da forma $k = 2^{e_2} \cdot 3^{e_3} \cdots r^{e_r}$, onde $2, 3, \ldots, r$ são os primeiros primos e e_i são inteiros positivos pequenos. Calculamos $d := (a^k - 1, n)$. Observamos que é necessário calcular $a^k - 1 (\text{mod } n)$. Pelos problemas discutidos acima, calculamos d em menos que $2\log_2(2kn)$ operações, que é uma quantidade razoável de operações mesmo para valores grandes de k e n.

Seja $p|n$, se $p-1|k$, então $p|a^k - 1$, logo $p|d$, em particular $d \geq p > 1$. Se $d \neq n$, então teremos um fator próprio de n e repetiremos o procedimento para cada fator de n obtido desta forma. Caso contrário, faremos o procedimento acima novamente da seguinte forma: se $d = n$, então escolhemos outro valor de a; e se $d = 1$, escolhemos um k maior.

Exemplo 4.3. $n = 246082373$. *A primeira coisa a verificar é se n não é primo: como* $2^{n-1} (\text{mod } n) \neq 1$*, então n é composto. Aplicaremos o algoritmo de Pollard tomando*

$$a = 2 \quad e \quad k = 2^2 \cdot 3^2 \cdot 5 = 180.$$

Como $180 = 2^2 + 2^4 + 2^5 + 2^7$*, precisamos calcular* $2^{2^i} (\text{mod } n)$ *para* $0 \leq i \leq 7$*. Estes valores são* $2, 4, 16, 256, 65536$, 111566955, 166204404 *e* 214344997 *respectivamente. Então*

$$\begin{aligned} 2^{180} &= 2^{2^2} \cdot 2^{2^4} \cdot 2^{2^5} \cdot 2^{2^7} \\ &\equiv 16 \cdot 65536 \cdot 111566955 \cdot 28795219 (\text{mod } n) \\ &\equiv 121299227 (\text{mod } n). \end{aligned}$$

Então pelo algoritmo de Euclides

$$(2^{180} - 1, n) = (121299226, n) = 1.$$

Isto é n não tem fatores p tais que $p-1|180$. Então escolhemos um k maior, por exemplo

$$k = [2, 3, \ldots, 9] = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520 = 2^3 + 2^4 + 2^6 + 2^7 + 2^8 + 2^{11}.$$

Usando o mesmo método,

$$2^{2520} = 2^{2^3+2^4+2^6+2^7+2^8+2^{11}} \equiv 101220672 (\text{mod } n),$$

e pelo algoritmo de Euclides

$$(2^{2520} - 1, n) = (101220671, n) = 2521,$$

ou seja, $2521|n$, de fato $n = 2521 \cdot 97613$, e cada fator é um número primo. Claramente a fatoração desse número pode ser feita facilmente verificando a divisibilidade de n por todos os primos menores ou iguais a $\sqrt{n} \approx 15687$ por meio de um computador, mas desta forma mostramos o quanto o algoritmo de Pollard pode ser eficiente.

Note que o algoritmo Pollard deve finalmente parar porque eventualmente k no passo 1 será igual a $\frac{1}{2}(p-1)$ para algum primo p que divide n, então, eventualmente haverá algum $p-1$ dividindo k. Este algoritmo não é muito prático para grandes valores de n; de fato funciona bem, ou seja, determina um fator de n fazendo uma quantidade razoável de operações, se n tiver um divisor primo p tal que

$$p - 1 = \text{ produto de pequenos primos a pequenas potências.}$$

O algoritmo de Pollard é baseado no fato de que o grupo $\mathbb{Z}_p^*$ é de ordem $p-1$. Assim se $p-1|k$, então $a^k = 1$ para todo $a \in \mathbb{Z}_p^*$. A ideia do algoritmo de Lenstra é substituir o grupo $\mathbb{Z}_p^*$ pelo grupo dos pontos de uma curva elíptica C definida sobre $\mathbb{Z}_p$, ou seja,

$$C(\mathbb{Z}_p) := \{(a, b) \in C | a, b \in \mathbb{Z}_p\}$$

e substituir o inteiro a por um ponto $P \in C(\mathbb{Z}_p)$. Como no algoritmo de Pollard, escolhemos um inteiro k composto de um produto de pequenos primos. Se ocorrer que $\#C(\mathbb{Z}_p)|k$, então $kP = \mathcal{O}$ em $C(\mathbb{Z}_p)$. Esse fato geralmente permite encontrar um fator próprio de n.

