Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 2

Prof. Samuel Feitosa

Aula 3

O Algoritmo de Euclides

Exemplo 1. *Seja S um conjunto infinito de inteiros não negativos com a seguinte propriedade: dados dois quaisquer de seus elementos, o valor absoluto da diferença entre eles também pertence a S. Se d é o menor elemento positivo de S, prove que S consiste de todos os múltiplos de d.*

Considere um elemento m qualquer de S. Pelo algoritmo da divisão, $m = qd + r$ com $0 \leq r < d$. Como todos os números $m - d, m - 2d, m - 3d, \ldots, m - qd = r$ pertencem a S e d é o menor elemento positivo de tal conjunto, devemos ter obrigatoriamente que $r = 0$. Sendo assim, podemos concluir que todos os elementos de S são múltiplos de d. Resta mostrarmos que todos os múltiplos de d estão em S. Seja kd um múltiplo positivo qualquer de d. Como S é infinito, existe um inteiro $m \in S$ tal que $m = qd > kd$. Assim todos os números $m - d, m - 2d, \ldots, m - (q - k)d = kd$ estão em S.

Definição 2. *Um inteiro a é um divisor comum de b e c se $a \mid b$ e $a \mid c$. Se b e c não são ambos nulos, denotaremos por $mdc(b, c)$ o máximo divisor comum de b e c.*

Como um inteiro não nulo possui apenas um número finito de divisores, se b e c são ambos não nulos, o número $mdc(b, c)$ sempre existe, isto é, sempre está bem definido.

Lema 3. *(Euclides) Se $x \neq 0$, $mdc(x, y) = mdc(x, x + y)$*

Demonstração. Seja d um divisor comum de x e y. Então $d \mid x + y$ e consequentemente d também á um divisor comum de x e $x + y$. Reciprocamente, se f é um divisor comum de $x + y$ e x, f também divide $(x + y) - y = x$ e assim f é um divisor comum de x e y. Como os conjuntos de divisores comuns dos dois pares de números mencionados são os mesmos, o maior divisor comum também é o mesmo. □

Então podemos calcular:

$$mdc(123, 164) = mdc(123, 41) = mdc(41, 123) = mdc(41, 82) = mdc(41, 41) = 41.$$

Exemplo 4. *Três máquinas I, R, S imprimem pares de inteiros positivos em tickets. Para a entrada (x, y), as máquinas I, R, S imprimem respectivamente $(x-y, y), (x+y, y), (y, x)$. Iniciando com o par $(1, 2)$ podemos alcançar*

a) (819, 357)?

b) (19, 79)?

Para o item a), calculemos inicialmente $mdc(819, 357)$:

$$mdc(819, 357) = mdc(462, 357) = mdc(105, 357) = mdc(105, 252) = \ldots = mdc(21, 21) = 21.$$

Pelo Lema de Euclides, o mdc entre os dois números em um ticket nunca muda. Como $mdc(1, 2) = 1 \neq 21 = mdc(819, 357)$, não podemos alcançar o par do item a).

Para o item b), indiquemos com $\rightarrow$ uma operação de alguma das máquinas. Veja que: $(2, 1) \overset{R}{\rightarrow} (3, 1) \overset{S}{\rightarrow} (1, 3) \overset{R}{\rightarrow} (4, 3) \overset{R}{\rightarrow} \ldots \overset{R}{\rightarrow} (19, 3) \overset{S}{\rightarrow} (3, 19) \overset{R}{\rightarrow} (22, 19) \overset{R}{\rightarrow} (41, 19) \overset{R}{\rightarrow} (60, 19) \overset{R}{\rightarrow} (79, 19)$.

Observação 5. *Procurar* **invariantes** *sempre é uma boa estratégia para comparar configurações diferentes envolvidas no problema. Confira o problema proposto 31.*

Definição 6. *Dizemos que dois inteiros p e q são primos entre si ou relativamente primos se $mdc(p, q) = 1$. Dizemos ainda que a fração $\frac{p}{q}$ é irredutível se p e q são relativamente primos.*

Exemplo 7. *(IMO 1959) Prove que $\dfrac{21n+4}{14n+3}$ é irredutível para todo número natural n.*

Pelo lema de Euclides, $mdc(21n+4, 14n+3) = mdc(7n+4, 14n+3) = mdc(7n+1, 7n+2) = mdc(7n+1, 1) = 1$.

O seguinte lema será provado na próxima aula.

Lema 8. *(Propriedades do MDC) Seja $mdc(a, b) = d$, então:*

i) Se $k \neq 0$, $mdc(ka, kb) = kd$.

ii) $mdc\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$.

iii) Se $mdc(a, c) = 1$, então $mdc(a, bc) = d$.

Exemplo 9. *(Olimpíada Inglesa) Se x e y são inteiros tais que $2xy$ divide $x^2 + y^2 - x$, prove que x é um quadrado perfeito*

Se $d = mdc(x, y)$, então $x = da$ e $y = db$, com $mdc(a, b) = 1$. Do enunciado, temos:

$$\begin{aligned} 2abd^2 \mid d^2a^2 + d^2b^2 - da &\Rightarrow \\ d^2 \mid d^2a^2 + d^2b^2 - da &\Rightarrow \\ d^2 \mid -da &\Rightarrow \\ d \mid a. \end{aligned}$$

Logo, $a = dc$, para algum c. Como $x \mid y^2$, obtemos $d^2c \mid d^2b^2$, ou seja, $c|b^2$ e $mdc(c, b^2) = c$. Usando que $mdc(a, b) = 1$ e que todo divisor comum de b e c também é um divisor comum de a e b, podemos concluir que $mdc(c, b) = 1$. Usando o item *iii)* do lema anterior, $mdc(c, b^2) = 1$. Assim, $c = 1$ e $x = d^2c = d^2$.

Exemplo 10. *No planeta X, existem apenas dois tipos de notas de dinheiro: \$5 e \$78. É possível pagarmos exatamente \$7 por alguma mercadoria? E se as notas fossem de \$ 3 e \$ 78?*

Veja que $2 \times 78 - 31 \times 5 = 1$ e consequentemente $14 \times 78 - 217 \times 5 = 7$. Basta darmos 14 notas de de \$ 78 para recebermos 217 notas de \$ 5 como troco na compra de nossa mercadoria. Usando as notas de \$3 e \$78 não é possível pois o dinheiro pago e recebido como troco por algo sempre é múltiplo de 3 e 7 não é múltiplo de 3.

Queremos estudar a versão mais geral desse exemplo. Quais são os valores que podemos pagar usando notas de \$$a$ e \$$b$? Em particular, estaremos interessados em conhecer qual o menor valor que pode ser pago. Para responder essa pergunta, precisaremos do algoritmo de Euclides:

Teorema 11. *(O Algoritmo de Euclides) Para os inteiros b e $c > 0$, aplique sucessivamente o algoritmo da divisão para obter a série de equações:*

$$\begin{aligned} b &= cq_1 + r_1, \;\; 0 < r_1 < c, \\ c &= r_1q_2 + r_2, \;\; 0 < r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, \;\; 0 < r_3 < r_2, \\ &\vdots \\ r_{j-2} &= r_{j-1}q_j + r_j, \;\; 0 < r_j < r_{j-1}, \\ r_{j-1} &= r_jq_{j+1} \end{aligned}$$

A sequência de restos não pode diminuir indefinidamente pois $0 \leq r_i < r_{i-1}$ e existe apenas um número finito de naturais menores que c. Assim, para algum j, obteremos $r_{j+1} = 0$. O maior divisor comum de b e c será r_j, ou seja, o último resto não nulo da sequência de divisões acima.

