Revista Eletrônica Paulista de Matemática

ISSN 2316-9664
v. 23, n. 1, jul. 2023
Artigo de Iniciação Científica

Um algoritmo de fatoração dos números inteiros usando curvas elípticas

An integer factorization algorithm using elliptic curves

Parham Salehyan
Instituto de Biociências, Letras e Ciências Exatas
UNESP - Universidade Estadual Paulista "Júlio de Mesquita Filho"
p.salehyan@unesp.br

Resumo

A teoria de curvas elípticas envolve uma bela mistura de álgebra, geometria, análise e teoria dos números. O objetivo principal deste texto é apresentar uma introdução a essa teoria numa maneira acessível aos alunos de graduação e aplicá-la num dos problemas mais familiares da aritmética dos inteiros: a fatoração em primos.
Palavras-chave: curvas elípticas, números primos, fatoração.

Abstract

The theory of elliptic curves involves a nice mix of algebra, geometry, analysis and number theory. The main objective of this text is to present a introduction to this theory in an accessible manner to undergraduate students and apply it to one of the most familiar problems about integers: their factorization into prime numbers.
Keywords: elliptic curves, prime numbers, factorization.

Artigo recebido em mar. 2023 e aceito em jun. 2023

1 Introdução

As curvas elípticas além de terem uma história longa, possuem diversos métodos utilizados no seu estudo. Por outro lado, já foram usadas na demonstração do último teorema de Fermat e são empregadas em criptografia e fatoração de números inteiros. Isso tudo e a facilidade de serem definidas, sem necessidade de muitos pré-requisitos, as torna objetos muito interessantes a serem apresentadas aos alunos de graduação.
O foco principal é fazer uma introdução à teoria de curvas elípticas e como aplicação, utilizá-las 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. 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 algoritmos para fatorar números inteiros, um deles é o algoritmo de Lenstra que utiliza curvas elípticas.
Com o objetivo de apresentar um texto que contenha todos os pré-requisitos necessários, inicialmente faremos uma rápida revisão sobre os polinômios de duas e três variáveis e talmbém os polinômios homogêneos. Em seguida definiremos o espaço projetivo e estudaremos a relação dos objetos geométricos nos espaços afim e projetivo. Essa relação é exemplificada por retas e cônicas. Nesse momento temos os pré-requisitos necessários para definir as cúbicas.
Após a definição e apresentar 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 dessa 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 desses por meio da operação definida anteriormente, ou seja, o grupo dos pontos racionais de uma curva elíptica racional é finitamente gerado.
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, faremos alguns exemplos para ilustrar o funcionamento desses algoritmos.

2 Preliminares

Nesta seção reunimos alguns resultados básicos que serão utilizados nos próximos capítulos. As demonstrações dos resultados poderão ser consultadas na bibliografia apresentada.
Sempre K representa o corpo dos números reais ou complexos, os quais serão denotados por $\mathbb{R}$ e $\mathbb{C}$ respectivamente. O conjunto dos números racionas é denotado por $\mathbb{Q}$, dos números inteiros por $\mathbb{Z}$, e dos inteiros não negativos por $\mathbb{N}$.

2.1 Polinômios

Definição 2.1 *Um polinômio na variável x com coeficientes em K é uma expressão da forma $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, onde $n \in \mathbb{N}$ e $a_0, \ldots, a_n \in K$. Dois polinômios $p(x) = a_n x^n + \cdots + a_0$ e $q(x) = b_m x^m + \cdots + b_0$ são iguais, se $n = m$ e $a_i = b_i$ para todo $i = 0, \ldots, n$.*

SALEHYAN, P. Um algoritmo de fatoração dos números inteiros usando curvas elípticas. **C.Q.D. Revista Eletrônica Paulista de Matemática**, Bauru, v. 23, n. 1, p. 205–223, jul. 2023.
DOI: 10.21167/cqdv23n1ic2023205223 Disponível em: https://sistemas.fc.unesp.br/ojs/index.php/revistacqd/index

O conjunto de todos os polinômios na variável x com coeficientes em K é denotado por $K[x]$. Esse conjunto, munido das operações adição e multiplicação definidas a seguir, possui estrutura de um anel comutativo com unidade. Sejam $p(x) = a_n x^n + \cdots + a_0, q(x) = b_m x^m + \cdots + b_0 \in K[x]$ tais que $m \geq n$. Defina $a_i := 0$ se $i > n$.

- Adição: para todo $0 \leq i \leq m$, seja $c_i := a_i + b_i$, então

$$p(x) + q(x) := c_m x^m + \cdots + c_0;$$

- Multiplicação: para todo $0 \leq i \leq m + n$, seja $c_i := \sum_{j=0}^{i} a_j b_{i-j}$

$$p(x) \cdot q(x) := c_{m+n} x^{m+n} + \cdots + c_0.$$

O maior n tal que $a_n \neq 0$ é chamado do *grau* de $p = p(x)$ e denotado por $\deg p$ e a_n é chamado do *coeficiente líder*. Chamamos a_0 do *termo constante*. O grau do polinômio zero, $p = 0$, é definido como $-\infty$. Por convenção, para todo $n \in \mathbb{Z}$,

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

Nenhuma outra operação é definida com $-\infty$. Usando estas convenções, podemos mostrar que

$$\deg(pq) = \deg p + \deg q, \quad \deg(p + q) \leq \max\{\deg p, \deg q\}.$$

Observamos que as operações acima são baseadas apenas nas operações entre os coeficientes. Portanto podemos definir os polinômios de uma maneira um pouco mais geral, ou seja, considerar um anel comutativo com unidade como o conjunto dos coeficientes e a partir disso definir polinômios e operações entre eles de forma análoga ao caso de $\mathbb{R}$ ou $\mathbb{C}$. Em particular, definiremos o anel de polinômios em duas e três variáveis.