Ao escolher uma cúbica C, o algoritmo de Lenstra funciona bem se o número a ser fatorado possui um fator primo p tal que $\#C(\mathbb{Z}_p)$

seja produto de pequenos primos a pequenas potências. Isto é parecido com o algoritmo de Pollard quando queríamos que $p-1 = \#\mathbb{Z}_p^*$ tivesse essa propriedade. Então qual seria a vantagem desse novo algoritmo? Se escolhermos apenas uma curva C com coeficientes inteiros e considerarmos sua redução módulo números primos, então não há vantagens. Pois, como mencionamos anteriormente, este algoritmo funcionará se, para algum primo p que divida n, $\#C(\mathbb{Z}_p)$ seja produto de primos pequenos. Mas com o algoritmo de Lenstra, existe a flexibilidade de escolher uma nova curva elíptica e de repetir o processo. Variando a curva C e desde que $\#C(\mathbb{Z}_p)$ varie consideravelmente para cada primo p, nossas chances para concluirmos o algoritmo são bastante boas. Antes de explicar o algoritmo de Lenstra, vale lembrar-se de que pelo teorema de Hasse-Weil

$$\#C(\mathbb{Z}_p) = p + 1 + \varepsilon_p, \quad |\varepsilon_p| \leq 2\sqrt{p}.$$

Além disso, pode-se mostrar que variando C, os números ε_p são bem distribuídos ao longo do intervalo $[-2\sqrt{p}, 2\sqrt{p}]$. Por isso, é bastante provável (mas ainda não rigorosamente provado) que possamos achar, de forma bastante rápida, uma curva C tal que $\#C(\mathbb{Z}_p)$ seja igual a um produto de números primos pequenos.

4.3 Algoritmo de Lenstra

Seja $n \geq 2$ um inteiro composto para o qual buscamos um fator. O algoritmo de Lenstra consiste nos seguintes passos:

Passo 1. Verifique que $(n, 6) = 1$ e também que n não seja da forma m^r para algum $r \geq 2$.
Passo 2. Escolha aleatoriamente inteiros b, x_1, y_1 entre 1 e n.
Passo 3. Seja $c = y_1^2 - x_1^3 - bx_1 (\text{mod } n)$, considere a cúbica $C : y^2 = x^3 + bx + c$. Pela escolha de c, $P = (x_1, y_1) \in C$.
Passo 4. Verifique se $d := (4b^3 + 27c^2, n) = 1$. Se $d = n$, volte e escolha um novo b. Se $1 < d < n$, então d é um fator não trivial de n.
Passo 5. Escolha k como produto de pequenos primos a pequenas potências. Por exemplo $k = [1, 2, 3, \ldots, m]$, onde $m \in \mathbb{N}$.
Passo 6. Calcule $kP = (\frac{a_k}{d_k^2}, \frac{b_k}{d_k^3})$.

Passo 7. Calculamos $D = (d_k, n)$. Se $1 < D < n$, então D é um fator não trivial de n. Se $D = 1$, ou voltaremos ao *Passo 5* e aumentamos o valor de k, ou voltaremos ao *Passo 2* para escolher uma outra curva. Se $D = n$, voltaremos ao *Passo 5* e reduziremos o valor de k.

Observamos que existem várias coisas a serem discutidas neste algoritmo. Primeiro explicaremos porque funciona. Imaginem que conseguimos uma curva C e $k \in \mathbb{N}$ tais que para algum fator primo p de n, $\#C(\mathbb{Z}_p)|k$. Então a ordem de todos os pontos de $C(\mathbb{Z}_p)$ divide k, em particular $kP = \mathcal{O}$, mais precisamente, $kP(\text{mod } p)$ é o ponto no infinito $\mathcal{O}$. Então $p|d_k$, logo $p|D$. Consequentemente obteremos um fator de n, a não ser que $n|d_k$.

