CÓDIGOS CORRETORES DE ERROS BINÁRIOS – Parte I: Teoria dos Números, Congruências e Inteiros Módulo *m*.

Danilo Henrique Bento dos Santos[1].
Orientador: Samir Assuena[2].
Departamento de Matemática, Centro Universitário FEI
danilo.henrique360z@gmail.com
samir.assuena@fei.edu.br

Resumo: Neste trabalho, estudaremos o conjunto dos números inteiros, bem como sua fundamentação axiomática, os conceitos de máximo divisor comum *(m.d.c.)* e mínimo múltiplo comum *(m.m.c.)* de um conjunto de números inteiros e os inteiros módulos *m*.

1. Introdução – Números Inteiros

Nesta fase do projeto, faremos uma introdução à Teoria dos Números, considerada uma abordagem matemática autocontida, no sentido de não demandar conhecimentos avançados e que pode ser compreendida sem assistência de outros conceitos; em contrapartida, é a base para estudarmos *Anéis*, *Corpos* e *Códigos Corretores de Erros*.

- **Operações** - Estão definidas duas operações, que chamamos de adição (+) e multiplicação (·);
- **Tricotomia (*Relação de ordem*)** - Dados dois inteiros quaisquer a e b tem-se que ou $a < b$ ou $a = b$ ou $a > b$;
- **Princípio da Boa Ordem (*WOP*)** - Todo conjunto não-vazio de inteiros não negativos contém um elemento mínimo.
- **Princípio da Indução Matemática (*PMI*)** - Seja a um inteiro dado. Suponhamos que para cada inteiro $n \geq a$ está dada um afirmação $A(n)$ de forma que:
  - *i.* *A (a) é verdadeira;*
  - *ii.* *Se para um inteiro $k \geq a$, A (k) é verdadeira, então A(k + 1) é verdadeira;*

  Então, A (n) é verdadeira para todo $n \geq a$.

- **Divisibilidade** - Dados $a, b \in \mathbb{Z}$ dizemos que a divide b, denotaremos por $a|b$, se existe $x \in \mathbb{Z}$ tal que $b = ax$ com $a \neq 0$:
  - *i.* $\forall n \in N, n|0;$
  - *ii.* $a|b, b|c \Rightarrow a|c;$
  - *iii.* $a|b, a|c \Rightarrow a|(bx + cy) \forall x,y \in Z;$

2. Divisibilidade

Nosso ponto de partida é o algoritmo da divisão ou Divisão Euclidiana. Uma equação do tipo $bx = a$ pode ou não ter solução no conjunto dos inteiros; isso dependerá dos coeficientes a e b da equação. Quando tal solução existe, diz-se que a é *divisível* por b ou $b|a$. O caso contrário, no qual b não divide a, denotaremos por $b \nmid a$ (*MILLES; 1998*).

Teorema 2.1 *(Algoritmo da Divisão). Sejam a e b inteiros, com $b \neq 0$. Então, existem inteiros q e r, únicos, tais que: $a = bq + r$ e $0 \leq r < |b|$.*

Definição 2.1 *Um conjunto não-vazio J de números inteiros diz-se um **ideal** de Z se:*

i. $\alpha, \beta \in J \Rightarrow \alpha + \beta \in J;$
ii. $\alpha \in J, a \in \mathbb{Z} \Rightarrow \alpha a \in J.$

Torna-se fácil darmos alguns exemplos triviais de *ideais*: o próprio conjunto Z de todos os números inteiros certamente é um ideal de Z, assim como o também o conjunto *{0}*. Outro exemplo interessante é o conjunto dos números pares, que nada mais é do que o conjunto dos múltiplos de 2. Assim, podemos obter novos exemplos com uma construção análoga. Dado um inteiro m, indicaremos por $m\mathbb{Z}$ o conjunto: $m\mathbb{Z} = \{mx \mid x \in \mathbb{Z}\}$, isto é, o conjunto de todos os múltiplos de m. Para firmarmos esta notação, generalizamos através do teorema abaixo:

Teorema 2.2 *Seja J um **ideal** de Z. Então, $J = \{0\}$ ou existe um inteiro positivo m, tal que $J = m\mathbb{Z}$.*

A partir de agora, a e b indicarão inteiros, ambos não nulos. Um inteiro c diz-se um *divisor comum* de a e b se $c|a$ e $c|b$. O conjunto $D(a, b)$ de todos os divisores comuns de a e b é limitado superiormente (pois se $a \neq 0$, para todo elemento $c \in D(a, b)$ temos que $c \leq |a|$). Consequentemente, $D(a, b)$ tem máximo.