Definição 2.2 *O anel de polinômios em duas variáveis x e y é definido como $K[x, y] := K[x][y]$. Mais precisamente um polinômio em duas variáveis é uma expressão finita da forma $\sum p_i(x) y^{n_i}$, onde $p_i(x) \in K[x]$ e $n_i \in \mathbb{N}$.*

É comum considerar a forma geral de um polinômio em duas variáveis como uma soma finita $p(x, y) := \sum a_{mn} x^m y^n$, onde $a_{mn} \in K$ e $m, n \in \mathbb{N}$. Cada termo $a_{mn} x^m y^n$ é chamado de um *monômio* e seu grau é definido por $m + n$. O grau de p é definido como o maior inteiro entre os graus desses monômios. Se todos os monômios tiverem o mesmo grau, ou seja, se existe $d \in \mathbb{N}$ tal que $m + n = d$ para todo m e n, então p é chamado de *polinômio homogêneo*. É fácil mostrar que p é homogêneo de grau d se, e somente se para todo $\lambda \in K$, $p(\lambda x, \lambda y) = \lambda^d p(x, y)$. As operações de adição e multiplicação são definidas da forma análoga ao caso de uma variável, ou seja, assumindo as regras de comutatividade e distribuição de multiplicação em relação à adição e $x^{i_1} y^{j_1} \cdot x^{i_2} y^{j_2} := x^{i_1+i_2} y^{j_1+j_2}$. É um exercício simples verificar que $K[x, y]$ munido dessas operações se torna um anel comutativo com unidade.
O conjunto dos polinômios em três variáveis é definido como $K[x, y, z] := K[x, y][z]$. Um polinômio de três variáveis pode ser escrito como uma soma finita $\sum a_{ijk} x^i y^j z^k$. Por indução podemos definir o conjunto de polinômios em n variáveis $x_1, \ldots, x_n$ com coeficientes em K por $K[x_1, \ldots, x_n] := K[x_1, \ldots, x_{n-1}][x_n]$. Os conceitos de monômio, grau, homogeneidade e as operações entre polinômios são generalizadas naturalmente.

2.2 Espaço Projetivo

Nos cursos elementares de geometria análitica, 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. Outro exemplo é a interseção da reta dada pela equação $x = 0$ e a hipérbole dada pela equação $xy = 1$. Essa *falha* do plano cartesiano pode ser superada se estudarmos esses problemas no *plano projetivo* construído a seguir.

Seja $K^3 = K \times K \times K$. Em $K^3 \setminus \{(0,0,0)\}$ defina a seguinte relação:

$$(a_0, a_1, a_2) \sim (b_0, b_1, b_2) \Leftrightarrow \exists \lambda \in K \setminus \{0\}; (a_0, a_1, a_2) = \lambda(b_0, b_1, b_2).$$

Em outras palavras, dois pontos distintos da origem são relacionados, se pertencem a mesma reta que passa pela origem. Essa relação é de equivalência e o conjunto quociente

$$\mathbb{P}^2_K := \frac{K^3 \setminus \{(0,0,0)\}}{\sim}$$

é chamado de *plano projetivo*. Geometricamente $\mathbb{P}^2_K$ é o conjunto de todas as retas em K^3 que passam pela origem. A classe de (a_0, a_1, a_2), ou, um ponto de $\mathbb{P}^2_K$ é denotado por $(a_0 : a_1 : a_2)$. Chamaremos a_0, a_1 e a_2 de *coordenadas homogêneas* do ponto $(a_0 : a_1 : a_2)$.

Agora explicamos como plano projetivo resolve as *falhas* do plano cartesiano. A aplicação

$$\begin{cases} \iota & : & K^2 & \longrightarrow & \mathbb{P}^2_K \\ & & (a_0, a_1) & \longmapsto & (a_0 : a_1 : 1) \end{cases}.$$

é injetiva, então ao identificar K^2 com sua imagem em $\mathbb{P}^2_K$, podemos considerar o plano cartesiano como um subconjunto do plano projetivo, em outras palavras, $\mathbb{P}^2_K$ possui uma cópia de K^2. Essa cópia é o plano dado pela equação $z = 1$ se usarmos (x, y, z) para denotar os pontos de K^3. Lembrando a definição da relação de equivalência, $\iota(K^2) = \{(a_0 : a_1 : a_2) | a_2 \neq 0\}$. Defina $H_\infty := \mathbb{P}^2_K \setminus \iota(K^2)$. Então $\mathbb{P}^2_K = \iota(K^2) \cup H_\infty$. Novamente pela definição,

$$H_\infty = \{(a_0 : 1 : 0) | a_0 \in K\} \cup \{(1 : 0 : 0)\}.$$

Os pontos de H_∞ são chamados de *pontos no infinito*. Existe também a aplicação

$$\begin{cases} \widetilde{\iota} & : & \iota(K^2) & \longrightarrow & K^2 \\ & & (a_0 : a_1 : a_2) & \longmapsto & (\frac{a_0}{a_2} : \frac{a_1}{a_2}) \end{cases}.$$

Observamos que $\iota \circ \widetilde{\iota} = \mathrm{id}_{\iota(K^2)}$ e $\widetilde{\iota} \circ \iota = \mathrm{id}_{K^2}$. Utilizando ι e $\widetilde{\iota}$ podemos visualizar os *objetos* de K^2 em $\mathbb{P}^2_K$ e também olhar para os objetos no plano projetivo como união de seus pontos no infinito e o complementar desses pontos que é chamado de sua parte *afim*.