Demonstração. Pelo Lema de Euclides,

$$mdc(x + qy, y) = mdc(x + (q-1)y, y) = mdc(x + (q-2)y, y) = \ldots = mdc(x, y).$$

Então,
$$mdc(b,c) = mdc(c,r_1) = mdc(r_1,r_2) = \ldots = mdc(r_{j-1},r_j) = r_j.$$
$\square$

Exemplo 12. *Calcule* $mdc(42823, 6409)$.

Pelo Algoritmo de Euclides,

$$\begin{aligned}
42823 &= 6 \times 6409 + 4369\\
6409 &= 1 \times 4369 + 2040\\
4369 &= 2 \times 2040 + 289\\
2040 &= 7 \times 289 + 17\\
289 &= 17 \times 17.
\end{aligned}$$

Portanto, $mdc(42823, 6409) = 17$.

Podemos extrair mais informações do Algoritmo de Euclides. Para isso, iremos organizar as equações do exemplo acima de outra forma.

Essencialmente, a equação $mdc(x+qy, y) = mdc(x, y)$ nos diz que podemos subtrair q vezes um número de outro sem alterar o máximo divisor comum do par em questão. Realizando esse procedimento sucessivas vezes, subtraindo o número menor do maior, podemos obter pares com números cada vez menores até que chegarmos em um par do tipo (d, d). Como o máximo divisor comum foi preservado ao longo dessas operações, d será o máximo divisor comum procurado. Iremos repetir o exemplo anterior registrando em cada operação quantas vezes um número é subtraido do outro. Isso será feito através de dois pares de números auxiliares:

$$\begin{aligned}
(42823, 6409) &\mid (1,0)(0,1)\\
(4369, 6409) &\mid (1,-6)(0,1)\\
(4369, 2040) &\mid (1,-6)(-1,7)\\
(289, 2040) &\mid (3,-20)(-1,7)\\
(289, 17) &\mid (3,-20)(-22,147)\\
(17, 17) &\mid (355,-2372)(-22,147)
\end{aligned}$$

Da primeira linha para a segunda, como subtraímos 6 vezes o número 6409 de 42823, subtraímos 6 vezes o par $(0, 1)$ de $(1, 0)$, obtendo: $(1, 0) - 6(0, 1) = (1, -6)$. Se em uma dada linha, temos:
$$(x, x + qy)) \mid (a, b)(c, d);$$
então, a próxima linha deverá ser:
$$(x, y) \mid (a, b)(c - aq, d - bq);$$

porque representará a operação de subtrairmos q vezes o primeiro número do segundo. Veja que o par (a, b) foi subtraido de (c, d) exatamente q vezes. Os números escritos nos últimos dois pares representam os coeficientes dos números originais para cada número do primeiro par. Por exemplo, analisando a linha:

$$(289, 2040) \mid (3, -20)(-1, 7);$$

obtemos que:

$$\begin{aligned} 289 &= 3 \times 42823 - 20 \times 6409, \\ 2040 &= -1 \times 42823 + 7 \times 6409. \end{aligned}$$

Em cada linha, essa propriedade é mantida pois a mesma subtração que é realizada no primeiro par também é realizada entre os dois últimos pares. Analisando o último par, podemos escrever 17 como combinação de 42823 e 6409 de duas formas diferentes:

$$\begin{aligned} 17 &= -22 \times 42823 + 147 \times 6409, \\ 17 &= 355 \times 42823 + -2372 \times 6409, \end{aligned}$$

Assim, se no planeta X tivéssemos apenas notas de \$42823 e \$6409, poderíamos comprar algo que custasse exatamente \$17.

Como conclusão da discussão anterior e do algoritmo de Euclides, podemos concluir que:

Teorema 13. *(Bachet-Bèzout) Se $d = mdc(a, b)$, então existem inteiros x e y tais que $ax + by = d$.*

De fato, a discussão anterior também nos mostra um algoritmo para encontrarmos x e y. Voltando à discussão sobre o planeta X, podemos concluir em virtude do teorema anterior que qualquer valor múltiplo de d poderá ser pago usando apenas as notas de \$$a$ e \$$b$. Como todo valor pago, necessariamente é um múltiplo do máximo divisor comum de a e b, descobrimos que o conjunto que procurávamos consiste precisamente do conjunto dos múltiplos de d.

Observação 14. *(Para professores) A prova mais comum apresentada para o teorema anterior baseia-se na análise do conjunto de todas as combinações lineares entre a e b e quase sempre se preocupa apenas com mostrar a existência de x e y. Acreditamos que o algoritmo para encontrar x e y facilite o entendimento do teorema para os alunos mais jovens. Entretanto, frequentemente utilizemos apenas a parte da existência descrita no enunciado. Além disso, preferimos discutir um exemplo numérico ao invés de formalizarmos uma prova e sugerimos que o professor faça o mesmo com mais exemplos em aula.*

Exemplo 15. *(Olimíada Russa 1995) A sequência $a_1, a_2, ...$ de naturais satisfaz $mdc(a_i, a_j) = mdc(i, j)$ para todo $i \neq j$ Prove que $a_i = i$ para todo i.*

Para qualquer inteiro n, $mdc(a_{2n}, a_n) = mdc(2n, n) = n$, consequentemente $n \mid a_n$. Seja d um divisor qualquer de a_n diferente de n, então $d \mid mdc(a_d, a_n)$. De $mdc(a_d, a_n) = mdc(d, n)$, podemos concluir que $d \mid n$. Sendo assim, todos os divisores de a_n que são diferentes de n são divisores de n. Como já sabemos que $a_n = nk$, para algum k, não podemos ter $k > 1$ pois nk não divide n e assim concluímos que $a_n = n$.

Exemplo 16. *Mostre que* $mdc(2^{120} - 1, 2^{100} - 1) = 2^{20} - 1$.

Pelo lema de Euclides,

$$\begin{aligned}
mdc(2^{120} - 1, 2^{100} - 1) &= mdc(2^{120} - 1 - 2^{20}(2^{100} - 1), 2^{100} - 1),\\
&= mdc(2^{20} - 1, 2^{100} - 1),\\
&= mdc(2^{20} - 1, 2^{100} - 1 - 2^{80}(2^{20} - 1)),\\
&= mdc(2^{20} - 1, 2^{80} - 1),\\
&= mdc(2^{20} - 1, 2^{80} - 1 - 2^{60}(2^{20} - 1)),\\
&= mdc(2^{20} - 1, 2^{60} - 1),\\
&= mdc(2^{20} - 1, 2^{60} - 1 - 2^{40}(2^{20} - 1)),\\
&= mdc(2^{20} - 1, 2^{40} - 1),\\
&= mdc(2^{20} - 1, 2^{40} - 1 - 2^{20}(2^{20} - 1)),\\
&= mdc(2^{20} - 1, 2^{20} - 1) = 2^{20} - 1.
\end{aligned}$$

Exemplo 17. *(Olimpíada Russa 1964) Sejam x, y inteiros para os quais a fração*

$$a = \frac{x^2 + y^2}{xy}$$

é inteira. Ache todos os possíveis valores de a.

A primeira estratégia é cancelar os fatores comuns com o objetivo de reduzir o problema ao caso em que x e y são primos entre si. Seja $d = \text{mdc}(x, y)$, com

$$\begin{cases} x = d \cdot x_0 \\ y = d \cdot y_0 \end{cases}, \ \text{mdc}(x_0, y_0) = 1,$$

então

$$a = \frac{x^2 + y^2}{xy} = \frac{{x_0}^2 + {y_0}^2}{x_0 y_0}.$$

Nessa condição, como x_0 divide y_0^2 e y_0 divide x_0^2, cada um deles é igual a 1, donde

$$a = \frac{1^2 + 1^2}{1 \cdot 1} = 2.$$

Definição 18. *Os inteiros $a_1, a_2, \ldots, a_n$, todos diferentes de zero, possuem múltiplo comum b se $a_i | b$ para $i = 1, 2, \ldots, n$(note que $a_1 a_2 \ldots a_n$ é um múltiplo comum). O menor múltiplo comum positivo para tal conjunto de inteiros é chamado de mínimo múltiplo comum e será denotado por $mmc(a_1, a_2, \ldots, a_n)$.*

Proposição 19. *Se a e b são não nulos, então: $mmc(a, b) \cdot mdc(a, b) = |ab|$.*

(A prova desta proposição também será deixada para a próxima seção)

Exemplo 20. *(Olimpíada Russa 1995) Sejam m e n interios positivos tais que:*

$$mmc(m, n) + mdc(m, n) = m + n.$$

Prove que um deles é divisível pelo o outro.

