Divisibilidade Básica

BRUNO HOLANDA

Nesta aula vamos ter nosso primeiro contato com uma das mais importantes áreas da Matemática: *A Teoria dos Números.* Esta se concentra em estudar os número inteiros e as suas propriedades. Uma destas propriedades é conhecida como *divisibilidade*.

1 Números Primos e Compostos

Um dos principais objetos de estudo da teoria dos números são os *números primos*. Mas para entender o que sào números primos antes é necessário saber quando um número é múltiplo de outro.

Dizemos que M é um múltiplo de a quando o resto da divisão de M por a é zero. Por exemplo, o resto da divisão de 12 por 4 é zero. Logo, 12 é um múltiplo de 4. Por outro lado, o resto da divisão de 21 por 5 é 1. Portanto, 21 não é um múltiplo de 5.

Agora observe as três listas de números abaixo:

$$\text{Lista 1: } 2, 4, 6, 8, \boxed{10}, 12, 14, 16, 18, 20, ...$$
$$\text{Lista 2: } 3, 6, 9, 12, \boxed{15}, 18, 21, 24, 28, \boxed{30}, ...$$
$$\text{Lista 3: } 5, \boxed{10}, \boxed{15}, 20, 25, \boxed{30}, 35, 40, 45, 50, ...$$

Na primeira lista estão escritos os números múltiplos de 2, também conhecido como números pares. Na segunda lista estão escritos os números múltiplos de 3 e na outra os números múltiplos de 5. Observe que existem alguns números que aparecem em mais de uma lista, como o 10, 15 e o 30. Eles aparecem mais de uma vez porque são múltiplos de números menores que eles próprios. Por exemplo, o 10 é múltiplo de 2 e 5; o 15 é múltiplo de 3 e 5; equanto o 30 é múltiplo de 2, 3 e 5. Estes números que são múltiplos de números menores que eles são chamados de números *compostos*.

Já os números que não possuem essa propriedade, ou seja: não são múltiplos de nenhum número menor do que eles (exceto o 1)[1] são chamados de números *primos*. Por exemplo, os 2, 3, 5, 11, 23 são todos primos.

Neste momento você deve estar pensando: "Ok, eu já sei o que são os números primos mas, porque eles são tão importantes assim?". Bem, essa pergunta não é difícil de responder. Eles são importantes pois qualquer número composto pode ser fatorado em números primos (mesmo que alguns deles apareçam repetidos). Por exemplo, $35 = 5.7$, $144 = 2^4.3^2$ e $2000 = 2^4.5^3$. Este é o famoso teorema fundamental da aritmética.

Teorema Fundamental da Aritmética. Todo inteiro possitivo $n > 1$ pode ser expresso como produto de fatores primos de maneira única.

[1] Todos os números são múltiplos de 1

Ou seja, os números primos funcionam como os tijolos dos números inteiros. Assim, se você souber tudo sobre os números primos, saberá tudo sobre todos os números inteiros! Dessa forma, seria ótimo saber quando um número é primo ou não. Para isto vamos usar a seguinte idéia:

i. Primeiramente liste o máximo de números que você puder. (Aqui vamos listar de 1 a 100).

ii. Sabemos que 2 é primo e que todos os seus múltiplos (maiores que 2) são compostos. Dessa forma, vamos "riscar" todos eles.

1	$\boxed{2}$	$\boxed{3}$	4	$\boxed{5}$	6	$\boxed{7}$	8	9	10
$\boxed{11}$	12	$\boxed{13}$	14	15	16	$\boxed{17}$	18	$\boxed{19}$	20
21	22	$\boxed{23}$	24	25	26	27	28	$\boxed{29}$	30
$\boxed{31}$	32	33	34	35	36	$\boxed{37}$	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

iii. O primeiro número que não foi riscado é 3. Logo, ele também é primo. E todos os números múltiplos de 3 são compostos. Assim, também vamos riscá-los.

iv.

Este processo é conhecido como *Crivo de FULANO*. [...] Por outro lado, se você quizer descobrir se 6901 é primo ou não vai levar muito tempo se você utilizar apenas o crivo de FULANO. Assim, é importate o método abaixo.

1. Qual é o algarismo das unidades do produto $1 \times 3 \times 5 \times 7 \times \cdots \times 2007$?

2. Joana escreve a seqüência de números naturais 1, 6, 11, ..., onde cada número, com exceção do primeiro, é igual ao anterior mais cinco. Joana pára quando encontra o primeiro número de três algarismos. Que número é esse?