Exemplo Seja $l \subset K^2$ a reta dada pela equação $y = mx + h$. Para obter $\iota(l)$ devemos fazer as mudanças $x \longrightarrow \frac{x}{z}$ e $y \longrightarrow \frac{y}{z}$. Então $\iota(l) = \{(x : y : z) | mx - y + hz = 0\}$. O único ponto no infinto de $\iota(l)$ é $(1 : m : 0)$. No caso da reta l' dada pela equação $x - a = 0$, $\iota(l') = \{(x : y : z) | x - az = 0\}$ e seu ponto no infinito é $(0 : 1 : 0)$. Consequentemente concluímos que as retas paralelas $y = mx + h$ e $y = mx + h'$ possuem ponto $(1 : m : 0)$ em comum quando vistas no plano projetivos.

Exemplo Seja $C = \{(x : y : z) | x^2 - y^2 - z^2 = 0\} \subset \mathbb{P}^2_K$. Ao substituir $z = 0$, obtemos $x^2 - y^2 = 0$, ou, $x = \pm y$. Então os pontos no infinito de C são $(1 : \pm 1 : 0)$. Sua parte afim é dada pela equação

$x^2 - y^2 = 1$ o que é uma hipérbole. Então podemos pensar em C como a união de uma hipérbole e dois pontos no infinito.

Exemplo A hipérbole e a reta dadas pelas equações $xy = 1$ e $x = 0$ não se intersectam 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.

3 Cúbicas

Nesta seção faremos uma breve introdução às curvas cúbicas planas projetivas. Após a definição e os exemplos, falaremos de suas classificações. Veremos a estrutura de um grupo abeliano no conjunto dos pontos dessas curvas. Comentaremos vários resultados sobre esse grupo. A maioria das demonstrações precisam de estudos um pouco mais avançdos e por isso não serão apresentadas. Mas sua importância e sua utilidade são esclarecidas por meio dos exemplos.

Definição 3.1 *Sejam K um corpo e $P \in K[x, y, z]$ um polinômio homogêneo de grau 3. O conjunto dos zeros de P, denotado por $V(P)$, é chamado de uma cúbica plana projetiva ou simplesmente uma cúbica.*

Exemplo As cúbicas: $C_1 : y^2z = x^3$, $C_2 : y^2z = x^2(x + z)$ e $C_3 : y^2 = x(x - z)(x - 2z)$ 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 $y^2 = x(x - 1)(x - 2)$, veja a Figura 1.

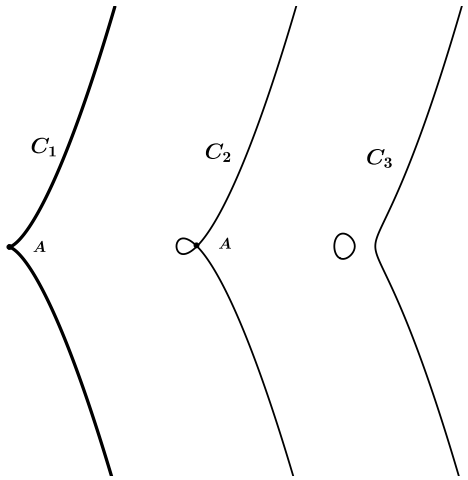

Figura 1:

As curvas citadas no exemplo anterior são bons exemplos para observar o seguinte fato: em todos os pontos de C_3 podemos escrever a equação da reta tangente à curva, o que não acontece no caso de C_1 e de C_2. Isto ocorre pelo fato de que as funções implícitas $y^2 = x^3$ e $y^2 = x^2(x + 1)$ não possuem derivada no ponto $A(0, 0)$. As derivadas parciais destas funções nesse ponto se anulam. Isso não acontece no caso de C_3, em cada ponto pelo menos uma das derivadas parciais não é nula. Essa observação nos leva a dar a seguinte definição. Denote as derivadas parciais usuais por $\frac{\partial}{\partial x}$, $\frac{\partial}{\partial y}$ e $\frac{\partial}{\partial z}$.

Definição 3.2 *Um ponto* $(a : b : c) \in C = V(P)$ *é dito um ponto singular se* $\frac{\partial}{\partial x}P(a : b : c) = \frac{\partial}{\partial y}P(a : b : c) = \frac{\partial}{\partial z}P(a : b : c) = 0$. *Se* C *tiver pelo menos um ponto singular, então é chamada de uma curva singular, caso contrário é uma curva suave ou não singular.*

Exemplo Pela observação feita antes da Definição 3.2 as curvas C_1 e C_2 são singulares e C_3 é uma curva suave.