Se $d = mdc(m, n)$, então podemos escrever $m = da$ e $n = db$. Pela proposição anterior,

$$mmc(m, n) = \frac{d^2 ab}{d} = dab.$$

Temos:

$$\begin{aligned} mmc(m, n) + mdc(m, n) - m - n &= 0 \Rightarrow \\ dab + d - da - db &= 0 \Rightarrow \\ ab + 1 - a - b &= 0 \Rightarrow \\ (a - 1)(b - 1) &= 0. \end{aligned}$$

Portanto, ou $a = 1$ e $m \mid n$ ou então $b = 1$ e $n \mid m$.

Exemplo 21. *(Torneio das Cidades 1998) Prove que, para quaisquer inteiros positivos a e b, a equação $mmc(a, a + 5) = mmc(b, b + 5)$ implica que $a = b$.*

Para o item a), como $(a + 5) - a = 5$, temos $mdc(a, a + 5)$ é igual a 1 ou 5. O mesmo vale para $mdc(b, b + 5)$. Pela proposição anterior, temos:

$$\begin{aligned} mmc(a, a + 5) &= \frac{a(a + 5)}{mdc(a, a + 5)}, \\ mmc(b, b + 5) &= \frac{b(b + 5)}{mdc(b, b + 5)}. \end{aligned}$$

Suponha que $mdc(a, a + 5) = 5$ e $mdc(b, b + 5) = 1$, então $a(a + 5) = 5b(b + 5)$. Consequentemente, a é múltiplo de 5 e $a(a + 5)$ é múltiplo de 25. Isso implica que $b(b + 5)$ também é múltiplo de 5 e que $mdc(b, b + 5) > 1$. Uma contradição. Analogamente, não podemos ter $mdc(a, a + 5) = 1$ e $mdc(b, b + 5) = 5$. Sendo assim, $mdc(a, a + 5) = mdc(b, b + 5)$ e:

$$\begin{aligned} a(a + 5) - b(b + 5) &= 0 \Rightarrow \\ (a - b)(a + b + 5) &= 0. \end{aligned}$$

Como $a + b + 5 > 0$, concluímos que $a = b$.

Exemplo 22. *Uma máquina f executa operações sobre o conjunto de todos os pares de inteiros positivos. Para cada par de inteiros positivos, ela fornece um inteiro dado pelas regras:*

$$f(x,x) = x,\ f(x,y) = f(y,x),\ (x+y)f(x,y) = yf(x,x+y).$$

Determine $f(2012, 2012! + 1)$.

Claramente $mmc(x,x) = x$ e $mmc(x,y) = mmc(y,x)$. Usando a proposição anterior e o lema de Euclides temos:

$$(x+y)mmc(x,y) = (x+y)\frac{xy}{mdc(x,y)} = y \cdot \frac{x(x+y)}{mdc(x,x+y)} = y \cdot mmc(x,x+y)$$

Temos então uma forte suspeita de que $f = mmc$. Seja S o conjunto de todos os pares de inteiros positivos (x,y) tais que $f(x,y) \neq mmc(x,y)$, e seja (m,n) o par em S com a soma $m+n$ minima. Note que todo par da forma (n,n) não está em S pois $f(n,n) = n = mmc(n,n)$. Assim, devemos ter $m \neq n$. Suponha sem perda de generalidade que $n > m$. Portanto:

$$\begin{aligned} nf(m,n-m) &= [m+(n-m)]f(m,n-m) \Rightarrow \\ &= (n-m)f(m,m+(n-m)) \Rightarrow \\ f(m,n-m) &= \frac{n-m}{n} \cdot f(m,n) \end{aligned}$$

Como o par $(m, m-n)$ não está em S, dado que a soma de seus elementos é menor que $m+n$, temos:

$$\begin{aligned} f(m,n-m) &= mmc(m,n-m) & \Rightarrow \\ \frac{n-m}{n} \cdot f(m,n) &= (n-m)mmc(m,m+(n-m)) & \Rightarrow \\ f(m,n) &= mmc(m,n) & \end{aligned}$$

Uma contradição. Desse modo, S deve ser um conjunto vazio e $f(x,y) = mmc(x,y)$ para todos os pares de inteiros positivos. Como $2012 \mid 2012!$, $mdc(2012, 2012!+1) = 1$ e consequentemente $mmc(2012, 2012!+1) = 2012(2012!+1)$.

Problemas Propostos

Problema 23. *Calcule:*

a) $mdc(n, n^2+n+1)$.

b) $mdc(3 \times 2012, 2 \times 2012 + 1)$.

c) $mdc\left(\dfrac{2^{40}+1}{2^8+1}, 2^8+1\right)$.

Problema 24. *Encontre* $mdc(2n+13, n+7)$

Problema 25. *Prove que a fração* $\frac{12n+1}{30n+2}$ *é irredutível.*

Problema 26. *Sejam* a, b, c, d *inteiros não nulos tais que* $ad-bc=1$. *Prove que* $\frac{a+b}{c+d}$ *é uma fração irredutível.*

Problema 27. *Mostre que* $mdc(a^m-1, a^n-1) = a^{mdc(m,n)}-1$.

Problema 28. *Mostre que se* $mdc(a,b)=1$, *então:*

$$mdc(a+b, a^2-ab+b^2) = 1 \text{ ou } 3$$

Problema 29. *Dado que* $mdc(a,4)=2$, $mdc(b,4)=2$, *prove que:*

$$mdc(a+b,4)=4.$$

Problema 30. *Prove que, para todo natural* n,

$$mdc(n!+1, (n+1)!+1) = 1.$$

Problema 31. *No exemplo 4, determine todos os pares que podem ser obtidos começando-se com o par* $(1,2)$.

Problema 32. *Qual o máximo divisor comum do conjunto de números:*

$$\{16^n+10n-1, n=1,2,3\ldots\}?$$

Problema 33. *A sequência* F_n *de Farey é a sequência de todos as frações irredutíveis* $\dfrac{a}{b}$ *com* $0 \le a \le b \le n$ *arranjados em ordem crescente.*

$$\begin{aligned}
F_1 &= \{0/1, 1/1\}\\
F_2 &= \{0/1, 1/2, 1/1\}\\
F_3 &= \{0/1, 1/3, 1/2, 2/3, 1/1\}\\
F_4 &= \{0/1, 1/4, 1/3, 1/2, 2/3, 3/4, 1/1\}\\
F_5 &= \{0/1, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 1/1\}\\
F_6 &= \{0/1, 1/6, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 1/1\}
\end{aligned}$$

Claramente, toda fração $\frac{a}{b}<1$ *com* $mdc(a,b)=1$, *está em algum* F_n. *Mostre que se* m/n *e* m'/n' *são frações consecutivas em* F_n *temos* $|mn'-nm'|=1$.