3. Quantos números de dois algarismos não são primos nem múltiplos de 2, 3 ou 5?

4. A soma de dois números primos a e b é 34 e a soma dos primos a e c é 33. Quanto vale $a + b + c$?

5. Quantos números inteiros positivos menores que 900 são múltiplos de 7 e terminam em 7?

6. Existe algum número cujo produto dos dígitos seja 1980?

7. Qual é o menor inteiro positivo que é o dobro de um cubo e o quíntuplo de um quadrado?

8. (Teste IMO 1997) Sejam p_1 e p_2 dois primos ímpares consecutivos. Mostre que $p_1 + p_2$ possui pelo menos 3 fatores primos (não necessariamente distintos).

9. (OBM 2001) Dizemos que um número natural é *legal* quando for soma de dois inteiros consecutivos e também for soma de três naturais consecutivos.

   a) Mostre que 2001 é legal, mas 1999 e 2002 não são legais.

   b) Mostre que 2001^{2001} é legal.

10. (Seletiva Rioplatense 2004) É possível distribuir todos os números inteiros de 1 a 30 nas casas de um tabuleiro 5×6 (5 linhas e 6 colunas), um por casa, de modo que:

    a) todas as colunas possuam a mesma soma?

    b) todas as linhas tenham a mesma soma?

    Em cada item, se for possível construa um exemplo. Se não for possível, justifique.

11. (HMMT 2004) João escolheu cinco números do conjunto $\{1, 2, 3, 4, 5, 6, 7\}$. Se ele contar a Claudia o produto dos números que ele escolheu, ela não terá informação suficiente para descobrir quais eles são. Porém, se ele também falar se a soma dos números escolhidos é par ou ímpar, ela saberá os números escolhidos. Qual o produto dos números escolhidos?

12. (OBM 2008) Quantos números inteiros maiores que zero e menores que 100 possuem algum divisor cuja soma dos dígitos seja 5?

13. (Rússia 1995) É possível que os números $1, 2, ..., 100$ sejam termos de no máximo 12 progressões geométricas?

2 Divisibilidade

A grande maioria dos problemas de Teoria dos Números se apoia na seguinte pergunta: *Quando um número a é divisível por b.* Nosso objetivo nesta e na próxima seção será tentar responder (em parte) essa pergunta.

Dados os inteiros a e b, com $a \neq 0$, dizemos que a divide b se existe algum inteiro x tal que $b = ax$. Denotamos por $a \mid b$. Assim, $2 \mid 18$, $3 \mid 15$ e $5 \mid 75$. Se esse inteiro x não existir, dizemos que a não divide b, e escrevemos $a \nmid b$. Por exemplo, $4 \nmid 10$, $9 \nmid 16$ e $15 \nmid 25$.

Vamos listar algumas propriedades extremamente úteis sobre divisibilidade:

(1) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

(2) Se $a \mid b$ e $a \mid c$, então $a \mid bx + cy$ para todo par de inteiros x e y.

(3) No caso em que $a, b > 0$, se $a \mid b$, então $b \geq a$.

(4) Se p é um primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Problema 1. Qual o maior inteiro positivo n tal que

$$\frac{n^3 + 100}{n + 10}$$

também seja um inteiro?

Solução. Primeiramente note que $n+10 \mid n^2(n+10)$. Assim, pela propriedade (2), $n+10 \mid n^3+100-n^2(n+10) = 100-10n^2$. Agora, como $n+10 \mid 10n(n+10)$, então $n+10 \mid 100-10n^2+10n(n+10) = 100+100n$. Por último, como $n+10 \mid 100(n+10)$, $n+10 \mid 100+100n-100(n+10) = -900$. Ou seja $n+10 \mid 900$. Pela propriedade (3), $n+10 \leq 900$, logo o maior valor possível para n é 890. $\square$

Note que para saber se a divide b, basta dividir b por a. Se o resto for zero, então $a \mid b$. Caso contrário, $a \nmid b$. O processo pelo qual descobrimos este resto é conhecido como *algoritmo da divisão.*

Algoritmo da Divisão. Dados inteiros a e b, com $b > a > 0$, existem inteiros q e r tais que

$$b = qa + r,$$

onde q é o quociente e r é o resto. Além disso, podemos garantir que $0 \leq r < a$.

Vamos provar a eficácia do algoritmo resolvendo os próximos problemas.

Problema 2. Prove que nenhum quadrado perfeito deixa resto 2 quando dividido por 3.

Solução. Quando dividimos qualquer número por 3, os únicos valores possíveis que o resto pode assumir são: 0, 1 ou 2. Assim, podemos dizer que todo número inteiro pode assumir uma de três formas:

- n é da forma $3k$ quando n for um múltiplo de 3.
- n é da forma $3k+1$ quando o resto da divisão de n por 3 for 1.
- n é da forma $3k+2$ quando o resto da divisão de n por 3 for 2.

