NÚMEROS INTEIROS

PROF. FRANCISCO MEDEIROS

Álgebra Abstrata - Verão 2012

Faremos, nessas notas, uma breve discussão sobre o conjunto dos números inteiros. O texto é basicamente a seção 3 do capítulo 1 de [1]. Caso o leitor se interesse por uma construção axiomática dos números inteiros, sugerimos a leitura de [2].

Nosso intuito é lembrá-lo de alguns resultados básicos que são amplamente conhecidos e que serão úteis no curso de **Álgebra Abstrata**.

Como de costume, denotaremos o conjunto dos números inteiros por $\mathbb{Z}$ e seus elementos por letras minúsculas (em *itálico*!) do nosso alfabeto: $a, b, \ldots, m, n, \ldots$.

Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, podemos dividir a por b e obter um resto não negativo r que é menor do que o módulo de b, ou seja, podemos encontrar m e r tais que $a = mb + r$, onde $0 \leq r < |b|$. Isto é conhecido como o *algorítmo da divisão de Euclides* e suporemos que ele é familiar ao leitor.

Dizemos que $b \neq 0$ *divide* a se existe $m \in \mathbb{Z}$ tal que $a = mb$. Para indicar que b divide a escreveremos $b \mid a$, e para indicar que b não divide a, $b \nmid a$. Se $b \mid a$, dizemos que b é um *divisor* de a. Por exemplo, $3 \mid 12$ (pois $12 = 4 \cdot 3$), $-4 \mid 20$ (pois $20 = -5 \cdot (-4)$) e $3 \nmid 10$ (pois $10 = 1 \cdot 10$ ou $10 = 2 \cdot 5$).

Lema 1. (a) *Se* $a \mid 1$, *então* $a = \pm 1$.

(b) *Se* $a \mid b$ *e* $b \mid a$, *então* $a = \pm b$.

(c) *Se* $b \mid g$ *e* $b \mid h$, *então* $b \mid (rg + sh)$, *quaisquer que sejam* $r, s \in \mathbb{Z}$.

Prova. **(a)** Exercício.

(b) $a \mid b \Rightarrow \exists m \in \mathbb{Z}$ tal que $a = mb$ (I); $b \mid a \Rightarrow \exists n \in \mathbb{Z}$ tal que $b = na$ (II). Substituindo (II) em (I) temos que $a = m(na)$ e, portanto, $mn = 1$, ou seja, $m \mid 1$. De (a) temos que $m = \pm 1$ e de (I) podemos concluir que $a = \pm b$.

(c) $b \mid h \Rightarrow \exists m \in \mathbb{Z}$ tal que $h = mb$ (I); $b \mid g \Rightarrow \exists n \in \mathbb{Z}$ tal que $g = nb$ (II). Então $rg + sh = r(nb) + s(mb) = (rn + sm)b = kb$, onde $k = rn + sm$. Logo b é um divisor de $rg + sh$. □

A partir do conceito de divisibilidade podemos definir o **mdc** entre dois inteiros.

Definição 2. *O inteiro positivo d se diz o* máximo divisor comum *entre a e b se:*

(1) *d é um divisor de a e b;*
(2) *qualquer divisor de a e b é um divisor de d.*

Exemplo 3. *O máximo divisor comum entre* 16 *e* 20 *é igual a* 4*, pois* $4 \mid 16$*,* $4 \mid 20$ *e qualquer outro divisor comum de* 16 *e* 20 *é um divisor de* 4*. Note também que o máximo divisor comum entre* 16 *e* -20 *é igual a* 4*.*

Usaremos a notação $\mathrm{mdc}(a, b)$ para representar o máximo divisor comum entre a e b.[1] Assim, com essa notação, $\mathrm{mdc}(16, 20) = 4$. Como na definição exigimos que o máximo divisor comum seja positivo, então $\mathrm{mdc}(a, b) = \mathrm{mdc}(a, -b) = \mathrm{mdc}(-a, b) = \mathrm{mdc}(-a, -b)$. Note que para usarmos essa notação para o máximo divisor comum, é necessário garantirmos que tal número (caso exista!) seja único: dados $a, b \in \mathbb{Z}$, suponha que existam d_1 e d_2 satisfazendo as condições da Definição 2. Então da condição (2) temos que $d_1 \mid d_2$ e $d_2 \mid d_1$. Logo, do Lema 1.(b), temos que $d_1 = \pm d_2$. Mas como tanto d_1 quanto d_2 são positivos, segue que $d_1 = d_2$.