Definição 3.3 *Uma cúbica* $C = V(P)$, $P \in K[x, y, z]$, *é chamada de irredutível, se* P *for um polinômio irredutível em* $K[x, y, z]$, *caso contrário, diremos que* C *é redutível.*

Seja $C = V(P)$ uma cúbica. Dependendo do número de fatores de P teremos os seguintes casos para uma cúbica redutível: união de uma reta com uma cônica e união de três retas. Cada um destes casos possui várias configurações, como mostrado na Figura 2. As cúbicas redutíveis são singulares.

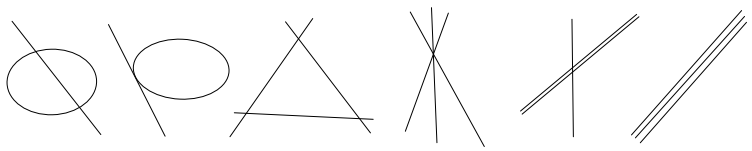

Figura 2: Cúbicas Redutíveis

Isso pode ser verificado facilmente usando a Definição 3.2. De fato, se $P = GH$, então utilizando a regra da derivada do produto, os pontos de $V(G) \cap V(H)$ são pontos singulares de $V(P)$.

3.1 Classificação de Cúbias Planas Projetivas

Em geometria analítica aprendemos a classificação de cônicas, ou seja, aprendemos que para trabalhar com uma cônica não precisamos considerar uma equação geral de grau dois, é suficiente considerar apenas alguns casos particulares. Isso é garantido por meio de mudanças de coordenadas, ou seja, aplicações $T : K^2 \to K^2$ da forma $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto A \begin{pmatrix} x \\ y \end{pmatrix} + B$, onde A é uma matriz 2×2 invertível e $B \in K^2$. Se quisermos classificar as cônicas em $\mathbb{P}^2_K$, ou seja, o conjunto dos zeros de uma equação dada por um polinômio homogêneo de grau 2, devemos trabalhar com aplicações $\mathbb{P}^2_K \to \mathbb{P}^2_K$ induzidas pelas transformações lineares de K^3. Mais precisamente:

Definição 3.4 *Uma mudança de coordenadas projetivas de* $\mathbb{P}^2_K$ *é uma aplicação dada por* $P \mapsto AP$, *onde* A *é uma matriz invertível de ordem 3 e* $P(x : y : z) \in \mathbb{P}^2_K$ *é representado da forma* $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$.

Diremos que $X_1, X_2 \subset \mathbb{P}^2_K$ *são projetivamente equivalentes, se existe uma mudaça de coordenadas projetivas* T *tal que* $T(X_1) = X_2$.

Exemplo As cônicas $C_1, C_2 \subset \mathbb{P}^2_{\mathbb{C}}$ 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: $(x : y : z) \mapsto (ix - z : y : ix + z)$.

Usando mudança de coordenadas, podemos obter formas muito simples para cúbicas. Esta classificação pode ser feita em qualquer corpo mesmo com característica positiva. Nesse texto precisamos apenas de caso em que a característica é zero, uma vez que trabalhamos com $\mathbb{C}$ ou seus subcorpos. Os demais casos podem ser encontrados em [1].

Teorema 1 *Seja $L \subseteq \mathbb{C}$ um corpo. Uma cúbica suave definida sobre L é projetivamente equivalente à cúbica $y^2z = x(x - z)(x - \lambda z)$, onde $\lambda \in L \setminus \{0, 1\}$.*

A demonstração desse teorema pode ser encontrada em [1] e [2]. O único ponto no infinito de uma cúbica projetiva suave dada no Teorema 1 é $O = (0 : 1 : 0)$ 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. Essa forma de apresentar uma cúbica afim suave é conhecida por sua *forma de Weierstrass*. A forma apresentada no Teorema 1 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 3. 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.

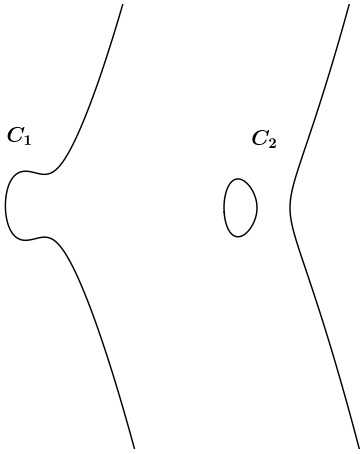

Figura 3: Cúbicas com uma ou duas componentes reais

Teorema 2 *Uma cúbica singular é projetivamente equivalente à cúbica $y^2z = x^3$ ou $y^2z = x^2(x+z)$.*

Veja [1] para sua demonstração. Observamos que em cada um dos casos no Teorema 2, existe apenas um ponto singular. O ponto singular de $y^2z = x^3$ é chamado de *cúspide* e de $y^2z = x^2(x + z)$ é chamado de *nó*, veja as cúbicas C_1 e C_2 na Figura 1.

