POST QUANTUM CRYPTOGRAPHY

TIAGO VERISSIMO

Abstract. Number Theory Chapter

Contents

1. Objetivos 1
2. Definições Fundamentais da Teoria 2
3. O conjunto dos naturais e a divisibilidade 2
4. Números Primos e Números Compostos 2
5. O Máximo Divisor Comum e o Mínimo Múltiplo Comum 3
6. Aritmética de Módulos e Congruências 3
7. Resultados Essenciais 3
8. Investigação Moderna 5
8.1. Novas Estruturas e Fronteiras da Investigação 5
8.1.1. Aritmética das Curvas Elípticas 5
8.2. Hipótese de Riemann 6
8.3. O Programa de Langlands 6
9. Ferramentas Computacionais 6
10. Bibliografia 7
10.1. Introdução 7
10.2. Nível Avançado 7
10.3. Investigação 7
References 7

1. Objetivos

A Teoria dos Números é uma área matemática que é primariamente destinada a estudar os números naturais, explorando os padrões e estruturas fundamentais destes mesmos, havendo um particular foco dentro do conceito de número primo e as suas relações com a divisibilidade dos outros números.

A Teoria dos Números apresenta-se como uma das primeiras áreas de conhecimento matemático humano, havendo mesmo registo em pequenas placas de barro fenícias. Grandes mentes passaram por esta área como Carl Gauss e Ramanujan, revelando-se uma área extremamente produtiva do ponto de vista matemático ainda hoje em dia, podendo-se verificar uma enorme quantidade de medalhas e prémios prestigiantes nos últimos tempos.

A Teoria dos Números é uma área onde perguntas simples conseguem ser absolutamente impossíveis de resolver, tendo assim de se recorrer a imensas áreas diversas da matemática para responder a perguntas como a proposta por Fermat, onde este conjecturara que não seria possível encontrar números (x, y, z) tais que a equação $x^n + y^n = z^n$ a partir de $n > 2$, ou como a Conjectura de Goldbach, que afirma que qualquer número par maior que 2 pode ser escrito como a soma de dois números primos, e que ainda continua por resolver. São afirmações como

esta que revelam a simplicidade das afirmações tidas, podendo estas ser entendidas por alunos de 3º ciclo de escolaridade, mas no entanto só resolvidas pelos mestres absolutos da área.

A Teoria dos Números possui uma história algo fora do comum; até ao século passado, esta seria uma área desprovida de qualquer tipo de interesses comerciais, havendo mesmo matemáticos como Harvey gabando-se da "pureza" inalcançável da área. Ora, com o advento dos computadores, mais longe da verdade não se poderia estar, dado que as nossas comunicações digitais somente se revelam seguras porque possuímos criptografia que, pondo os detalhes de engenharia à parte, está assente na enorme complexidade que se revela nos problemas de fatorização dos números naturais.

Hoje em dia a Teoria dos Números pode ser dividida entre uma área aplicada e uma área pura; dentro da matemática pura estuda-se os números e as relações e padrões entre eles de forma desinteressada com a realidade, enquanto que na área aplicada estuda-se questões algorítmicas de fatorização e algoritmos de criptografia e até mesmo a quebra deles.

2. Definições Fundamentais da Teoria

Iremos fazer uma pequena digressão pelos principais conceitos de Teoria dos Números, primeiro conceitos clássicos e depois conceitos da teoria de números moderna.

3. O conjunto dos naturais e a divisibilidade

A estrutura de definições de Teoria dos Números cresce a partir do conceito de número natural: $N = \{1, 2, ...\}$. Dentro deste conjunto o estudo da divisibilidade entre os números acaba por fazer grande parte do estudo nesta área, onde por divisibilidade entendemos pela pergunta de se um número natural a pode ser escrito como $a = bc$ ou não. Por exemplo, o número $12 = 4c \cdot 3$ é divisível por 4; no entanto, o número 3 só é divisível por 1 e mais nenhum número.

Este conceito do estudo da divisibilidade, assim como a necessidade de divisão de terrenos agrícolas e mercantis, levou ao estudo deste tipo de relações na civilização antiga. O pensador Euclides da Antiga Grécia, no seu monumental trabalho "Os Elementos", dedicou-se a pensar sobre estas questões da divisibilidade.

O primeiro registo do algoritmo de divisão. Este afirma que dado um par de números naturais (a, b) onde $b < a$, podemos então escrever $a = bq + r$ onde $0l = r < b$. Como por exemplo, repare-se que se tivermos o par $(7, 3)$, temos que $7 = 2c \cdot 3 + 1$.