Problema 34. *(Resvista Quantum - Jornal Kvant) Todas as frações irredutíveis cujos denominadores não excedem 99 são escritas em ordem crescente da esquerda para a direita:*

$$\frac{1}{99}, \frac{1}{98}, \ldots, \frac{a}{b}, \frac{5}{8}, \frac{c}{d}, \ldots$$

Quais são as frações $\dfrac{a}{b}$ *e* $\dfrac{c}{d}$ *em cada lado de* $\dfrac{5}{8}$*?*

Problema 35. *(OBM) Para cada inteiro positivo $n > 1$, prove que $1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$ não é inteiro.*

Problema 36. *Determine todas as soluções em inteiros positivos para $\frac{1}{a} + \frac{1}{b} = \frac{1}{c}$.*

Problema 37. *Inteiros positivos a e b, relativamente primos, são escolhidos de modo que $\dfrac{a+b}{a-b}$ seja também um inteiro positivo. Prove que pelo menos um dos números $ab+1$ e $4ab+1$ é um quadrado perfeito.*

Problema 38. *(IMO 1979) Sejam p, q números naturais primos entre si tais que:*

$$\frac{p}{q} = 1 - \frac{1}{2} + \frac{1}{3} - \ldots - \frac{1}{1318} + \frac{1}{1319}.$$

Prove que p é divisível por 1979.

Respostas, Dicas e Soluções

23. (a)

$$\begin{aligned} mdc(n, n^2+n+1) &= mdc(n, n^2+n+1-n(n+1)), \\ &= mdc(n, 1), \\ &= 1. \end{aligned}$$

(b)

$$\begin{aligned} mdc(3\times 2012, 2\times 2012+1) &= mdc(3\times 2012 - (2\times 2012+1), 2\times 2012+1), \\ &= mdc(2012-1, 2\times 2012+1), \\ &= mdc(2012-1, 2\times 2012+1-2(2012-1)), \\ &= mdc(2012-1, 3), \\ &= mdc(2012-1-3\times 670, 3), \\ &= mdc(2,3) = 1. \end{aligned}$$

Outra opção seria observar que o mdc procurado deve dividir o número $3(2\times 2012+1) - 2(3\times 2012) = 3$ e que $2\times 2012+1$ não é múltiplo de 3.

(c)

$$\begin{aligned} mdc\left(\frac{2^{40}+1}{2^8+1}, 2^8+1\right) &= mdc\left(2^{32}+2^{24}+2^{16}+2^8+1, 2^8+1\right), \\ &= mdc\left((2^{32}-1)+(2^{24}+1)+(2^{16}-1)+(2^8+1)+1, 2^8+1\right), \\ &= mdc(1, 2^8+1) = 1. \end{aligned}$$

24.

$$\begin{aligned} mdc(2n+13, n+7) &= mdc(2n+13-2(n+7), n+7), \\ &= mdc(2n+13-2(n+7), n+7), \\ &= mdc(-1, n+7) = 1 \end{aligned}$$

25.

$$\begin{aligned} mdc(12n+1, 30n+2) &= mdc(12n+1, 30n+2-2(12n+1)), \\ &= mdc(12n+1, 6n), \\ &= mdc(12n+1-2(6n), 6n), \\ &= mdc(1, 6n) = 1 \end{aligned}$$

26. Seja $f = mdc(a+b, c+d)$. Então $f \mid d(a+b) - b(c+d) = 1$ e consequentemente $f = 1$.

27. Veja que

$$\begin{aligned} mdc(a^m - 1, a^n - 1) &= mdc(a^{m-n} - 1 + (a^n - 1)a^{m-n}, a^n - 1) \\ &= mdc(a^{m-n} - 1, a^n - 1) \end{aligned}$$

O resultado segue aplicando o Algoritmo de Euclides aos expoentes.

28. Seja $f = mdc(a+b, a^2 - ab + b^2)$. Então $f \mid (a+b)^2 - (a^2 - ab + b^2) = 3ab$. Se $mdc(f, a) > 0$, devemos ter $mdc(f, b) > 0$ pois $f \mid a+b$. O mesmo argumento vale para $mdc(f, b) > 0$. Assim, $mdc(f, a) = mdc(f, b) = 1$. Portanto, $f \mid 3$.

30. Pelo lema de Euclides,

$$\begin{aligned} mdc(n!+1, (n+1)!+1) &= mdc(n!+1, (n+1)!+1-(n+1)(n!+1)) \\ &= mdc(n!+1, -n) \\ &= mdc(n!+1-n[(n-1)!], -n) = 1 \end{aligned}$$

34. Sejam $l = mmc\{1, 2, \ldots, n\}$ e $a_i = l/i$. A soma considerada é

$$\frac{a_1 + a_2 + \ldots + a_n}{l}.$$

Queremos analisar o expoente do fator 2 no numerador e no denominador. Seja k tal que $2^k \leq n < 2^{k+1}$. Então $2^k || l$ e a_i é par para todo $i \neq 2^k$. Como a_{2^k} é ímpar, segue que o numerador é ímpar enquanto que o denominador é par. Consequentemente a fração anterior não representa um inteiro.

36. Sejam $d = mdc(a,b)$, $a = dx$, $b = dy$. Consequentemente $mdc(x,y) = 1$ e podemos escrever a equação como:

$$\begin{aligned}\frac{1}{a}+\frac{1}{b} &= \frac{1}{c} \Rightarrow \\ bc+ac &= ab \\ dyc+dxc &= d^2xy \\ c(x+y) &= dxy\end{aligned}$$

Como $mdc(xy, x+y) = 1$ pois $mdc(x,y) = 1$, devemos ter $xy \mid c$ e consequentemente $c = xyk$. Assim, $d = k(x+y)$. O conjunto solução é formado pelas triplas (a,b,c) onde $(a,b,c) = (kx(x+y), ky(x+y), xyk)$ com $mdc(x,y) = 1$ e x, y e k inteiros positivos.

38. Use a identidade de Catalão:

$$1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\ldots-\frac{1}{2n}=\frac{1}{n+1}+\frac{1}{n+2}+\ldots+\frac{1}{2n}$$

Em seguida, agrupe os termos da forma $\dfrac{1}{n+i}+\dfrac{1}{2n-i+1}$ e analise o numerador da fração obtida.

Referências

[1] S. B. Feitosa, B. Holanda, Y. Lima and C. T. Magalhães, Treinamento Cone Sul 2008. Fortaleza, Ed. Realce, 2010.

[2] D. Fomin, A. Kirichenko, Leningrad Mathematical Olympiads 1987-1991, MathPro Press, Westford, MA, 1994.

[3] D. Fomin, S. Genkin and I. Itenberg, Mathematical Circles, Mathematical Words, Vol. 7, American Mathematical Society, Boston, MA, 1966.

[4] I. Niven, H. S. Zuckerman, and H. L. Montgomery, An Introduction to the Theory of Numbers.

Teoria dos Números 03 - Algoritmo de Euclides

Problema 1. Calcule $mdc(3k + 2, 5k + 3)$ onde k é um inteiro qualquer.

Solução. Se $d = mdc(3k + 2, 5k + 3)$, então d divide $3k + 2$ e divide $5k + 3$. Logo d divide $5 \cdot (3k + 2) - 3 \cdot (5k + 3) = 1$. Como d deve ser positivo, temos $d = 1$.

Problema 2. Encontre todos os valores de a tais que as frações da forma $\dfrac{7n + 2a}{n + 5}$ sejam todas irredutíveis.

Solução. Devemos ter, para todo n inteiro,

$$\begin{aligned} 1 &= mdc(7n + 2a, n + 5) \\ &= mdc(7n + 2a - 7(n + 5), n + 5) \\ &= mdc(2a - 35, n + 5). \end{aligned}$$

Suponha que $2a - 35$ é diferente de 1 e de -1. Então tomando $n = |2a - 35| - 5$ teremos mdc igual a $|2a - 35|$, isto é, diferente de 1.

Logo, para que $mdc(7n + 2a, n + 5) = 1$ devemos ter $2a - 35 = \pm 1$. Dessa forma, $a = 18$ ou $a = 17$.