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 desses objetos tão fácies de serem

definidos, veja [3]. Um dos problemas onde essas curvas aparecem é calcular perímetro de uma elipse. Esse 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 3.5 *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 1, uma curva elíptica sobre $\mathbb{Q}$ é

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

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

3.2 Operação entre os Pontos e suas Propriedades

Nesta seção definiremos uma operação entre os pontos de uma curva elíptica C e mostraremos que esse conjunto munido dessa operação possui estrutura de um grupo abeliano. É fácil verificar que uma reta e uma curva elíptica possuem três pontos em comum, não necessariamente distintos. Portanto dados dois pontos de C, existe outro ponto de C, em geral distinto dos pontos dados. Sejam $P, Q \in C$, e O seu único ponto no infinito (Teorema 1). A operação é definida da seguinte forma:

• Considere a reta que passa por P e Q, obtenha o terceiro ponto de interseção dessa reta com a cúbica e denote por $R := P * Q$;

• Analogamente obtenha $R * O$. Esse último é a *soma* de P e Q denotado por $P + Q$.

Uma vez que dados dois pontos, existe apenas uma única reta que passa pelos dois portanto a operação está bem definida e é comutativa. Pela construção, observamos

- $O * O = O$, portanto $O + O = O$;
- $P + O = P$, para todo $P \in C$, ou seja, O é o elemento neutro da operação;
- $O * P$ é o inverso de P, denotado por $-P$.

Falta apenas demonstrar a associatividade dessa operação para poder afirmar que $(C, +)$ é um grupo abeliano. A demonstração geométrica da associatividade pode ser encontrada em [4]. A seguir obteremos explicitamente as coordenadas de $P_1 + P_2$ com as quais podemos mostrar algebricamente a associatividade.

Pelas obsevações feitas acima, basta determinar $P_1 + P_2$ quando $P_1(x_1, y_1), P_2(x_2, y_2) \in C_f$, a parte afim de C. Pelo teorema 1, podemos considerar C_f na sua forma de Weierstrass, ou seja,

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

onde $f \in \mathbb{C}[x]$ possui raízes simples. Sejam $L : y = mx + n$ a reta que passa por P_1 e P_2 e x_3, y_3 as coordenadas de $P_1 * P_2$.

Se $x_1 \neq x_2$, então as primeiras coordenadas dos pontos de $L \cap C_f$ satisfazem a equação

$$(mx + n)^2 = f(x) = x^3 + ax^2 + bx + c \Rightarrow x^3 + (a - m^2)x^2 + (b - 2mn)x + (c - n^2) = 0.$$

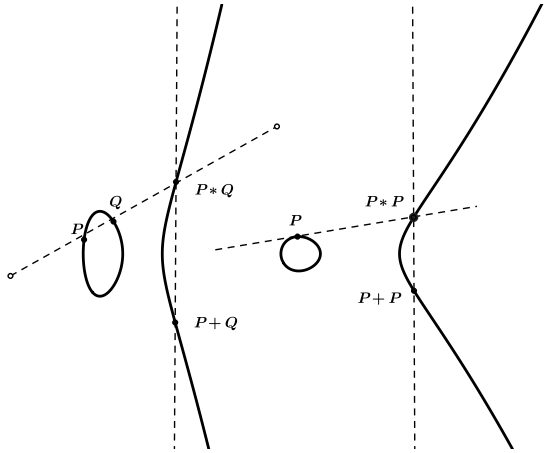

Figura 4: Operação

Utilizando a relação entre a soma das raízes e os coeficientes 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 $n = y_1 - mx_1$. Nesse 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 $P_1 * P_1 = O$, portanto $P_1 + P_1 = O$. Quando $P_1 \neq P_2$, a equação de L é $x = x_1$, portanto $P_1 * P_2 = O$ e $P_1 + P_2 = O$.

Usando essas fórmulas para $P_1 + P_2$, podemos verificar facilmente a associatividade. Outro fato muito importante é o seguinte. Considere um corpo $K \subset \mathbb{C}$, $f \in K[x]$ e os pontos de C_f cujas coordenadas pertencem a K, ou seja, $C_f(K) := \{(x, y) \in C_f | x, y \in K\}$. Essas fórmulas mostram que

Proposição 1 *$(C_f(K) \cup \{O\}, +)$ é um subgrupo de $(C, +)$. Em particular $(E(\mathbb{Q}), +)$ é um grupo abeliano.*

Na definição dada para a adição dos pontos C, tudo é feito a partir de um *ponto fixo*, nesse caso o ponto no infinito. Essa escolha facilita obter as fórmulas explícitas. Mas tomando qualquer outro ponto de C podemos definir a operação usando o mesmo processo e obter um grupo abeliano. O teorema a seguir garante que esses grupos são isomorfos.

Teorema 3 *(Poincaré) Sejam C uma cúbica suave, O seu ponto no infinito e $\mathcal{P} \in C$. Denote por $+'$ a operação definida em C tomando $\mathcal{P}$ como o ponto fixo. Então $A +' B = A + B - \mathcal{P}$, para todo $A, B \in C$. Em particular $A \mapsto A - \mathcal{P}$ define um isomorfismo entre $(C, +')$ e $(C, +)$.*

Para a demonstração do teorema 3, veja [5].

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 Por meio de mudança de coordenadas projetivas, veja [5], podemos transformar a equação $u^3 + v^3 = w^3$ na $y^2z = x^3 - \frac{27}{4}z$. A cúbica dada por $y^2z = x^3 - \frac{27}{4}z$ é chamada de *cúbica de Fermat*. As soluções triviais de $u^3 + v^3 = w^3$ correspondem a 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 $P_1 + P_2 = O$ e $P_1 * P_1 = P_1$, portanto $P_1 + P_1 = P_2$, ou, $3P_1 = O$.