4. Números Primos e Números Compostos

Dentro deste estudo da divisibilidade, naturalmente nos perguntamos quais são os números que não são divisíveis, por outras palavras, quais são os números a tais que não seja possível escrever $a = bc$, onde b e c são números diferentes (onde por questões técnicas assume-se sempre $b, cne1$). Nesta área, estes números conhecem-se como números primos. Os números primos são: $2, 3, 5, 7, 11, ...$, onde excluímos o número 1. Por oposição, temos o conceito de números compostos, que são os que não são primos, ou seja, os que são divisíveis, como por exemplo $12 = 3 \cdot 4$.

5. O Máximo Divisor Comum e o Mínimo Múltiplo Comum

Ideias naturalmente associadas ao contexto de divisibilidade são os conceitos de máximo divisor comum e mínimo múltiplo comum, que normalmente se denotam respetivamente $mdc(a,b)$ e $mmc(a,b)$ para números naturais a, b. Para calcular o $mdc(a,b)$ usa-se o algoritmo de Euclides, que se revela extremamente eficiente, dado que se procede computando uma sequência de números $(r_i)_{\{iinN\}}$ onde N é um conjunto finito da seguinte forma: Seja a e b dois números naturais com $a > b$. Aplicamos o algoritmo da divisão sucessivamente: $a = bq_1 + r_1$ $b = r_1q_2 + r_2$ ... $r_{\{n-2\}} = r_{\{n-1\}}q_n + r_n$ onde r_n é o último resto não nulo. O $mdc(a,b)$ é o valor de r_n.

Com este valor podemos calcular o $mmc(a,b)$ usando uma identidade útil: $mmc(a,b) = \frac{|a \cdot b|}{m} dc(a,b)$

6. Aritmética de Módulos e Congruências

De facto, o conceito de resto encontra-se de tal forma estudado que existe o que nós chamamos de aritmética modular. Tal faz-se através do conjunto $Z\frac{Z}{nZZ} = \{[0], ..., [n-1]\}$ onde n é um número natural, e $[i] = \{k \cdot n + i : kinZZ\}$. Podemos definir uma aritmética neste conjunto através da operação + onde nós definimos $[i] + [j] = [i + j]$ para $[i], [j]inZ\frac{Z}{nZZ}$. Para dizermos que consideramos o conjunto com estas operações, utilizamos a notação $\left(Z\frac{Z}{nZZ}, +\right)$. Tal aritmética normalmente chama-se "aritmética de relógio" e este nome deve-se ao facto de se considerarmos a aritmética $\left(Z\frac{Z}{12ZZ}, +\right)$, pois tal funciona como se fosse um relógio. Note-se como esta analogia se revela: suponha que são 11 da noite, então o seu relógio indicaria o ponteiro nas 11 e o nosso sistema iria revelar-se como [11]. Imagine que um colega seu diz-lhe que se encontra consigo daqui a 35 horas. Pode começar a contar os ponteiros no relógio para saber as horas, mas se usar a aritmética modular pode-se fazer: $[11] + [35] = [11 + 35] = [46]$. Como $46 = 3 \cdot 12 + 10$, temos $[46] = [10]$. Então o seu colega vai-se encontrar consigo às 10 da manhã do dia a seguir.

7. Resultados Essenciais

No início dos estudos da fatorização em sistemas algébricos de números, o estudo da fatorização revela-se como um interesse natural, dado que as questões de divisibilidade de números rapidamente revelam problemas desafiantes.

Um dos primeiros teoremas produzidos neste âmbito foi produzido por Euclides na Antiga Grécia; citamos o seu famoso Teorema Fundamental da Aritmética.

Theorem 7.1. *Dado um número inteiro $n > 1$, temos que este número pode ser fatorizado por números primos $p_1, ..., p_k$, sendo assim $n = p_1 \cdot ... \cdot p_k$ e estes números $p_1, ...p_k$ são únicos.*

Desta forma, nós dizemos que os primos são os átomos dos números inteiros, pois eles conseguem desconstruir estes números. Este é o estudo local dos sistemas numéricos.

Note-se por exemplo o número $30 = 2 \cdot 3 \cdot 5$ ou $6 = 2 \cdot 3$.