Outra coisa é uma maneira eficiente para calcular kP. Considere a expressão binária de k :

$$k = k_0 + k_1 \cdot 2 + \cdots + k_{r-1} \cdot 2^{r-1} + 2^r, \quad k_i \in \{0, 1\}.$$

Lembre-se de que isso pode ser feito em no máximo $r \leq \log_2 k$ operações. A seguir calculamos

$$\begin{aligned} P_0 &= P \\ P_1 &= 2P_0 = 2P \\ P_2 &= 2P_1 = 2^2 P \\ P_3 &= 2P_2 = 2^3 P \\ &\vdots \\ P_r &= 2P_{r-1} = 2^r P, \end{aligned}$$

e finalmente fazemos $kP = \sum_{k_i \neq 0} P_i$. Desse modo calculamos kP em menos de $2 \log_2 k$ passos. Note entretanto que não queremos calcular as coordenadas de kP como números racionais porque o numerador e o denominador teriam aproximadamente k^2 dígitos, e isso pode ser um número muito grande. Então o melhor seria fazer as contas módulo n. Se n não é primo, teremos outro problema. Lembramos que pelas fórmulas explícitas, para determinar a soma de dois pontos

(x_1, y_1) e (x_2, y_2) devemos calcular $\frac{y_2-y_1}{x_2-x_1}$ e neste caso devemos fazer essa conta em $\mathbb{Z}_n$. Mas $\mathbb{Z}_n$ não é um corpo e $x_2 - x_1$ pode não ser invertível. Lembre-se de que $x_2 - x_1$ possui inverso, se, e somente se, $(x_2 - x_1, n) = 1$. Observe que se $1 < (x_2 - x_1, n) < n$, já temos um fator de n. O pior seria se $(x_2 - x_1, n) = n$; nesse caso o melhor caminho será voltar ao *Passo 5* e reduzir o valor de k, ou retornar ao *Passo 2* e tomar outra curva.
Para determinar $2(x_1, y_1)$ módulo n, precisamos calcular

$$\frac{f'(x_1)}{2y_1} = \frac{3x_1^2 + 2ax_1 + b}{2y_1} (\text{mod } n).$$

Nesse caso calcularemos (y_1, n) e faremos da mesma forma que no caso $(x_2 - x_1, n)$, explicado acima.
Essencialmente essas explicações mostram como e porque o algoritmo Lenstra funciona, embora na prática há diversos caminhos para torná-lo mais eficiente.

Exemplo 4.4. $n = 1715761513$. *A primeira coisa é verificar se n não é primo. Usando o método explicado no começo deste capítulo, facilmente calculamos*

$$2^{n-1} \equiv 93082891 (\text{mod } n).$$

Então pelo pequeno teorema de Fermat, n não é primo. Esse número é ímpar e $3 \nmid n$, *portanto* $(n, 6) = 1$. *Para verificar se n não é potência perfeita, calcularemos suas raízes r-ésimas*

$$\sqrt{n},\ \sqrt[3]{n},\ \sqrt[4]{n}, \ldots,\ \sqrt[31]{n} \approx 1,9855.$$

Nenhum desses é inteiro, assim n não é potência perfeita. Como $\sqrt{n} \approx 42422$, *concluímos que n possui algum fator primo* $p < 42422$. *Buscamos escolher um valor de k de modo que alguns inteiros próximos de p dividam k. Tentaremos* $k = [1, 2, 3, \ldots, 17] = 12252240$, *que tem muitos fatores menores que* 42422. *A seguir temos de escolher uma curva elíptica e um ponto seu. Como indicado na descrição do algoritmo de Lenstra, é mais fácil fixar o ponto P e um dos coeficientes da curva e escolher o outro coeficiente tal que o ponto esteja na curva. Tome* $P = (2, 1)$.

Dado b, seja $c := -7 - 2b$. Para começar tomamos $b = 1$, então $c = -9$ e

$$C : y^2 = x^3 + x - 9, \quad P = (2, 1) \in C.$$

Temos de calcular $kP \pmod n$. A expressão binária de k é

$$2^4 + 2^6 + 2^{10} + 2^{12} + 2^{13} + 2^{14} + 2^{15} + 2^{17} + 2^{19} + 2^{20} + 2^{21} + 2^{23}.$$

Então precisamos calcular $2^i P \pmod n$ para $0 \leq i \leq 23$. Claramente precisaríamos de muito tempo para fazer essas contas, mas com a ajuda de um pequeno computador

$$kP = 12252240(2, 1) \equiv (421401044, 664333727) \pmod n.$$

Isso não diz sobre os fatores de n. O ponto principal do algoritmo de Lenstra é que ele nos dá um fator de n quando a lei da adição falha, ou seja, esse algoritmo funciona quando não é possível calcular $kP \pmod n$.