Em matemática sempre que definimos um *elemento* novo devemos nos perguntar em que hipóteses tal *elemento* sempre **existe** e se tal *elemento* é **único**. E não poderia ser diferente no caso do *máximo divisor comum*. A unicidade já foi provada acima e o próximo resultado garante a **existência** do $\mathrm{mdc}(a, b)$, sempre que $a \neq 0$ ou $b \neq 0$. Para a verificação desse fato, faremos uso de um resultado bem conhecido que garante a existência de um *mínimo* em todo conjunto não vazio de inteiros positivos.

Lema 4. *Sejam $a, b \in \mathbb{Z}$, não ambos nulos. Então existe o* $\mathrm{mdc}(a, b)$*.*

Prova. Fixados $a, b \in \mathbb{Z}$, considere o subconjunto $\mathcal{M} := \{ma + nb \colon m, n \in \mathbb{Z}\} \subset \mathbb{Z}$. Como $a \neq 0$ ou $b \neq 0$, então $\mathcal{M}$ possui elementos diferentes de zero. Além disso, dado $x = ma + nb \in \mathcal{M}$, como $-m, -n \in \mathbb{Z}$ então $-x = (-m)a + (-n)b \in \mathcal{M}$, ou seja, $\mathcal{M}$ possui inteiros positivos. Então $\mathcal{M}$ possui um inteiro positivo mínimo d; por estar em $\mathcal{M}$, d tem a forma $d = m_0 a + n_0 b$. Afirmamos que $d = \mathrm{mdc}(a, b)$. De fato, notemos primeiro que, pelo Lema 1.(c), se $c \mid a$ e $c \mid b$, então $c \mid x$, para todo $x \in \mathcal{M}$. Em particular $c \mid d$. Resta-nos, portanto, verificar que $d \mid a$ e $d \mid b$. Dado um elemento qualquer $x = ma + nb$ de $\mathcal{M}$, pelo algorítmo da divisão de Euclides temos que $x = qd + r$, onde $0 \leq r < d$, ou seja,

$$ma + nb = q(m_0 a + n_0 b) + r \Rightarrow r = ma + nb - [(qm_0)a + (qn_0)b] = (m - qm_0)a + (n - qn_0)b$$

[1] Também é comum a notação (a, b) para indicar o máximo divisor comum entre a e b.

de onde segue que $r \in \mathcal{M}$. Mas com $0 \leq r$ e $r < d$, pela minimalidade de d temos que $r = 0$. Logo $x = qd$, ou seja, $d \mid x$, para todo $x \in \mathcal{M}$. Em particular, dado que $a = 1 \cdot a + 0 \cdot b \in \mathcal{M}$ e $b = 0 \cdot a + 1 \cdot b \in \mathcal{M}$, segue que $d \mid a$ e $d \mid b$. □

Na prova acima, a existência do $\text{mdc}(a, b)$ é dada pela existência de um inteiro positivo *mínimo* no conjunto $\mathcal{M}$. Poderíamos, também, usar a unicidade desse elemento mínimo para garantir a unicidade do $\text{mdc}(a, b)$. Além disso, como resultado direto da existência do $\text{mdc}(a, b)$ na prova acima, temos o seguinte resultado:

Corolário 5. *Sejam $a, b \in \mathbb{Z}$, não ambos nulos. Então existem $m_0, n_0 \in \mathbb{Z}$ tais que $\text{mdc}(a, b) = m_0 a + n_0 b$.* □

A partir da noção de máximo divisor comum, podemos definir *números primos entre si*, também conhecidos como relativamente primos ou primos relativos.