Exemplo Por meio de mudança de coordenadas projetivas, veja [5], o caso quártica do último teorema de Fermat, $u^4 + v^4 = w^4$, se transforma em $y^2z = x^3 - 4xz^2$. Nesse caso as soluções triviais correspondem a $\{O, (0,0), (2,0), (-2,0)\}$. Como todos esses pontos possuem ordem no máximo dois, $E(\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Essa é uma propriedade das curvas elípticas $y^2 = x^3 - n^2x$, onde n é um inteiro livre de quadrados.

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

3.3 Teorema de Mordell-Weil

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, 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 $n_1, \ldots, n_r \in \mathbb{Z}$. Este resultado foi apresentado por Poincaré como uma conjectura por volta de 1900 e somente cerca de duas décadas depois foi demonstrado por Mordell. Sua demonstração pode ser encontrada em [6].

Teorema 4 *O grupo dos pontos racionais de uma curva elíptica é um grupo abeliano finitamente gerado.*

Pela classificação de grupos abelianos finitamente gerados,

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

onde $E(\mathbb{Q})_{tor}$ 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 $E(\mathbb{Q})$ ser abeliano e finitamente gerado, $E(\mathbb{Q})_{tor}$ 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 $O(0:1:0)$. Portanto naturalmente surgem várias perguntas: quais são os grupos finitos que podem aparecer como $E(\mathbb{Q})_{tor}$, bem como são as possibilidades do posto e se há técnicas para determiná-los explicitamente. No caso de $E(\mathbb{Q})_{tor}$ um resultado de Mazur determina todas as possibilidades, em particular fornece uma cota para $\#E(\mathbb{Q})_{tor}$.

Teorema 5 *(Mazur) Se $E(\mathbb{Q})_{tor}$ não for trivial, então é isomorfo a um desses 14 grupos:*

$$\mathbb{Z}_n, n = 2, \ldots, 10, 12; \;\; \mathbb{Z}_2 \times \mathbb{Z}_2; \; \mathbb{Z}_2 \times \mathbb{Z}_4; \; \mathbb{Z}_2 \times \mathbb{Z}_6; \; \mathbb{Z}_2 \times \mathbb{Z}_8.$$

Em particular $\#E(\mathbb{Q})_{tor} \leq 16$.

Esse teorema foi apresentado por Mazur nos anos 1970. As demostrações podem ser encontradas em [7] e [8]. Segundo esse teorema a ordem dos pontos de $E(\mathbb{Q})_{tor}$ é no máximo 12 e não existem pontos de ordem 11. Para cada um desses grupos apresentados no teorema 5 existem exemplos. Para a lista completa veja [9]. Isso em particular garante que 16 é a melhor cota para $\#E(\mathbb{Q})_{tor}$. Além disso, existe a forma precisa das curvas elípticas cujo grupo de torção seja isomorfo a cada um dos grupos apresentados no teorema 5, a lista completa pode ser encontrada em [10]. Para determinar os pontos de ordem finita o seguinte teorema é muito útil. Sua demosntração pode ser encontrada em [6].

Teorema 6 *(Nagell-Lutz) Sejam $y^2 = f(x) \in \mathbb{Z}[x]$ uma curva elíptica e $P(x, y)$ um ponto racional de ordem finita. 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[1] de f.*

Exemplo Aplicamos o teorema 6 para $y^2 = x^3 - x^2 + x$. Claramente $P(0, 0)$ 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 $2P_1 = 2P_2 = P(0, 0)$ e P possui ordem 2, conluímos que P_1 e P_2 são de ordem 4. Então $E(\mathbb{Q})_{tor} \simeq \mathbb{Z}_4$.

Outro resultado muito útil e fácil de usar é redução a módulo números primos, para detalhes veja [6]. Por meio dos resultados citados acima é fácil determinar $E(\mathbb{Q})_{tor}$. Quanto ao posto a situação é bem mais complicada. Até agora não existe um método eficiente para determiná-lo em geral. Existe uma conjectura que afirma que 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, digamos, α, β e γ. Seja d o discriminante de f. Diremos que um primo p é

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

Sejam n_1 e n_2 números primos quase ruim e muito ruim respectivamente. Então o posto de $E(\mathbb{Q})$ é no máximo $n_1 + 2n_2 - 1$, veja [5]. Existem resultados sobre o posto de algumas cúbicas. Por exemplo para alguns inteiros n as curvas elípticas dadas pela equação $y^2 = x^3 - n^2x$ possuem posto zero, logo $E(\mathbb{Q})$ é finito, veja [5].

3.4 Caso Singular

Nesta seção falaremos um pouco sobre as cúbicas singulares. Veremos o que acontece se tentarmos definir a mesma operação definida no caso suave e se o teorema de Mordell-Weil vale nesse caso.

Seja C uma cúbica singular. Pelo teorema 2, $S = (0 : 0 : 1)$ é o único ponto singular de C. Seja $C_{ns} = C \setminus \{S\}$. Dados $P, Q \in C_{ns}$, podemos definir $P + Q$ da forma análoga ao caso suave e verificar que $(C_{ns}, +)$ possui estrutura de um grupo abeliano, o ponto no infinito permanece como o elemento neutro. Além disso, se P e Q forem pontos racionais, então $P + Q$ também será, isto é, $(C_{ns}(\mathbb{Q}), +)$ é um grupo (abeliano). Então faz sentido perguntarmos se o teorema de Mordell-Weil vale para $(C_{ns}(\mathbb{Q}), +)$. Infelizmente a respsota é *negativa*!
Certamente uma condição necessária para $(C_{ns}(\mathbb{Q}), +)$ não ser finitamente gerado é que $C_{ns}(\mathbb{Q})$ seja infinito. As parametrizações das cúbicas singulares definidas a seguir garantem que C_{ns} são infinitos. Lembre-se que no caso suave isto nem sempre acontece, por exemplo a cúbica de Fermat possui apenas 4 pontos racionais. Vale destacar que as curvas elípticas não possuem parametrização racional.