Problema 3. Calcule $mdc(3^{600}, 7)$

Solução. Vamos primeiramente descobrir o resto de 3^{600} na divisão por 7. Veja que $3^3 = 27$ deixa resto 6 por 7. Logo, 3^6 deixa mesmo resto que $6^2 = 36$, isto é, deixa resto 1 por 7. Dessa forma, $3^{600} = (3^6)^{100}$ deixa mesmo resto que $1^{100} = 1$ na divisão por 7. Concluímos que $mdc(3^{600}, 7) = mdc(1, 7) = 1$.

Problema 4. Na sequência de Fibonacci $1, 1, 2, 3, 5, 8, 13, \ldots$, cada número depois do segundo é soma dos dois anteriores. Denotando por f_n o n-ésimo termo da sequência temos portanto que

$$f_n = f_{n-1} + f_{n-2}$$

e que $f_1 = f_2 = 1$. Mostre que o máximo divisor comum de dois termos consecutivos da sequência de Fibonacci é sempre 1.

Solução. Temos o seguinte:

$$\begin{aligned} mdc(f_n, f_{n-1}) &= mdc(f_{n-1} + f_{n-2}, f_{n-1}) \\ &= mdc(f_{n-1} + f_{n-2} - f_{n-1}, f_{n-1}) \\ &= mdc(f_{n-2}, f_{n-1}) \end{aligned}$$

Proseguindo desta maneira, encontramos que o mdc inicial é igual a $mdc(f_{n-2}, f_{n-3})$, $mdc(f_{n-3}, f_{n-4}), \ldots$. De forma que $mdc(f_n, f_{n-1})$ é constante para todo n natural. Consequentemente, este valor é sempre igual a $mdc(f_1, f_2) = mdc(1, 1) = 1$.

Problema 5. Para quais inteiros positivos k ocorre $mdc(n! + k, 3n) = 3$ para todo $n > 3$?

Solução. Se $n > 3$ então $q = \dfrac{(n-1)!}{3}$ é inteiro. Sendo assim temos que $mdc(n! + k, 3n) = mdc(n! + k - 3nq, 3n) = mdc(k, 3n) = 3$. Devemos ter, então, $k = 3t$, $t \in \mathbb{Z}$. Logo, deve ocorrer $mdc(t, n) = 1$ para todo n. Como k é natural, $t = 1$ e $k = 3$. k só pode assumir um valor natural.

Problema 6. Qual o maior valor possível para $mdc(n, 2015 + n)$?

Solução. Note que $mdc(n, 2015 + n) = mdc(n, 2015 + n - n) = mdc(2015, n)$. Tomando $n = 2015$ temos o mdc máximo e igual a 2015.

Problema 7. Qual é o maior valor possível para $mdc(n + 1, n^3 + 5)$?

Solução. Da fatoração $n^3 + 1 = (n + 1)(n^2 - n + 1)$ temos que $n^3 + 5 = (n + 1)k + 4$. Portanto $mdc(n + 1, n^3 + 5) = mdc(n + 1, (n + 1)k + 4) = mdc(n + 1, 4)$ que tem máximo 4.

Problema 8. Quantos inteiros n, com $1 \leq n \leq 100$, podem ser escritos na forma $n = 462x + 966y$?

Solução. Pelo algoritmo de Euclides encontramos $mdc(966, 462) = 42$. Pelo teorema de Bezout, existem x' e y' tais que $42 = 462x' + 966y'$. Portanto, se 42 divide n, digamos $n = 42k$, então existem $x = k \cdot x'$ e $y = k \cdot y'$ tais que $n = 42k = 462x + 966y$. Além disso, se n pode ser escrito dessa forma então, claramente, é múltiplo de 42. Concluímos que n pode ser escrito na forma $462x + 966y$ se, e só se, for múltiplo de 42. Existem 2 múltiplode 42 entre 1 e 100. Sendo assim, a resposta é 2.

Problema 9. Qual é o maior valor possível para $mdc(122 + n^2, 122 + (n + 1)^2)$?

Solução. Temos que

$$mdc(122 + n^2, 122 + (n + 1)^2) = mdc(122 + n^2, 2n + 1).$$

Como $2n+1$ é ímpar, multiplicar $122+n^2$ por 2 não altera o mdc. Logo,

$$\begin{aligned} mdc(122+n^2, 122+(n+1)^2) &= mdc(244+2n^2, 2n+1) \\ &= mdc(244+2n^2-n(2n+1), 2n+1) \\ &= mdc(244-n, 2n+1). \end{aligned}$$

Novamente, como $2n+1$ é ímpar, multiplicar $244-n$ por 2 não afetará o mdc. Dai,

$$\begin{aligned} mdc(122+n^2, 122+(n+1)^2) &= mdc(488-2n, 2n+1) \\ &= mdc(488-2n+(2n+1), 2n+1) \\ &= mdc(489, 2n+1). \end{aligned}$$

Portanto, o maior valor para o mdc será 489, quando $2n+1$ for múltiplo de 489.

Problema 10. Qual é o menor valor positivo de N, tal que existem inteiros x e y satisfazendo

$$2013x + 3102y = N$$

.

Solução. Usando o algoritmo de Euclides:

$$\begin{aligned} mdc(3102, 2013) &= mdc(1089, 2013) \\ &= mdc(1089, 924) \\ &= mdc(924, 165) \\ &= mdc(165, 99) \\ &= mdc(99, 66) \\ &= mdc(66, 33) = 33. \end{aligned}$$

Claramente $33 = mdc(3102, 2013)$ divide N. Pelo teorema de Bezout existem inteiros x e y tais que $2013x + 3102y = 33$. Nessas condições, o menor valor de N é 33.

Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 2

Aula 4

Prof. Samuel Feitosa

Números Primos, MDC e MMC.

Definição 1. *Um inteiro $p > 1$ é chamado número primo se não possui um divisor d satisfazendo $1 < d < p$. Se um inteiro $a > 1$ não é primo, ele é chamado de número composto. Um inteiro m é chamado de composto se $|m|$ não é primo.*

O próximo teorema nos diz que os primos são as "peças"fundamentais dos números inteiros:

Teorema 2. *Todo inteiro n, maior que 1, pode ser expresso como o produto de número primo.*

Demonstração. Se o inteiro n é um primo, então ele mesmo é o produto de um único fator primo. Se o inteiro n não é primo, existe uma decomposição do tipo: $n = n_1 n_2$ com $1 < n_1 < n$ e $1 < n_2 < n$. Repetindo o argumento para n_1 e n_2, podemos escrever n como o produto de primos ou podemos obter parcelas menores escrevendo n como um produto de naturais. Como não existe uma sucessão infinita de naturais cada vez menores, após um número finito de operações desse tipo, poderemos escrever n como um produto de números primos.

Quantos números primos existem?

Teorema 3. *(Euclides) Existem infinitos números primos.*

Demonstração. Suponha, por absurdo, que exita apenas uma quantidade finita de primos: $p_1, p_2, \ldots, p_n$. Considere o número $X = p_1 p_1 \ldots p_n + 1$. Pelo teorema anterior, esse número deve ser o produto de alguns elementos do conjunto de todos os números primos. Entretanto, nenhum dos primos p_i divide X.

Exemplo 4. *Existe um bloco de 1000 inteiros consecutivos não contendo nenhum primo?*

Sim. Um exemplo é o conjunto $1001! + 2, 1001! + 3, \ldots, 1001! + 1001$. Veja $i \mid 1001! + i$ para todo $i = 2, 3, \ldots, 1001$.

