TEORIA DOS NÚMEROS E CRIPTOGRAFIA RSA

Gustavo Massao Yoshitome (PIBIC/CNPq/FA/UEM) ra98534@uem.br,
Emerson Luiz do Monte Carmelo (Orientador).

Universidade Estadual de Maringá / Centro de Ciências Exatas/Maringá, PR.

Ciências Exatas e da Terra / Matemática

Palavras-chave: Números primos, Criptografia RSA, Chave pública.

Resumo

A Teoria dos Números é um ramo da matemática que estuda propriedades aritméticas de números inteiros e de certas extensões. A pedra fundamental da Teoria dos Números é o conceito de divisibilidade, que nos leva à definição de fatoração de números inteiros em primos. Tal fatoração é até hoje uma tarefa algorítmica muito difícil de ser realizada.

Por outro lado, a Criptografia consiste em métodos de “esconder” mensagem de tal maneira que apenas o emissor e receptor da mensagem consigam lê-la. A conexão entre Teoria dos Números e Criptografia está na Criptografia RSA, um método que faz uso da Teoria dos Números para criptografar mensagens de maneira extremamente segura.

Introdução

Uma das principais propriedades dos números inteiros é a fatoração em números primos. O Teorema Fundamental da Aritmética nos diz que a fatoração sempre existe e é única. Esta afirmação, apesar de parecer óbvia no primeiro momento, nos garante que se conseguirmos achar os primos cujo produto é n, não precisamos mais nos preocupar com outra possível fatoração. Entretanto, um problema que surge naturalmente desta propriedade é: *como fatorar, de forma eficiente, um dado inteiro positivo n?*

A princípio, podemos montar um algoritmo que divida este inteiro por todos outros inteiros positivos menores do que ele. Mas obviamente, este método pode ser muito ineficiente se considerarmos números muito grandes.

Para isso existem métodos para aperfeiçoar este trabalho, e até mesmos outros algoritmos que podem ser mais vantajosos em alguns casos particulares, como o algoritmo de Fermat, que fatora de maneira muito eficiente números que possuem dois fatores muito próximos entre si, ou seja, um dos fatores é próximo de sua raiz.

A Criptografia consiste em técnicas de “esconder” mensagem de tal maneira que apenas o emissor e receptor da mensagem consigam lê-la. Sabe-se que sua origem remota à Idade Antiga; há registros da sua

utilização desde as guerras do século VI A.C. como forma de comunicação entre tropas para que estratégias não fossem reveladas aos inimigos, caso alguma mensagem fosse interceptada. Entretanto, com o advento da tecnologia, compras online e transações sigilosas, métodos mais seguros foram necessários. A Criptografia RSA surgiu como uma alternativa.

Passamos agora a uma descrição breve e intuitiva da Criptografia RSA. Ela foi desenvolvida por dois matemáticos, Ron Rivest e Adi Shamir, e um cientista da computação, Leonard Adleman.

Este tipo de criptografia consiste em utilizar dois primos p e q para gerar um terceiro número inteiro, digamos n=pq. Assim, se tivermos um texto escrito apenas por letras (sem números), podemos associar cada letra a um número, e então particionar este texto em vários blocos de números que são determinados por n.

A segurança deste método vem justamente da fatoração de n, pois o texto que será criptografado só poderá ser lido se conhecermos p e q. Isto significa que a escolha dos dois números primos p e q é essencial. Claramente primos grandes garantem mais segurança, mas é necessário tomar cuidado com algoritmos, como o de Fermat, que podem fatorar n se p e q forem escolhidos de forma inconveniente.

Materiais e métodos

Embora o tema seja interdisciplinar, este projeto segue uma abordagem teórica, ambientada na matemática. Assim o método dedutivo é constituído por meio de teoremas e conceitos. Dentre eles, destacamos os seguintes:

- Princípio da Boa Ordenação e Princípio de Indução Finita,
- Divisibilidade e números primos,
- Teorema da Fatoração Única,
- Congruência,
- Aritmética modular e propriedades,
- Teorema de Fermat,
- Teorema de Euler,
- Teorema Chinês do Resto,
- Codificação por números primos e algoritmo RSA.

Tendo em vista o método utilizado no projeto, os materiais são as referencias bibliográficas listadas, em particular, a bibliografia [1] foi o foco neste estudo.

Resultados e Discussão

No campo da Teoria dos Números, estudamos diversos teoremas e problemas clássicos dessa área. A aritmética modular, por exemplo, é uma maneira de atacar problemas de uma forma mais simples, permitindo reinterpretar resultados já conhecidos e obter novos teoremas.

Dentre os resultados obtidos, foi visto o Teorema da Fatoração Única que, apesar de simples, carrega informações de grande importância, e sua

demonstração faz uso de dois importantes princípios, o Princípio da Boa Ordem e o Princípio de Indução Finita.

Outro teorema que não podemos deixar de citar é o Pequeno Teorema de Fermat. Este é um dos principais resultados para o desenvolvimento da Teoria dos Números, uma vez que a partir dele podemos obter vários outros.

Por último, podemos citar o Teorema Chinês do Resto. Apesar de não ser tão frequente quanto o Teorema de Fermat, este resultado é central para resolver sistemas de congruência, além de resolver problemas práticos muito interessantes.

Por outro lado, a criptografia RSA revela um caráter aplicado da Teoria dos Números e descreve uma ferramenta poderosa de codificação, uma vez que ela permite codificar mensagens de tal maneira que métodos como contagem por frequência revelam-se ineficientes para 'quebrar' o código. Assim, apenas o possuidor da chave de decodificação seria capaz de decifrar o código, e a única maneira de obter tal chave é por meio de um algoritmo de fatoração muito eficiente, que até hoje é desconhecido.

Conclusões

Este projeto permitiu concluir que a Teoria dos Números possui uma fundamentação teórica muito importante. Em particular, teoremas como o de Fermat e de Euler produzem resultados relevantes. Além disso, tal teoria apresenta diversos problemas em aberto e conjecturas, revelando que há muitos resultados a serem desvendados.

Mas além do estudo teórico, também é possível aplicá-la, como visto no método de Criptografia RSA. Com todo estudo teórico preliminar, pode-se concluir que de fato esta criptografia é uma das mais eficientes e seguras, uma vez que ela faz proveito da falta de algoritmos eficientes para fatoração. Esta aplicabilidade particular da Teoria dos Números deixa claro que o desenvolvimento de campos cujo caráter seja de natureza abstrata possa, eventualmente, ser ferramenta essencial para outras aplicações.

Agradecimentos

Ao CNPq pela bolsa concedida tornando este trabalho possível. Ao revisor, pelas observações. Por último, mas não menos importante, ao professor Marcos André Verdi pela valiosa contribuição e esforço feito neste projeto.

Referências

[1] COUTINHO, S. C. **Números inteiros e Criptografia RSA**. 5. ed. Rio de Janeiro: IMPA, 2007.

[2] SANTOS, J. P. O. **Introdução a Teoria dos Números**. 3. ed. Rio de Janeiro: IMPA, 2007.
[3] GERÔNIMO, J. R.; FRANCO, V. S. **Fundamentos de Matemática**. 2. ed. Maringá: EDUEM, 2008.
[4] NIVEN, I.; ZUCKERMAN, H. S.; MONTGOMERY, H. L. **An introduction to the Theory of Numbers**. 5. ed. New York: John Wiley & Sons, 1991.
[5] ANDREWS, G. E. **Number Theory**. New York: Dover Publications, 1997.