Definição 6. *Os inteiros a e b são* primos entre si *se $\text{mdc}(a, b) = 1$.*

Como uma consequência direta do Corolário 5 temos o seguinte resultado:

Corolário 7. *Se a e b são relativamente primos, então existem inteiros m e n tais que $ma + nb = 1$.* □

Exemplo 8. *Os inteiros 4 e 15 são primos entre si. Além disso, $4 \cdot 4 + (-1) \cdot 15 = 1$.*

Introduzimos agora outro conceito familiar: *números primos.*

Definição 9. *O inteiro $p > 1$ é um* número primo *se seus únicos divisores positivos são 1 e p.*

Equivalentemente, dizemos que um número p, maior do que 1, é um número primo se, e somente se, dado outro inteiro n qualquer, tem-se $\text{mdc}(p, n) = 1$ ou $p \mid n$. (Verifique!)

São exemplos de números primos: $2, 3, 5, 7, 11, 13, \ldots$.

Como veremos adiante, os números primos são os "blocos de construção" dos números inteiros. Mas primeiro faremos o seguinte resultado:

Lema 10. *Se $a \mid bc$ e a e b são primos entre si, então $a \mid c$.*

Prova. Dado que a e b são primos entre si, do Corolário 7 temos que existem $m, n \in \mathbb{Z}$ tais que $ma + nb = 1$. Assim $(ma)c + (nb)c = c$. Mas como $a \mid mac$ e, por hipótese, $a \mid nbc$,

segue que $a \mid (mac + nbc)$ e, portanto, $a \mid c$. □

Como consequência imediata desse lema e da definição de número primo, obtemos o seguinte resultado:

Corolário 11. *Se p é um número primo tal que $p \mid bc$, então $p \mid b$ ou $p \mid c$.*

Prova. Basta observar que se p é primo, então $\text{mdc}(p, b) = 1$ ou $p \mid b$. O resultado segue do lema anterior. □

Falamos acima que os números primos servem como "blocos de construção" para o conjunto dos números inteiros. Abaixo enunciamos (sem prova!) precisamente isto através do seguinte teorema:

Teorema 12 (Teorema da Fatoração Única)**.** *Qualquer inteiro positivo $a > 1$ pode ser fatorado de forma única como $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_t^{\alpha_t}$, onde $p_1 > p_2 > \cdots > p_t$ são números primos e cada $a_i > 0$.* □

Uma questão que se apresenta naturalmente é saber se o conjunto dos primos é finito ou se, pelo contrário, a sequência dos primos é infinita. A resposta aparece na obra de Euclides, num teorema cuja demonstração é considerada, até hoje, um modelo de raciocínio matemático.

Teorema 13. *O conjunto dos números primos é infinito.*

Prova. Suponhamos que o conjunto dos primos seja finito e sejam $p_1, p_2, \ldots, p_n$ esses primos. Consideremos, então, o número

$$p = p_1 \cdot p_2 \cdots p_n + 1.$$

Do *Teorema da Fatoração Única*, algum dos p_i's, $i \in \{1, 2, \ldots, n\}$, divide p. Como p_i é um dos elementos do conjunto acima, p_i divide o produto $p_1 \cdot p_2 \cdots p_n$. Então, p_i divide também $p - p_1 \cdot p_2 \cdots p_n = 1$, o que é uma contradição. □

Há diversas outras demonstrações desse resultado, mas a dada por Euclides é considerada a mais simples.

Mudaremos um pouco de assunto e passaremos a estudar a importante noção de **congruência**. Dentre as diversas utilidades desse conceito, encontram-se os problemas sobre números perfeitos (que não seram abordados nessas notas) que levam a estudar números

da forma $2^n - 1$ e a procurar seus divisores. Mais geralmente, podemos pensar em estudar os números da forma $a^n - 1$, com $a \in \mathbb{Z}$. A seguir um pouco de história, extraída de [2], página 104:

> Numa carta de 1640 dirigida a Bernhard Frénicle de Bessy, Fermat anunciava um resultado surpreendente: se p é um primo e a um inteiro que não é divisível por p, então p divide $a^{p-1} - 1$. Na mesma carta, comentava: "Eu lhe enviaria a demonstração se não temesse que ela é demasiado comprida".
> A primeira demonstração desse resultado, conhecido como "Pequeno Teorema de Fermat" (para distingui-lo do Grande Teorema de Fermat, mencionado em 2.3), foi publicada em 1736, quase um século depois, por Euler. Posteriormente, Euler deu outras demonstrações do mesmo resultado. Numa delas, ele utiliza freqüentemente os "restos de divisores por p", que deram origem à Teoria das Congruências. Esse método de trabalho também foi usado por Lagrange e Legendre, mas só se tornou explícito nas *Disquisitiones* de Gauss, na qual aparecem a definição precisa e o simbolismo que se usa até hoje.