Definição 2.3 *Chamamos de **máximo divisor comum** de a e b o maior de seus divisores comuns, isto é:*

$$mdc(a,b) = maxD(a,b) \quad (1)$$

Teorema 2.4 *(Bézout). Sejam a, b inteiros e $d = mdc(a, b)$. Então existem r, s inteiros tais que $d = ra + sb$.*

O teorema a seguir sugere uma definição muito importante para o estudo da matemática em geral e de áreas mais específicas, tais como Teoria dos Códigos e Criptografia. Este conceito é o de *primos relativos*, *co-primos* ou até *relativamente primos*. Abordaremos os principais teoremas relacionados às questões tratadas em seções futuras, destacando o papel que os *números primos* desempenham na Teoria dos Números e nas demais áreas anteriormente citadas.

Teorema 2.5 *(Euclides). Sejam $a, b, c \in \mathbb{Z}$ tais que $a|bc$. Se $mdc(a, b) = 1$, ou seja, são co-primos, então $a|c$.*

Prova: Se $mdc(a, b) = 1$, temos que $mdc(ac, bc) = |c|$. Agora, obviamente $a|ac$ e, da hipótese, $a|bc$. Consequentemente, Se $a|ac$ e $a|bc$, então dizemos que $a||c|$, logo $a|c$. ■

Agora, um inteiro c diz-se um múltiplo comum de *a* e *b* se *a|c* e *b|c*. Indicaremos por $M^+(a,b)$ o conjunto de todos os múltiplos comuns positivos de *a* e *b*. Certamente $M^+(a,b)$ *é não vazio* , pois $|a||b| \in M^+(a,b)$; logo, pelo *WOP*, esse conjunto contém um elemento mínimo.

Definição 2.6 *Chama-se mínimo múltiplo comum de a e b o menor dos seus múltiplos positivos comuns, isto é:*
$mmc(a,b) = min\ M^+(a,b)$ (2)

Teorema 2.7 *Sejam a, b* $\in Z$, $d = mdc(a,b)$ *e* $m = mmc(a,b)$. *Então,* $md = |ab|$.

O Teorema acima nos dá um método de cálculo para o *mmc(a.b).* Dados *a, b* $\in Z$, podemos calcular o *mdc(a,b)* pelo método baseado em divisões sucessivas chamado de *Algoritmos de Euclide*s e depois obter:
$$mmc(a,b) = \frac{|ab|}{\text{mdc(a,b)}} \quad (3)$$

3. Números Primos

Mostraremos que todo número diferente de *0, 1* e *-1* pode-se expressar como produto de números primos, de forma única, a menos da ordem dos fatores. Esse resultado, conhecido como o *Teorema Fundamental da Aritmética, (TFA)* já aparece do livro *IX* dos *Elementos de Euclides* e basicamente trata que todos os outros números podem ser obtidos através de produtos dos números primos. Vamos lembrar sua definição.

Definição 3.1 *Um inteiro p diz-se primo se tem exatamente dois divisores positivos, 1 e |p|.*

Uma aplicação interessante para os números primos é dada pelo Teorema a seguir.

Teorema 3.2 *(Teorema Fundamental da Aritmética). Seja a um inteiro diferente de 0, 1 e -1. Então, existem primos positivos* $p_1<p_2<...<p_r$ *e inteiros* $n_1, n_2, ..., n_r$ *tais que* $a = Ep_1^{n1} ... p_r^{nr}$, *em que E = ±1, conforme a seja positivo ou negativo. Além disso, essa decomposição é única.*

Uma consequência direta do *TFA* é que ele nos dá uma nova forma de calcular o *mdc* e *mmc* de dois números.

Lema 3.3 *Sejam* $a = p_1^{n1} ... p_t^{nt}$ *e* $d = p_1^{m1} ... p_t^{mt}$ *inteiros positivos, onde* $p_1, ..., p_t$ *são primos positivos e* $n_i, m_i, 1 \leq i \leq t$ *são inteiros não negativos. Então, d|a se e somente se* $m_i \leq n_i, 1 \leq i \leq t$.