Neste tipo de trabalhos envolvendo a fatorização de números, tipicamente estuda-se se existem fatorizações para todos os números e se estas são únicas

para todos os números; de certa forma, andamos a perceber quais são os átomos de um dado sistema de números. Uma das formas para estudar a distribuição destes átomos nos sistemas numéricos é estudando a sua distribuição nos sistemas algébricos. Este é o estudo global dos átomos em sistemas algébricos. O principal teorema no estudo global do sistema dos números inteiros, possuímos o Teorema da Distribuição dos Primos:

Theorem 7.2. *Seja $pi(n)$ o número de primos que antecede n, então assintoticamente temos que o número de primos é dado por $pi(n) s\,\mathrm{im}\,\frac{n}{l} n(n)$.*

Temos teoremas como o referido acima que descrevem o número de primos, mas nunca sabemos bem as posições exatas ou quais são os números primos e os números compostos de forma imediata. Para fazer esta decisão precisamos sempre de algoritmos sofisticados que nem são rápidos ou então são probabilísticos. Existe assim um grande conflito entre o nosso conhecimento dos números primos em termos locais, quer isto dizer em termos de fatorizações, e em termos globais, quer isto dizer a sua distribuição. Grande motivação pela investigação na célebre Hipótese de Riemann prende-se precisamente pelo facto de esta nos vir a trazer uma perceção global sobre os números primos.

Alguns teoremas fundacionais em Teoria dos Números relativos à caracterização de números primos. Uma das primeiras caracterizações de números primos é dada por:

Theorem 7.3. *Se p é um número primo, então para qualquer número natural a que não é divisível por p, temos que $a^{p-1} \iff 1(\mathrm{mod}\, p)$*

Temos a generalização dada por Euler da caracterização de números primos dada por Fermat:

Theorem 7.4. *Sejam n, a números naturais. Suponhamos que $\varphi(n)$ é uma função que conta o número de números a tais que $mdc(a, n) = 1$. Se $mdc(a, n) = 1$, então temos que $a^{\varphi(n)} \iff 1(\mathrm{mod}\, n)$.*

Outro resultado que eu gostaria de mencionar seria o Teorema de Wilson, onde é feita uma caracterização suficiente e necessária dos números primos:

Theorem 7.5. *Um número p é primo se e só se $(p-1)! \iff -1(\mathrm{mod}\, p)$*

Por fim, convido os leitores a irem investigar por iniciativa própria o conceito de número perfeito e número de Mersenne e a sua relação com os números primos, onde podemos encontrar conjecturas simples e poderosas como:

- Conjectura de Goldbach: Todos os números naturais pares maiores que 2 podem ser escritos como uma soma de 2 números primos.
- Odd Perfect Number: Será que existe um número perfeito ímpar?
- Twin Prime Conjecture: Existem infinitos números primos que diferem exatamente por 2?

Para além dos números primos, o outro grande alvo de estudo é dado pelo estudo de equações diofantinas, ou seja, equações do tipo $\mathrm{P(x\_1,dots,x\_n)} = 0$ onde P é um polinómio de n variáveis de grau arbitrário e coeficientes nos números inteiros, e procuramos exclusivamente soluções de números inteiros.

Por exemplo, equações do tipo $3x_1^2 - 7x_2^3 = 5$ ou $x_1^2 + x_2^2 = x_3^2$.

As questões que se costumam estudar nesta área relativamente a este tipo de equações são dadas por:

- Existência de Soluções?
- Finitude ou Infinitude?
- Conseguimos explicitar as soluções?

Alguns exemplos de equações diofantinas famosas:

- Equações Lineares Diofantinas - $a_1x_1 + ... + a_nx_n = c$.
- Equação de Pell - $x^2 - Dy^2 = 1$.
- O Último Teorema de Fermat - $x^n + y^n = z^n$ para $n > 2$.

Muitas destas equações diofantinas revelam-se lindos aspetos de investigação matemática e também estupendas aplicações com encriptação usando equações diofantinas através da encriptação elíptica.

Para se perceber a profundidade deste tipo de questões, o matemático alemão David Hilbert, na sua famosa lista de problemas para o século 20 e 21, formulou o seu décimo problema:

Theorem 7.6. *Existe algum algoritmo para, na situação de equações diofantinas, sabermos se existem soluções num número finito de execuções?*

A resposta foi não intuitiva:

Theorem 7.7. *O 10º Problema de Hilbert não possui um algoritmo com os requisitos pedidos.*

Mesmo assim, existem matemáticos que vão além do razoável e conseguem demonstrar resultados assombrosos como o Último Teorema de Fermat, demonstrado por Andrew Wiles, que diz, nem mais nem menos, que, assumindo um $n > 2$, a equação a^n + b^n = c^n não possui soluções para nenhum número inteiro.