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

No caso da cúbica nodal $C : y^2 = x^3 + x^2$ a parametrização é dada da seguinte forma. Para todo $P(x, y) \in C_{ns}$, $x \neq 0$; e $S = (0, 0)$ é seu ponto singular. Então a aplicação

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

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 $(x, y) \in C_{ns}$ e $\frac{y}{x} = r$. Usando $(\frac{y}{x})^2 = x + 1$, basta tomar $x = r^2 - 1$ e $y = r^3 - r$. Isso de fato define a inversa de ν:

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

No caso da cúspide $C : y^2 = x^3$, usando a mesma ideia do caso nodal, obteremos as seguintes aplicações:

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

Observem que geometricamente essas parametrizações são obtidas pela interseção das retas $y = rx$, $r \in \mathbb{Q}$, e a curva $C : y^2 = x^3$. A existência dessas 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.

Lembrando que $(\mathbb{Q}, +)$ e $(\mathbb{Q}^*, \cdot)$ não são grupos finitamente gerados, a consequência imediata do próximo teorema é que o teorema de Mordell-Weil não vale para as cúbicas singulares.

Teorema 7 *Seja C a cúbica singular $y^2 = x^3 + x^2$. Então $\phi : C_{ns} \to \mathbb{Q}^*$ definido por*

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

é um isomorfismo entre grupos. No caso da cúbica singular $C : y^2 = x^3$ a aplicação $\varphi : C_{ns} \to \mathbb{Q}$ definida por

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

é um isomorfismo entre grupos.

A demonstração desse teorema é fácil e pode ser consultada em [6].

O único elemento de ordem finita de $(\mathbb{Q}, +)$ é zero, então pelo Teorema 7 a cúbica cuspidal possui apenas o ponto O de ordem finita. Como $(\mathbb{Q}^*, \cdot)$ possui apenas um elemento não trivial de ordem finita, -1 é de ordem 2, concluímos que a cúbica nodal possui apenas um ponto de ordem finita (exceto O), $(-1, 0)$ é de ordem 2.

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 de números grandes que são as chave 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. Lembrem que esse teorema afima que se $a \in \mathbb{Z}$ e p primo tais que $(a, p) = 1$, então $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$. Em particular, se n é primo ímpar, então $2^{n-1} \equiv 1 (\mathrm{mod}\ n)$. Isto é, se $2^{n-1} \not\equiv 1 (\mathrm{mod}\ n)$, então n não é primo. Outra maneira seria usar o teorema de Al-Haytham/Wilson: n é primo, se, e somente se, $(n-1)! \equiv -1 (\mathrm{mod}\ n)$.

Para fatorar o número n o primeiro e mais natural modo de fazer isso é tomar os números naturais $k < n$ e verificar se esses são faoroes de n. Esse método pode ser otimizado usando o fato de que o menor fator de n é menor ou igual a $\sqrt{n}$, mas mesmo assim para números grandes não é muito prático. Antes de apresentar alguns métodos mais eficientes de fatoração, veremos um método para calcular $a^k (\mathrm{mod}\ n)$ e estimar o número de operações para esse cálculo. Além disso, faremos uma estimativa para o número de operações necessáarias 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.

Problema 1. Dados $a, k, n \in \mathbb{N}$, calcular $a^k (\mathrm{mod}\ n)$, e o número de operações para isso.

Escrevemos k na base 2:

$$k = k_0 + k_1 \cdot 2 + k_2 \cdot 2^2 + k_3 \cdot 2^3 + \cdots + k_{r-1} \cdot 2^{r-1} + 2^r, \quad \forall i, k_i \in \{0, 1\}.$$

Então a^k = (produto dos a^{2^i}s para cada $k_i = 1$). Portanto para calcular $a^k (\mathrm{mod}\ n)$ basta calcular $A_i := a^{2^i} (\mathrm{mod}\ n)$ e em seguida multiplicá-los. Além disso, observem que $A_0 = a,\ A_1 = A_0^2,\ A_2 = A_1^2, \ldots, A_r = A_{r-1}^2$. 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 2 *Dados $a, k, n \in \mathbb{N}$, é possível calcular $a^k (\mathrm{mod}\ n)$ em no máximo $2 \cdot \log_2 k$ operações, onde cada operação consiste de uma multiplicação e uma redução módulo n.*

Esse método para calcular $a^k (\mathrm{mod}\ n)$ 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 de 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. Esse algoritmo é baseado em fazer divisões sucessivas:

$$\begin{aligned} a &= bq_1 + r_2, \ \ 0 \leq r_2 < b, \\ b &= r_2q_2 + r_3, \ \ 0 \leq r_3 < r_2, \\ r_2 &= r_3q_3 + r_4, \ \ 0 \leq r_4 < r_3, \\ &\vdots \\ r_{n-1} &= r_nq_n + r_{n+1}, \ \ 0 \leq r_{n+1} < r_n, \\ r_n &= r_{n+1}q_{n+1}. \end{aligned}$$

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

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

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

$$r_{i-1} = r_iq_i + r_{i+1}, \quad 0 \leq r_{i+1} < r_i$$

implica

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

Claramente $q_i \neq 0$, pois caso contrário $r_{i-1} = r_{i+1}$ e isso 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 (✠), 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 3 *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.