Nesse caso temos três escolhas: recomeçar com um novo k, um novo P, ou uma nova curva. Tomamos a última alternativa. Tomando $3 \leq b \leq 41$ e seu respectivo valor para $c = -7 - 2b$, veremos que ainda é possível determinar $kP \pmod n$. Quando tentamos $b = 42$ e $c = -91$, a lei da adição falha e encontramos um fator de n. O que acontece é o seguinte: não temos nenhuma dificuldade em fazer uma tabela dos $2^i P \pmod n$ para $0 \leq i \leq 23$, como acima. Então começamos adicionando os pontos da tabela para calcular $kP \pmod n$. Como um penúltimo passo, encontramos

$$\begin{aligned} (2^4 + \cdots + 2^{20} + 2^{21})P &= 386363P \\ &\equiv (11150004543, 1676196055) \pmod n \end{aligned}$$

Também

$$2^{23} P \equiv (1267572925, 848156341) \pmod n.$$

Então para calcular kP teremos que somar esses últimos pontos módulo n. Para fazer isso temos de fazer a diferença de suas coordenadas x e encontrar o inverso de n. Ao fazer isto, descobrimos que o inverso não existe:

$$(11150004543 - 1267572925, n) = (-152568382, n) = 26927.$$

Assim a tentativa de calcular $12252240(2,1)$ *na curva*

$$y^2 = x^3 + 42x - 91 (\text{mod } n)$$

falha e isto leva a fatoração

$$n = 1715761513 = 26827 \cdot 63719$$

É fácil conferir que cada um desses fatores é primo, portanto obtemos a fatoração completa de n*.*

Nesse caso conseguimos determinar um fator de n para um valor relativamente pequeno de b, caso isso não fosse possível, teríamos de aumentar o valor de k por exemplo para $[1, 2, \cdots, 25]$ e talvez até tomar um outro ponto, por exemplo $P(3, 1)$.

Exercício

Use o algoritmo de Lenstra para fatorar 35.

Bibliografia

[F] Fischer, G. Plane Algebraic Curves, Student Mathematica Library, volume 15, *AMS* (2001)

[GA] Garcia, A. Pontos Racionais em Curvas sobre Corpos Finitos, 20° Colóquio Brasileiro de Matemática, *IMPA* (1995)

[G] Gibson, C. G. Elementary Geometry of Akgebraic Curves, An Undergraduate Introduction, *Cambridge University Press*, 1998

[H] Hefez, A. Introdução à Geometria Projetiva, Monografias de Matemática Nº 46, *IMPA* (1990)

[DH] Husemöller, D. Elliptic Curves, Graduate Texts in Matehmatics 111, *Springer-Verlag* (1987)

[KF] Kirwan, F. Complex Algebraic Curves, London Mathematical Society Student Texts 23, *Cambridge University Press* (1992)

[KA] Knapp, A. W. Elliptic Curves, Mathematical Notes 40, *Princeton University Press* (1992)

[KE] Kunz, E. Introduction to Plane Algebraic Curves, *Birkhäuser* (2005)

[KD] D. S. Kubert, Universal bounds on the torsion of elliptic curves, Proc. London Math. Soc. (3), 33(2) 193-237, 1976.

[L] Lang, S. Algebra, GTM 211, *Springer*, (2002)

[M1] Mazur, B. Modular Curves and the Eisenstein idela, IHES Publ. Math. 47 33-186, 1977.

[M2] Mazur, B. Rational isogenies of prime degree, Invent. Math. 44, 129-162, 1978.

[SSG] Shokranian, S.; Soares, M. e Godinho, H. Teoria dos Números, *Editora UnB* (1999)

[S1] Silverman, J. H. The Arithmetic of Elliptic Curves, Graduate Texts in Matehmatics, *Springer-Verlag* (1986)

[S2] Silverman, J. H. The Ubiquity of Elliptic Curves, 2007.

[ST] Silverman, J. H. and Tate, J. Rational Points on Elliptic Curves, Undergraduate Texts in Matehmatics, *Springer-Verlag* (1992)

[V] Vainsencher, I. Introdução às Curvas Algébricas, *IMPA* (2005)

[VW] van der Waerden, B. L. Algebra volume 1, *Springer-Verlag* (1991)

[W] Walker, R. J. Algebraic Curves, *Springer-Verlag* (1978)

Índice