8. Investigação Moderna

A Teoria dos Números moderna representa-se como um esforço de perceber ainda mais profundamente as propriedades dos números. Porém, atualmente fazemos este estudo dos números através do estudo de teorias abstratas que nos permitem codificar certas características dos números. Por exemplo, no estudo das equações diofantinas do tipo $x^n + y^n = z^n$, o matemático Andrew Wiles, através da conversão deste problema para equações elípticas (geometria) que depois iria ser traduzido às formas modulares da análise matemática, conseguiu perceber que tais equações não têm soluções a partir de $n > 2$ no domínio dos naturais.

8.1. **Novas Estruturas e Fronteiras da Investigação.**

A Teoria dos Números atualmente é governada pelos seguintes regimes de investigação que pretendem conectar estruturas abstratas à estrutura concreta de números.

8.1.1. *Aritmética das Curvas Elípticas.*

Uma curva elíptica é uma equação cúbica como por exemplo $y^2 = x^3 + x + 1$. Estas equações apresentam propriedades extremamente contra-intuitivas, como por exemplo o facto de os números racionais que são soluções deste tipo de equações

formarem o que se apelida em álgebra abstrata de grupo, através do uso de uma operação que utiliza uma lei geométrica que estas soluções apresentam. Alguns resultados e conjecturas sobre este conceito revelam-se como:

- Teorema das Formas Modulares: Demonstrou que existe uma conexão entre curvas elípticas e formas modulares.
- A Conjectura de Birch e Swinnerton-Dyer (BSD): Este é um dos problemas do milénio apresentados pelo instituto Clay de Matemática. O Teorema propõe que existe uma

conexão entre uma curva elíptica e um objeto analítico associado a este, apelidado de função L. Nomeadamente, esta conjectura afirma que o número de zeros da função L que desvanece no chamado "ponto central" da curva elíptica é igual ao rank do grupo dos pontos racionais de uma dada curva elíptica.

8.2. **Hipótese de Riemann.**

Dado um número complexo $s = \sigma + it$, definimos a função zeta de Riemann como:

$$z\eta(s) = \sum_{n=1}^{\infty}\left(\frac{1}{n^s}\right) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + ... \tag{1}$$

Ora, a Hipótese de Riemann afirma que se $z\eta(s) = 0$, então necessariamente a parte real de s, denotada como $\mathrm{Re}(s)$, é $0 < \mathrm{Re}(s) < 1$. Caso se demonstre esta propriedade, poderíamos ter propriedades magníficas como uma fórmula explícita para contar primos de forma muito precisa e perceber a forma como os números primos se distribuem.

8.3. **O Programa de Langlands.**

O Programa de Langlands é um projeto que pretende estabelecer uma ponte entre a Teoria dos Números e a teoria de representação. Nomeadamente, consiste numa ponte que conecta a teoria das formas automorfas (funções harmónicas generalizadas da análise matemática) com a teoria das representações de Galois (representações que codificam informação aritmética de corpos de números). A dualidade entre álgebra e análise matemática é algo que há muito se tenta encontrar conexões; este programa é mais uma neste sentido, no entanto mesmo assim existem muitas outras pontes que existem e que iremos falar.

9. Ferramentas Computacionais

Dado o caráter discreto dos números naturais, não admira que os computadores sejam muito úteis na análise e implementação de ideias matemáticas. Descrevo abaixo uma série de programas que podem vir a ser úteis a pessoas que queiram entrar em Teoria dos Números ou, mais geralmente, dominar números naturais de forma computacional sem ter de recorrer a meios mais antigos.

- PARI: Um software de base de C que permite computar de forma eficiente: Fatorizações, Curvas Elípticas, Formas Modulares, funções L.
- SageMath: Software open-source generalista de desenvolvimento matemático.
- L-calc: Software especializado em computar zeros de funções L.

- Magma: Software closed-source que possui uma variedade de propriedades algébricas associadas à Teoria dos Números.

10. Bibliografia

10.1. **Introdução.**

10.2. **Nível Avançado.**

10.3. **Investigação.**

- Curvas Elípticas
- Hipótese de Riemann
- Programa de Langlands

References

Department of Mathematics, Statistics and Physics, Newcastle University, Newcastle Upon Tyne, England
Email address: t.mesquita-santos-verissimo2@newcastle.ac.uk
URL: math.ue.edu/~jdoe