Exemplo 5. *(Torneio das Cidades) Existe um bloco de 1000 inteiros consecutivos contendo apenas um primo?*

Para cada bloco de 1000 números consecutivos, contemos sua quantidade de números primos. Por exemplo, no bloco $1, 2, 3, \ldots, 1000$, temos 168 números primos (mas só usaremos o fato de que existem mais de dois primos nesse bloco). Comparando os blocos consecutivos $k+1, k+2, \ldots, k+1000$ e $k+2, k+3, \ldots, k+1001$, ou o número de números primos aumenta em uma unidade, ou fica constante ou diminui em uma unidade. Analisando todos os blocos consecutivos desde $1, 2, \ldots, 1000$ até $1001! + 2, 1001! + 3, \ldots, 1001! + 1001$, o número de números primos deve ser igual à 1 em algum deles. Para ver isso, usaremos um argumento de continuidade discreta: Começando com o número 168 e realizando alterações de no máximo uma unidade na quantidade de primos em cada bloco, para chegarmos no número 0, necessariamente deveremos passar pelo número 1 em algum momento.

Relembremos um importante resultado da aula passada:

Teorema 6. *(Bachet- Bèzout) Se $d = mdc(a, b)$, então existem inteiros x e y tais que $ax + by = d$.*

Proposição 7. *Sejam a, b e c inteiros positivos com $a \mid bc$ e $mdc(a, b) = 1$. Então, $a \mid c$.*

Demonstração. Pelo teorema anterior, existem x e y inteiros tais que $ax + by = 1$. Assim, $acx + bcy = c$. Como $a \mid acx$ e $a \mid bcy$, podemos concluir que $a \mid c$.

Em particular, se p é um número primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$. Podemos usar esse fato para garantir a unicidade em nosso primeiro teorema, obtendo o importante:

Teorema 8. *(Teorema Fundamental da Aritmética) A fatoração de qualquer inteiro $n > 1$, em fatores primos, é única a menos da ordem dos fatores.*

Exemplo 9. *(Rússia 1995) É possível colocarmos 1995 números naturais ao redor de um círculo de modo que para quaisquer dois números vizinhos a razão entre o maior e o menor seja um número primo?*

Não, é impossível. Suponha, por absurdo, que isso seja possível e denotemos por $a_0, a_1, \ldots, a_{1995} = a_0$ tais inteiros. Então, para $k = 1, \ldots, 1995$, $\frac{a_{k-1}}{a_k}$ é primo ou o inverso de um primo. Suponha que a primeira situação ocorra m vezes e a segunda ocorra $1995 - m$ vezes entre esses quocientes. Como o produto de todos os números da forma $\frac{a_{k-1}}{a_k}$, para $k = 1, \ldots, 1995$ é igual à 1, podemos concluir que o produto de m primos deve ser igual ao produto de $1995 - m$ primos. Em virtude da fatoração única, $m = 1995 - m$. Um absurdo pois 1995 é ímpar.

Proposição 10. *Se as fatorações em primos de n e m são:*

$$\begin{aligned} n &= p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}, \\ m &= p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}. \end{aligned}$$

Então, $mdc(m, n) = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k}$ *e* $mmc(m, n) = p_1^{\theta_1} p_2^{\theta_2} \dots p_k^{\theta_k}$*, onde* γ_i *é o menor dentre* $\{\alpha_i, \beta_i\}$ *e* θ_i *é o maior dentre* $\{\alpha_i, \beta_i\}$.

Proposição 11. *Se* a *e* b *são inteiros positivos, mostre que* $mmc(a, b)mdc(a, b) = ab$.

Demonstração. Basta usar a proposição anterior e observar que:

$$max\{x, y\} + \min\{x, y\} = x + y.$$

Exemplo 12. *(Torneio das Cidades 1998) É possível que* $mmc(a, b) = mmc(a + c, b + c)$ *para alguma conjunto* $\{a, b, c\}$ *de inteiros positivos?*

Não. Suponha que $a+c$ e $b+c$ possuem algum divisor primo p. Como $p \mid mmc(a+c, b+c)$, caso existam tais inteiros, devemos ter que $p \mid mmc(a, b)$. Assim, usando que pelo menos um dentre a e b é divisível por p podemos concluir que c também é divisível por p. Então, podemos cancelar o fator p:

$$mmc\left(\frac{a}{p}, \frac{b}{p}\right) = \frac{mmc(a, b)}{p} = \frac{mmc(a + c, b + c)}{p} = mmc\left(\frac{a + c}{p}, \frac{b + c}{p}\right).$$

Efetuando alguns cancelamentos, podemos supor então que $a+c$ e $b+c$ não possuem fatores primos em comum. Obtivemos um absurdo pois:

$$mmc(a + c, b + c) = (a + c)(b + c) > ab \geq mmc(a, b).$$

Exemplo 13. *(OCM 2005) Determinar os inteiros* $n > 2$ *que são divisíveis por todos os primos menores que* n.

Como $mdc(n, n - 1) = 1$, se $n - 1$ possui algum fator primo, ele não dividirá n. Assim, $n - 1 < 2$. Consequentemente não existe tal inteiro.

Exemplo 14. *Mostre que* $n^4 + n^2 + 1$ *é composto para* $n > 1$.

Veja que $n^4 + n^2 + 1 = n^4 + 2n^2 + 1 - n^2 = (n^2 + 1)^2 - n^2 = (n^2 + n + 1)(n^2 - n + 1)$. Para $n > 1$, $n^2 - n + 1 = n(n - 1) + 1 > 1$ e assim $n^4 + n^2 + 1$ é o produto de dois inteiros maiores que 1.

Exemplo 15. *Mostre que* $n^4 + 4^n$ *é composto para todo* $n > 1$.

Se n é par, certamente o número em questão é divisível por 4. Para o caso em que n é impar, iremos usar a fatoração:

$$a^4 + 4b^4 = a^4 + 4a^2b^2 + 4b^4 - 4a^2b^2 = (a^2 + 2b^2) - 4b^2b^2 = (a^2 - 2ab + 2b^2)(a^2 + 2ab + 2b^2).$$

Para n da forma $4k + 1$, faça $a = n$ e $b = 4^k$. Para n da forma $4k + 3$, faça $a = n$ e $b = 2^{2k+1}$.

Exemplo 16. *Se* $2^n + 1$ *é um primo ímpar para algum inteiro positivo* n*, prove que* n *é uma potência de 2.*

Já vimos que $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \ldots + 1)$. Se n é impar,

$$\begin{aligned}(-a)^n - 1 &= (-a-1)((-a)^{n-1} + (-a)^{n-2} + \ldots + 1) \Rightarrow \\ a^n + 1 &= (a+1)(a^{n-1} - a^{n-2} + \ldots - a + 1)\end{aligned}$$

Sendo assim, se n possuísse algum divisor primo ímpar p com $n = pb$, poderíamos escrever: $2^n + 1 = (a+1)(a^{n-1} - a^{n-2} + \ldots - a + 1)$, onde $a = 2^b$. Como $a^{n-1} - a^{n-2} + \ldots - a + 1 > 1$, o número $2^n + 1$ não seria primo.

Exemplo 17. *Dados que $p, p+10$ e $p+14$ são números primos, encontre p.*

Vamos analisar os possíveis restos na divisão por 3 de p. Se p deixa resto 1, então $p + 14$ é um múltiplo de 3 maior que 3 e consequentemente não poderá ser um número primo. Se o resto é 2, então $p + 10$ é um múltiplo de 3 maior que 3 e também não poderá ser um número primo. Assim, o resto de p por 3 é 0 e consequentemente $p = 3$.