Definição 14. *Seja $m > 0$ um inteiro fixo. Dois inteiros a e b dizem-se* congruentes módulo *m se m divide a diferença $a - b$.*

Nesse caso, escrevemos $a \equiv b \mod m$, onde m se chama *módulo* da relação. Portanto, $a \equiv b \mod m$ se, e somente se $m \mid (a - b)$, ou, equivalentemente, se existe um inteiro q tal que $a = b + mq$.

Temos, por exemplo, $5 \equiv 9 \mod 2$, $73 \equiv 4 \mod 23$, $10 \equiv -2 \mod 3$, etc.

Exemplo 15. *Dois números são congruentes módulo 2 se, e somente se, eles são ambos pares ou ambos ímpares. (Verifique!)*

Podemos dar outra caracterização da noção de congruência, conforme mostra o resultado a seguir.

Lema 16. *Seja m um inteiro fixo. Dois inteiros a e b são congruentes módulo m se, e somente se, eles têm como resto o mesmo inteiro quando divididos por m.*

Prova. Sejam

$$a = mq_1 + r_1, \text{ com } 0 \leq r_1 < m$$
$$b = mq_2 + r_2, \text{ com } 0 \leq r_2 < m.$$

Então,

$$a - b = m(q_1 - q_2) + (r_1 - r_2).$$

Logo, $m \mid (a-b)$ se, e somente se, $m \mid (r_1 - r_2)$. Ainda, como $0 \leq |r_1 - r_2| < m$, temos que $m \mid (r_1 - r_2)$ se, e somente se, $r_1 - r_2 = 0$. Consequentemente, $a \equiv b \mod m$ se, e somente se, $r_1 = r_2$. □

A relação de congruência tem as seguintes propriedades básicas:

Lema 17. (1) *A relação de "congruência módulo m" define uma relação de equivalência no conjunto dos inteiros.*

(2) *Esta relação tem m classes de equivalência distintas.*

(3) *Se* $a \equiv b \mod m$ *e* $c \equiv d \mod m$, *então* $a + c \equiv b + d \mod m$ *e* $ac \equiv bd \mod m$.

(4) *Se* $ab \equiv ac \mod m$ *e se a e m são primos entre si, então* $b \equiv c \mod m$.

Prova. (1) *Reflexão*: Como $m \mid 0$, então $n \mid (a - a)$ e, portanto, $a \equiv a \mod m$;
Simetria: Se $a \equiv b \mod m$, então $m \mid (a-b)$ e, portanto, $m \mid -(a-b)$; logo $b \equiv a \mod m$;
Transitividade: Se $a \equiv b \mod m$ e $b \equiv c \mod m$, então $m \mid (a - b)$ e $m \mid (b - c)$, de onde segue que $m \mid \{(a - b) + (b - c)\}$, isto é, $m \mid (a - c)$ e, portanto, $a \equiv c \mod m$.

(2) Consequência direta do *algorítmo da divisão de Euclides* e do lema anterior.

(3) Suponhamos que $a \equiv b \mod m$ e $c \equiv d \mod m$. Logo $m \mid (a - b)$ e $m \mid (c - d)$ e assim $m \mid \{(a-b)+(c-d)\}$, ou seja, $m \mid \{(a+c)-(b+d)\}$, de onde segue que $a+c \equiv b+d \mod m$. Além disso, $m \mid \{(a - b)c + (c - d)b\} = ac - bd$ e, portanto, $ac \equiv bd \mod m$.

(4) Consequência direta do Lema 10. □

Referências

1. I. N. Herstein, *Tópicos de álgebra*, Polígono, 1964.
2. F. C. Polcino and S. P. Coelho, *Números: Uma introdução à matemática*, Edusp, 1998.