Agora vamos ver o que acontece quando estudamos seu quadrado:

- Se $n = 3k$, então $n^2 = 9k^2 = 3(3k^2)$ também é da forma $3k$.
- Se $n = 3k+1$, então $n^2 = (3k+1)^2 = 9k^2+6k+1 = 3(3k^2+2k)+1$ também é da forma $3k+1$.
- Se $n = 3k+2$, então $n^2 = (3k+2)^2 = 9k^2+12k+4 = 3(3k^2+4k+1)+1$ é da forma $3k+1$.

Assim, nenhum quadrado é da forma $3k+2$. $\square$

Usando o algoritmo da divisão podemos provar uma propriedade muito importante que os números primos possuem:

Propriedade: Todo primo $p > 3$ é da forma $6k+1$ ou da forma $6k+5$. Ou seja, o resto da divisão de qualquer primo p (maior que 3) por 6 deve ser 1 ou 5.

Prova. Sabemos que todo número pode assumir uma das seguintes formas: $6k$, $6k+1$, $6k+2$, $6k+3$, $6k+4$ ou $6k+5$. Nenhum primo maior que três pode ser da forma $6k$, $6k+2$ ou $6k+4$, pois elas representam números pares e o único primo par é 2. Além disso, esse primo não pode ser da forma $6k+3$, pois esta representa um número múltiplo de 3. Logo, as possíveis formas que p pode assumir são $6k+1$ ou $6k+5$. □

1. (OBM 2001) Se a n-ésima OBM é realizada em um ano múltiplo de n, dizemos que esse ano é *super-olímpico*. Determine todos os anos super-olímpicos, sabendo que a OBM nunca deixou de ser realizada desde sua primeira edição, em 1979, e supondo que continuará sendo realizada todo ano.
2. Sejam a, b inteiros tais que $56a = 65b$. Prove que $a+b$ é composto.
3. Prove que não existe nenhum inteiro n tal que $4 \mid n^2+2$.
4. Sejam a e b dois inteiros tais que a^2+b^2 seja um múltiplo de 3. Prove que a^2+b^2 também deve ser múltiplo de 9.
5. Prove que a soma dos quadrados de cinco naturais consecutivos não pode ser um quadrado perfeito.
6. Prove que n^3-n é um múltiplo de 24 sempre que n for um inteiro ímpar.
7. Mostre que se p e p^2+2 são ambos primos, então p^3+2 também é.
8. (Rússia 1995) Ache todos os primos p tais que p^2+11 possua exatamente seis divisores positivos (incluindo 1 e ele mesmo).

3 Critérios de Divisibilidade

A nossa busca para saber quando um número é multiplo de outro chega em uma nova fase. Agora vamos aprender que nem sempre é necessário fazer enormes contas de divisão para saber se um número é multiplo de outro.

Por exemplo, se seu professor lhe perguntasse se 1662597 é múltiplo de 2, você com certeza iria responder: *Claro que não, pois 1662597 é ímpar.* Ainda inconformado com a sua resposta ele te faz outra pergunta: *E como você sabe que 1662597 é ímpar?* E a resposta seria: *Eu olhei para o último dígito.*

Assim para saber se um número é múltiplo de 2, basta saber se seu último dígito é par ou ímpar. Esta propriedade é conhecida como *critério de divisibilidade por 2.* Vamos aprender alguns outros:

- Para saber se um número é múltiplo de 3, basta somar seus dígitos. Se a soma for múltipla de 3, então o número inicial também será. Por exemplo, a soma dos dígitos de 34561 é $3+4+5+6+1=19$ que não é múltiplo de 3, logo 34561 também não é múltiplo de 3.
- Para saber se um número é múltiplo de 4, basta olhar o número formado pelos seus dois últimos algarismos. Se este número for múltiplo de 4, então o número inicial também será múltiplo de 4. Por exemplo, 346216 é múltiplo de 4, pois 16 é múltiplo de 4.
- Para saber se um número é múltiplo de 5, o último dígito deve ser 0 ou 5.

- Para saber se um número é múltiplo de 8, basta olhar o número formado pelos seus três últimos algarismos. Se este número for múltiplo de 8, então o número inicial também será múltiplo de 8. Por exemplo, 346276 não é múltiplo de 8, pois 276 não é múltiplo de 8.

- Para saber se um número é múltiplo de 9, basta somar seus dígitos. Se a soma for múltipla de 9, então o número inicial também será. Por exemplo, a soma dos dígitos de 54963 é $5+4+9+6+3=27$ que é múltiplo de 9, logo 54863 também é múltiplo de 9.