Exemplo 18. *(Áustria-Polônia) Dados naturais n e $a > 3$ ímpar, mostre que $a^{2^n} - 1$ tem pelo menos $n + 1$ divisores primos distintos.*

Usando a fatoração da diferença de quadrados, temos que:

$$a^{2^k} - 1 = (a^{2^{k-1}} + 1)(a^{2^{k-2}} + 1) \ldots (a+1)(a-1).$$

Assim, $a^{2^m} + 1 \mid a^{2^k} - 1$ se $k > m$. Como a é impar, podemos concluir que:

$$mdc(a^{2^k} + 1, a^{2^m} + 1) = mdc(a^{2^k} - 1 + 2, a^{2^m} + 1) = mdc(2, a^{2^m} + 1) = 2.$$

Sendo assim, na fatoração:

$$\frac{a^{2^n} - 1}{2^n} = \frac{(a^{2^{n-1}} + 1)}{2} \frac{(a^{2^{n-2}} + 1)}{2} \ldots \frac{(a+1)}{2} \frac{(a-1)}{2},$$

temos o produto de pelo menos n inteiros primos entre si e consequentemente seus fatores primos são distintos. Para cada termo $\frac{(a^{2^i}+1)}{2}$, temos um fator primo p_{i+1} diferente de 2. Daí, $a^{2^n} - 1$ possui pelo menos $n + 1$ fatores primos distintos, a saber, $\{2, p_1, p_2, \ldots, p_n\}$.

Exemplo 19. *(Rioplatense 1999) Sejam $p_1, p_2, \ldots, p_k$ primos distintos. Considere todos os inteiros positivos que utilizam apenas esses primos (não necessariamente todos) em sua fatoração em números primos, formando assim uma seqüência infinita*

$$a_1 < a_2 < \cdots < a_n < \cdots .$$

Demonstre que, para cada natural c, existe um natural n tal que

$$a_{n+1} - a_n > c.$$

Suponha, por absurdo, que exista $c > 0$ tal que $a_{n+1} - a_n \leq c$, $\forall\, n \in \mathbb{N}$. Isso significa que as diferenças entre os termos consecutivos de $(a_n)_{n\geq 1}$ pertencem ao conjunto $\{1, 2, \ldots, c\}$, logo são finitas. Sejam $d_1, d_2, \ldots, d_r$ essas diferenças. Seja α_i o maior expoente de p_i que aparece na fatoração de todos os d_j.

Considere então o número $M = p_1^{\alpha_1+1}p_2^{\alpha_2+1}\cdots p_k^{\alpha_k+1}$. É claro que M pertence à seqüência, ou seja, $M = a_n$, para algum n. Vejamos quem será a_{n+1}. Por hipótese, existe i tal que $a_{n+1} - a_n = d_i$. Como $a_{n+1} > a_n$, existe um primo p_j que divide a_{n+1} com expoente maior ou igual a $\alpha_j + 1$. Caso contrário,

$$a_n < a_{n+1} < p_1^{\alpha_1+1}p_2^{\alpha_2+1}\cdots p_k^{\alpha_k+1} = a_n\,,$$

absurdo. Daí, $p_j^{\alpha_j+1}|a_n \Rightarrow p_j^{\alpha_j+1}|d_i$, novamente um absurdo, pela maximalidade de α_j.

Logo, o conjunto de todas as diferenças não pode ser finito e, portanto, dado qualquer $c > 0$, existe um natural n tal que $a_{n+1} - a_n > c$.

Problemas Propostos

Problema 20. *Dado que p, $2p+1$ e $4p^2+1$ são números primos, encontre p.*

Problema 21. *Dado o par de primos p e $8p^2+1$, encontre p.*

Problema 22. *Dado o par de primos p e p^2+2, prove que p^3+2 também é um número primo.*

Problema 23. *Dado que p, $4p^2+1$ e $6p^2+1$ são números primos, encontre p.*

Problema 24. *Os números de Fermat são os números da forma $2^{2^n}+1$. Prove que o conjunto dos divisores primos dos termos da seqüência de Fermat é infinito.*

Problema 25. *Mostre que todo inteiro n pode ser escrito de maneira única na forma $n = ab$, onde a é um inteiro livre de quadrado e b é um quadrado perfeito. Um inteiro é dito livre de quadrado se não é divisível por nenhum quadrado perfeito maior que 1.*

Problema 26. *Prove que todo primo maior que 3 é da forma 6k+1 ou 6k+5.*

Problema 27. *Prove que todo inteiro da forma 3k+2 tem um fator primo da mesma forma.*

Problema 28. *Prove que existem infinitos primos da forma 4k+3 e 6k +5.*

Problema 29. *Prove que se n é composto, então possui um fator primo $p \leq \sqrt{n}$.*

Problema 30. *(OBM 1998) São dados 15 números naturais maiores que 1 e menores que 1998 tais que dois quaisquer são primos entre si. Mostre que pelo menos um desses 15 números é primo.*

Problema 31. *Mostre que $n|$(n-1)! para todo número composto n.*

Problema 32. *Suponha que n >1. Mostre que a soma dos inteiros dos inteiros positivos não excedendo n divide o produto dos inteiros positivos não excedendo n se, e somente se, n é composto.*

Exemplo 33. *(Rússia* 1995*) Encontre todos os primos p para os quais* $p^2 + 11$ *tenha exatamente seis divisores distintos, incluindo* 1 *e* $p^2 + 11$.

Problema 34. *(Irlanda 2002) Encontre todas as soluções inteiras positivas de* $p(p+3) + q(q+3) = n(n+3)$, *onde* p, q *são primos.*

Exemplo 35. *Prove que qualquer quadrado perfeito positivo tem mais divisores que deixam resto* 1 *na divisão por* 3 *do que divisores que deixam resto* 2 *na divisão por* 3.

Dicas e Soluções

19. Analisemos o resto de p na divisão por 3. Se p deixar resto 1, o número $2p+1$ será divisível por 3. Se p deixar resto 2, o número $4p+1$ será divisível por 3. Em ambos os casos, $2p+1, 4p+1 > 3$ e obtemos assim um absurdo.

20. Analisemos o resto de p na divisão por 3. Se p deixa resto 1 ou 2, p^2 deixa resto 1 e consequentemente $8p^2+1$ deixa resto 0 por 3 mas certamente é maior que 3. Um absurdo, logo $p = 3$.

21. Analisemos o resto na divisão por 3. Se p não é múltiplo de 3, $p^2 + 2$ é divisível por 3 e maior que 3. Um absurdo, logo $p = 3$ e $p^3 + 2 = 29$.

22. Analise os restos na divisão por 5.

23. Iremos usar a fatoração do exemplo 17:

$$2^{2^n} - 1 = (2^{2^{n-1}} + 1)(2^{2^{n-2}} + 1)\dots(2+1)(2-1).$$

    Assim, se $k > m$,

$$mdc(2^{2^k} + 1, 2^{2^m} + 1) = mdc(2^{2^k} - 1 + 2, 2^{2^m} + 1) = mdc(2, 2^{2^m} + 1) = 1,$$

    produzindo que quaisquer dois números de Fermat distintos são primos entre si e isso necessariamente implica que o conjunto de seus divisores primos é infinito.

24. Analise os restos na divisão por 2 e 3.

27. Tente imitar a prova de Euclides para a existência de infinitos primos.

29. Se n é composto, podemos escrever $n = ab$ com $1 < a \leq b \leq <$. Assim, $a^2 \leq n$ e $a \leq \sqrt{n}$. Para terminar, basta considerar qualquer divisor primo de a.

30. Dado $1 < n < 1998$, se ele não for primo, usando o exercício anterior, ele tem que ter um fator primo menor que 1998, ou seja, um fator primo menor que 45. Como só existem 14 primos menores que 45, e são 15 números, um deles será primo.

31. Escreva $n = ab$ e analise as aparições de a e b no produto $(n-1)\cdot(n-2)\ldots 2\cdot 1$.

33. Se $p \neq 3$, $3 \mid p^2+11$. Analogamente, se $p \neq 2$, $4 \mid p^2+11$. Assim, exceto nesses dois casos, $12 \mid p^2+11$ e podemos encontrar mais que 6 divisores distintos: $\{1,2,3,4,6,12,p^2+11\}$. Agora, teste $p=2$ e $p=3$ para verificar que $p=3$ é a única solução.