Teorema 3.4 *Sejam* $a = p_1^{n_1} ... p_t^{n_t}$ *e* $b = p_1^{m_1} ... p_t^{m_t}$ *inteiros nas condições do lema 2.11. Então,*
$d = mdc(a,b) = p_1^{\alpha_1} ... p_t^{\alpha_t}$, *em que* $\alpha_i = min(n_i, m_i)\ 1 \leq I \leq t$,
$m = mmc(a,b) = p_1^{\beta_1} ... p_t^{\alpha_t}$, *em que* $\beta i = max(n_i, m_i)\ 1 \leq I \leq t$.

Ainda hoje permanecem sem respostas inúmeras questões, de formulação elementar, em torno dos números primos, tal como a conjectura de Mersenne (1588-1648) que afirma a existência de infinitos *números de Mersenne*, isto é, infinitos números primos na forma $2^n - 1$ onde *n* é também um número primo. Porém, daremos um enfoque maior em outro tipo de números, da forma $F_n = 2^{2^n} + 1$.

Em 1640, Fermat (1601-1665) mostrou que números F_n são primos para *n = 0, 1, 2, 3, 4*, e conjecturou que todo número dessa forma é primo. Em 1739, Euler (1707-1783) demonstrou que F_5 é divisível por 641, o que prova que a conjectura sobre os Números de Fermat é falsa. Tal prova, pode ser simplificada usando o seguinte conceito.

4. Congruências

Definição 4.1 *Seja m≠0 um inteiro fixo. Dois inteiros a e b dizem-se congruentes módulo m se m|(a-b). Neste caso escrevemos a≡b (mod m).*

Proposição 4.2 *Seja m um inteiro fixo. Dois inteiros a e b são congruentes módulo m se somente se eles têm como resto o mesmo inteiro quando dividindo por m.*

Daí, podemos dizer que $\{a_1, ..., a_m\}$ uma coleção de *m* inteiros diz-se um *sistema completo de resíduos módulos m* se cada inteiro é congruente módulo *m* a um único a_i. Por exemplo, os seguintes são *SCR* módulo 5: {0, 1, 2, 3, 4}, {5, 6, 7, 8, 9}, {12, 24, 35, -4, 18}.

Proposição 4.3 *Seja m um inteiro fixo e sejam a, b e c inteiros arbitrários. Se mdc(c, m)=1, então ac≡bc (mod m) implica a≡b (mod m).*

Prova: Se ac≡bc (mod m), temos que m|(a-b)c. Como mdc(c,m)=1, do Teorema 2.5 (Euclides) vem que m|(a-b), donde a≡b (mod m). ■

5. Conclusões

Assim, vemos que toda esta fundamentação teórica, nos dá uma excelente base para tratarmos resultados importantes na Teoria dos Números e em toda Matemática, tais como o *Pequeno Teorema de Fermat*, *Euler* e *Wilson*, que não enunciaremos aqui pois foge da primazia desde resumo, mas trataremos nas próximas oportunidades. Tais resultados, assim como o conceito de congruências são essenciais para a introduzirmos os Inteiros Módulo *m* que nada mais é do que o *alfabeto* que utilizaremos para estudarmos os Códigos Corretores de Erros Binários.

6. Referências

[1] POLCINO MILIES, C.; COELHO, S.P. **Números, uma introdução à matemática.** São Paulo: Edusp, 1998.

[2] HEFEZ, A.; VILLELA, M.L.T. **Códigos corretores de erros.** Rio de Janeiro: IMPA, 2008.

[3] MIT Open Course Ware – **Theory of Numbers** Massachusetts Institute of Technology – Disponível em: <https://ocw.mit.edu/courses/mathematics/18-781-theory-of-numbers-spring-2012/>. Acesso em: 06 de set. de 2019.

Agradecimentos

Ao Centro Universitário FEI por tornar esse estudo possível, nestes dias, quando a ciência pura é vista com impaciência, ou na melhor das hipóteses com indulgência bem-humorada.

[1] Aluno de IC do Centro Universitário FEI - Projeto com vigência de 04/18 a 04/19.

[2] Professor Assistente 1 do Centro Universitário FEI.