- Para saber se um número é múltiplo de 11, devemos proceder da seguinte maneira: Somar todos os dígitos de ordem ímpar (seja I essa soma). Somar todos os dígitos de ordem par (seja P essa soma). Se a diferença $I-P$ for um número múltiplo de 11, então o número inicial também será múltiplo de 11. Por exemplo, no número 13574 temos que $I=4+5+1$ e $P=7+3$. Como $I-P=0$, 13574 deve ser um número múltiplo de 11.

Problemas

1. O número $\overline{a1989b}$ é divisível por 72. Determine a e b.

2. Se $\underbrace{200120012001...2001}_{n\ 2001's}729$ é divisível por 11, ache o menor valor possível de n.

3. Existe algum quadrado perfeito cuja a soma dos dígitos seja 2004?

4. (Rússia 1941) Ache o número $\overline{523abc}$ divisível por 7, 8 e 9.

5. (Leningrado 1990) Existe algum número de seis dígitos divisível por 11 cujos dígitos sejam 1, 2, 3, 4, 5, 6 em alguma ordem e sem repetições?

6. (Rússia 1936) Determine todos os quadrados perfeitos com quatro dígitos e da forma $\overline{aabb}$, onde a e b representam os dígitos.

7. (Banco Rioplatense) A diferença entre dois primos é 100. Se você os concatena (i.e; coloca um ao lado do outro) obtem um outro primo. Encontre esse dois primos.

8. São dados 18 naturais consecutivos, cada um de três dígitos. Mostre que um deles é divisível pela soma de seus algarismos.

9. (Torneio das Cidades) Existe alguma potência de 2 tal que seja possível rearranjar seus dígitos e obter uma outra potência de 2?

10. (Kömal 2005) Usando os dígitos $1,2,3,4,5,6,7$ construímos vários números de sete dígitos distintos. É possível que existam dois números dentre eles de modo que um divida o outro?

4 Euclides e os Divisores

Não, *Euclides e os Divisores* não foi uma banda de Rock famosa durante o período Helênico. Na verdade, Euclides foi um matemático grego que viveu por volta de 300 a.C. que colaborou com sua bibliografia para um enorme crescimento no estudo de diversas áreas da matemática, principalmente a teoria dos números inteiros.

Dentre os principais feitos de Euclides está o estudo dos chamados divisores comuns. Sabemos que os divisores de 12 são 1, 2, 3, 4, 6 e 12. Já os divisores de 15 são 1, 3, 5 e 15. Assim, podemos ver que 1 e 3 são os divisores comuns de 12 e 15. Vamos chamar de *máximo divisor comum* o maior divisor de dois inteiros e denotá-lo por *mdc*. Logo, $\text{mdc}(12, 15) = 3$. Outros exemplos são: $\text{mdc}(36, 24) =??$ e $\text{mdc}(108, 52) =??$.

Juntamente com o mdc, estudamos o *mmc* que é o mínimo múltiplo comum entre um conjunto de números. Podemos calcular o mdc e o mmc entre dois números escrevendo-os como o produto de seus fatores primos.

(MOSTRAR COMO)

Mas existe outra forma de calcular o mdc entre dois números. Mas antes de mostrar este método, vamos um fato conhecido como *Lema de Euclides*.

Lema de Euclides. Dados dois inteiros quaisquer é verdadeira a seguinte equação:

$$\text{mdc}(a, b) = \text{mdc}(a, b - a).$$

1. Determine
   (a) $\text{mdc}(2^{100} + 1, 2^{100} - 1)$.
   (b) $\text{mdc}(5^{50} + 1, 5^{50} - 1)$.
   (c) $\text{mdc}(F_{n+1}, F_n)$, onde F_n é o n-ésimo termo da sequência de Fibonacci.
2. (IMO 1959) Mostre que a fração
   $$\frac{21n + 4}{14n + 3}$$
   é irredutível para todo inteiro n.
3. (Rússia 1995) A sequência $a_1, a_2, ...$ de números naturais satisfaz $\text{mdc}(a_i, a_j) = \text{mdc}(i, j)$, sempre que $i \neq j$. Prove que $a_n = n$ para todo n.
4. Prove que $(a, [b, c]) = [(a, b), (a, c)]$.
5. Mostre que se $a + b \neq 0$, $(a, b) = 1$ e p é um primo ímpar, então
   $$\left(a + b, \frac{a^p + b^p}{a + b}\right) = 1 \text{ ou } p.$$
6. Mostre que $(a^n - 1, a^m - 1) = a^{(n,m)} - 1$.
7. Janaína listou os 999 números a seguir
   $$\text{gcd}(1, 1998);\ \text{gcd}(2, 1998);\ \text{gcd}(3, 1998), ..., \text{gcd}(998, 1998)\ e\ \text{gcd}(999, 1998).$$
   Quantos são maiores que 19?