4.1 Algoritmo de Pollard

Esse algoritmo constitui um protótipo daquilo que iremos estudar posteriormente: a fatoração por meio de 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 $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$. Assim $p|(a^{p-1}-1, n)$. Não conhecemos p, portanto não podemos calcular $a^{p-1}-1$. Então escolheremos um inteiro da forma $k = p_1^{e_2} p_2^{e_3} \cdots p_r^{e_r}$, onde $p_1 = 2, p_2 = 3, \ldots, p_r$ são os primeiros r primos e e_i são inteiros positivos pequenos. Calculamos $d := (a^k - 1, n)$. Observamos que é necessário calcular $a^k - 1 (\mathrm{mod}\, n)$. 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 $n = 246082373$. A primeira coisa a verificar é se n não é primo: como $2^{n-1} (\mathrm{mod}\, n) \neq 1$, então n é composto. Aplicaremos o algoritmo de Pollard tomando

$$a = 2 \ \text{ e } \ k = 2^2 \cdot 3^2 \cdot 5 = 180.$$

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

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

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,

$$k = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520 = 2^3 + 2^4 + 2^6 + 2^7 + 2^8 + 2^{11}.$$

Usando o mesmo método,

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

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. Poderíamos obter essa fatoração verificando a divisibilidade de n por todos os primos menores ou iguais a $\sqrt{n} \approx 15687$ por meio de um computador, mas dessa 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. Esse algoritmo não é muito prático para grandes valores de n; de fato funciona bem, ou seja, determina uma 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 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 $\#C(\mathbb{Z}_p)|k$, então $kP = O$ 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 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, esse algoritmo funcionará se para algum fator primo p de 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 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 obsevar também o seguinte fato: se C é uma cúbica não sigular com coeficientes em $\mathbb{Z}_p$, então pelo teorema de Hasse-Weil, veja [6],

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

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.

4.2 Algoritmo de curvas elípticas de Lenstra

Seja $n \geq 2$ um inteiro composto para o qual buscamos um fator.

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.

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

voltamos 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 nesse 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 $kP = O$, mais precisamente, $kP(\text{mod } p)$ é o ponto no infinito O. Então $p|d_k$, logo $p|D$. Consequentemente obteremos um fator de n, a não ser que $n|d_k$.

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

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

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 então 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 $\mathbb{Z}_n$. Nesse caso $\mathbb{Z}_n$ não é um corpo e $x_2 - x_1$ pode não ser invertível. Lembre-se que $x_2 - x_1$ possui inverso, se, e somente se, $(x_2-x_1, n) = 1$. Se $1 < (x_2-x_1, n) < n$, então 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 devemos calcular (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 $n = 1715761513$. Primeiramente verificamos se n não é primo. Como

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

pelo pequeno teorema de Fermat concluímos que 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, portanto 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 $k = 2 \cdot 3 \cdot 5 \cdots 17 = 12252240$, 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 estas 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 há 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

$$y^2 = x^3 + 42x - 91 \pmod n$$

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 isto não fosse possível, teríamos de aumentar o valor de k por exemplo para $2 \cdot 3 \cdots 19 \cdot 23$ e talvez até tomar um outro ponto, por exemplo $P(3, 1)$.

Referências

[1] HEFEZ, A. **Introdução à geometria projetiva**. Rio de Janeiro: IMPA, [1990?].

[2] VAINSENCHER, I. **Introdução às curvas algébricas planas**. 2. ed. Rio de Janeiro: IMPA, 2005.

[3] SILVERMAN, J. H. **The ubiquity of elliptic curves**. Dublin: [Brown University], 2007. Powerpoint, Public lecture in University College of Dublin, September 2007. Disponível em: www.math.brown.edu/johsilve/Presentations.html. Acesso em: 22 maio 2023.

[4] HUSEMOLLER, D. **Elliptic curves**. New York: Springer-Verlag, c1987. (Graduate texts in mathematics; 111).

[5] KNAPP, A. W. **Elliptic curves**. Princeton, N.J.: 1992. (Mathematical notes; 40).

[6] SILVERMAN, J. H.; TATE, J. **Rational points on elliptic curves**. New York: Springer, 1992.

[7] MAZUR, B. Modular curves and the Eisenstein ideal. **Publications Mathématiques de L'Institut des Hautes Scientifiques**, v. 47, n. 1, p. 33-186, 1977.

[8] MAZUR, B. Rational isogenies of prime degree. **Inventiones Mathematicae**, v. 44, p. 129-162, 1978.

[9] SILVERMAN, J. H. **The arithmetic of elliptic curves**. New York: Springer, 2009. *E-book*. (Graduate texts in mathematics, 106).

[10] KUBERT, D. S. Universal bounds on the torsion of elliptic curves. **Proceedings of the London Mathematical Society**, v. s3-33, n. 2, p. 193-237, 1976.