8. (Rússia 1995) Sejam m e n inteiros positivos tais que

$$\mathrm{mmc(m, n) + mdc(m, n) = m + n.}$$

Prove que um dos números é divisível pelo outro.

9. (TT 1994) Sejam a, b, c, d quatro inteiros positivos tais que $ad = bc$. Prove que $a + b + c + d$ é um número composto.

10. (Rússia 1935) Prove que

$$\frac{\mathrm{mmc}(a, b, c)\mathrm{mdc}(a, b)\mathrm{mdc}(b, c)\mathrm{mdc}(c, a)}{\mathrm{mdc}(a, b, c)} = abc.$$

11. (OBM 1990) Seja k um inteiro positivo tal que $\dfrac{k(k+1)}{3}$ seja um quadrado perfeito. Prove que $\dfrac{k}{3}$ e $k + 1$ são ambos quadrados perfeitos.

12. (Rússia 2001) Sejam a e b dois inteiros positivos distintos tais que $ab(a+b)$ é divisível por a^2+ab+b^2. Prove que $|a - b| > \sqrt[3]{ab}$.

13. (USAMO 1972) Sejam a, b, c inteiros positivos. Mostre que

$$\frac{\gcd(a, b, c)^2}{}$$

5 Idéias Avançadas

Resolver problemas difíceis com pouco conhecimento teórico é uma das coisas que fazem da Teoria dos Números uma das áreas mais interesantes da matemática. Nesta seção vamos ganhar um pouco mais de maturidade que vai nos ajudar muito a entender melhor os assuntos que iremos abordar mais adiante.

Para começar veremos a prova de um fato fundamental em Teoria dos Números.

Teorema. Existem infinitos números primos.

Prova. Suponha que exista uma quantidade finita de números primos. Sejam $p_1, p_2, ..., p_k$ todos esses números primos. Considere agora o número $P = p_1p_2...p_k + 1$. Este número é relativamente primo com todos os primos $p_i's$, logo não pode ser escrito como produto dos mesmo. Isso é uma contradição ao teorema fundamental da aritmética. Assim, a seqüência dos números primos deve ser infinita. □

Outros fatos que merecem nossa atenção são:

Postulado de Bertrand. Para todo inteiro positivo n, existe pelo menos um número primo entre n e $2n$.

Teorema de Dirichlet. Se a, b são inteiros não nulos e primos entre si, existem infinitos primos da forma $an + b$.

Pórem, provar esses fatos não é nenhum pouco fácil. Por outro lado, podemos usá-los livremente para resolver problemas de olimpíada.

1. (Rio Platense 2004) Utilizando todos os dígitos 1, 2, 3, 4, 5, 6, 7, 8 e 9, Sofia escreveu três números de três algarismos cada um. Ao somar os três números obteve 1665. Em cada um dos três números anteriores, trocou de posição o algarismo das centenas com o algarismo das unidades, formando três novos números de três algarismos. Qual é a soma dos três novos números?

2. Ache todos os números que podem ser escritos como soma de dois compostos.

3. Prove que qualquer número maior que ou igual a 7 pode ser escrito como soma de dois inteiros relativamente primos (maiores que 1).

4. (Leningrado 1988) Cada um dos números naturais a, b, c, d é divisível por $ab - dc$, que também é um número natural. Prove que $ab - cd = 1$.

5. (Ibero 1999) Seja B um inteiro maior que 10 tal que cada um dos seus dígitos pertence ao conjunto $\{1, 3, 7, 9\}$. Demonstre que B tem um fator primo maior que ou igual a 11.

6. (Putnam 1956) Prove que todo inteiro positivo possui um múltiplo cuja a representação decimal possui todos os dez dígitos.

7. Se a e b são inteiros diferentes, mostre que existem infinitos naturais n tais que $(a + n, b + n) = 1$

8. Existe alguma seqüência infinita de números triangulares que são, dois a dois, primos entre si?

9. Se g é um divisor de cada um dos números ab, cd e $ac + bd$, prove que g também é um divisor de ac e bd, onde a, b, c e d são intieros.

10. (Russia 1991) Os inteiros positivos $a_1, a_2, ..., a_n$ são todos menores que 1000, e $[a_i, a_j] > 1000$ para todos $i \neq j$. Mostre que

$$\sum_{i=1}^{n} \frac{1}{a_i} < 2$$