34. Seja
$$n = 3^{\gamma}\cdot p_1^{\alpha_1}\cdots p_n^{\alpha_n}\cdot q_1^{\beta_1}\cdots q_m^{\beta_m}$$
a decomposição de n em fatores primos, onde cada p_i deixa resto 1 por 3 e cada q_j deixa resto 2 por 3. Então
$$n^2 = 3^{2\gamma}\cdot p_1^{2\alpha_1}\cdots p_n^{2\alpha_n}\cdot q_1^{2\beta_1}\cdots q_m^{2\beta_m}.$$
Um divisor de n^2 deixa resto 1 por 3 se e somente se possuir uma quantidade par de primos q_j, contados com repetição. Mais especificamente, se e somente se a soma dos expoentes de $q_1,\ldots,q_m$ for par. Assim, a quantidade de divisores dessa forma é igual a
$$D_1 = (2\alpha_1+1)\cdots(2\alpha_n+1)\left[\frac{1}{2}(2\beta_1+1)(2\beta_2+1)\cdots(2\beta_m+1)+1\right].$$
Enquanto para se obter um divisor que deixe resto 2 por 3, precisamos de uma quantidade ímpar de fatores primos da forma $3k+2$. Assim, a quantidade de divisores dessa forma é:
$$D_2 := (2\alpha_1+1)(2\alpha_2+1)\cdots(2\alpha_n+1)\left(\frac{1}{2}(2\beta_1+1)(2\beta_2+1)\cdots(2\beta_m+1)\right).$$
Daí, segue facilmente que $D_1 > D_2$.

Referências

[1] E. Carneiro, O. Campos and F. Paiva, Olimpíadas Cearenses de Matemática 1981-2005 (Níveis Júnior e Senior), Ed. Realce, 2005.

[2] S. B. Feitosa, B. Holanda, Y. Lima and C. T. Magalhães, Treinamento Cone Sul 2008. Fortaleza, Ed. Realce, 2010.

[3] D. Fomin, A. Kirichenko, Leningrad Mathematical Olympiads 1987-1991, MathPro Press, Westford, MA, 1994.

[4] D. Fomin, S. Genkin and I. Itenberg, Mathematical Circles, Mathematical Words, Vol. 7, American Mathematical Society, Boston, MA, 1966.

[5] I. Niven, H. S. Zuckerman, and H. L. Montgomery, An Introduction to the Theory of Numbers.

Teoria dos Números 04 - MMC, MDC e os Números Primos

Problema 1. Um primo p pode ser expresso como a diferença de quadrados de dois inteiros positivos. Encontre o resto da divisão de $p^2 + 138$ por 4.

Solução. Temos $p = a^2 - b^2 = (a-b)(a+b)$. Como p é primo devemos ter $a - b = 1$. Dai, $p = a + b = 2b + 1$. Portanto, $p^2 + 138 = 4b^2 + 4b + 1 + 138 = 4(b^2 + b + 34) + 3$ deixa resto 3 na divisão por 4.

Problema 2. Encontre todos os primos p tais que $p = 3^m - 3^n$, onde m, n são inteiros não negativos.

Solução. Devemos ter $n < m$. Sendo assim, $p = 3^m - 3^n = 3^n(3^{m-n} - 1)$. Como p é primo e $3^{m-n} - 1 \neq 1$, devemos ter $3^{m-n} - 1 = p$ e $3^n = 1$. Concluímos que $n = 0$ e $p = 3^m - 1$ é par. Dessa forma, p é igual ao único primo par, 2.

Problema 3. Encontre todos os inteiros positivos n para os quais $3n - 4$, $4n - 5$ e $5n - 3$ são todos primos.

Solução. A soma dos três números é um número par, então plo menos um deles é par. O único número primo par é 2. Só $3n - 4$ e $5n - 3$ podem ser pares. Resolvendo as equações $3n - 4 = 2$ e $5n - 3 = 2$ encontramos $n = 2$ e $n = 1$, respectivamente. É trivial conferir que $n = 2$ torna todos os três números primos.

Problema 4. Se p e q são primos e $x^2 - px + q = 0$ tem duas raizes inteiras positivas distintas, encontre p e q.

Solução. Sejam x_1 e x_2, com $x_1 < x_2$, as duas raizes. Então $x^2 - px + q = (x - x_1)(x - x_2)$, implicando que $p = x_1 + x_2$ e $q = x_1x_2$. Já que q é primo, $x_1 = 1$. Daí, $q = x_2$ e $p = x_2 + 1$ são dois primos consecutivos; são eles, $q = 2$ e $p = 3$.

Problema 5. Prove que se p e $p^2 + 8$ são primos, então $p^3 + 8p + 2$ é primo.

Solução. Se p não é múltiplo de 3 então p^2 deixa resto 1 na divisão por 3, de forma que $p^2 + 8$ é múltiplo de 3 e não é primo. Logo, p deve ser múltiplo de 3. Como é primo, $p = 3$. Daí, $p^3 + 8p + 2 = 53$ que é primo.

Problema 6. Encontre todos os possíveis valores de $n \geq 1$ para os quais existem n inteiros positivos consecutivos tais que sua soma é um número primo.

Solução. Claramente, nós temos $n = 1$ tomando qualquer número primo. Nós também temos $n = 2$ já que todo número ímpar pode ser escrito como soma de dois números consecutivos. Suponha $p = a + (a + 1) + \ldots + (a + k)$ para algum primo p e inteiros positivos a e $k \geq 2$. Então $2p = (k + 1)(2a + k)$. Tanto $k + 1$ quanto $2a + k$ são maiores que 2. De forma que $\frac{(k + 1)(2a + k)}{2}$ é composto. Isso é uma contradição já que p é um número primo. Sendo assim, $n = 1$ ou 2.

Problema 7. Seja p um primo ímpar. Encontre os pares de inteiros positivos (x, y) tais que $x^2 = p + y^2$.

Solução. Temos $p = x^2 - y^2 = (x - y)(x + y)$. Como x, y são inteiros positivos $x - y < x + y$. Do fato de p ser primo temos $x - y = 1$ e $x + y = p$. Resolvendo encontramos $x = \frac{p + 1}{2}$ e $y = \frac{p - 1}{2}$.

Problema 8. Para quantos valores de n o número $1! + 2! + \ldots + n!$ é primo?

Solução. Para $n = 1$ temos $1! = 1$ que não é primo. Para $n = 2$ temos $1! + 2! = 3$ que é primo. Para $n = 3$ temos $1! + 2! + 3! = 9$. Agora, para $n \geq 4$ temos

$$1! + 2! + 3! + 4! + \ldots + n! = 9 + 4! + \ldots + n!.$$

Note que todos os termos são divisíveis por 3, logo para $n \geq 4$ não temos solução. Sendo assim, o único inteiro n que satisfaz essa condição é $n = 3$.

Problema 9. Mostre que não existe nenhuma progressão aritmética infinita composta somente de números primos.

Solução. Suponha que existe uma progressão deste tipo. Seja p_1 o termo inicial e r a razão da sequência. Então o termo geral da sequência é $p_n = p_1 + (n - 1)r$. Tomando $n = p_1 + 1$ temos $p_{p_1+1} = p_1 + [(p_1 + 1) - 1]r = p_1(1 + r)$, um número composto. Chegamos a um absurdo. Logo, não existe nenhuma $P.A.$ infinita composta somente de primos.

Problema 10. Encontre todos os valores inteiros positivos de n para os quais $n^4 + 4$ é um número primo.

Solução. $n^4 + 4 = n^4 + 4n^2 + 4 - 4n^2 = (n^2 + 2n + 2)(n^2 - 2n + 2)$. Para $n = 1$, $n^4 + 4 = 5 \cdot 1$, um primo. Para $n > 1$, $n^2 + 4$ é um número composto uma vez que ele tem dois fatores $n^2 + 2n + 2$ e $n^2 - 2n + 2$, cada um maior do que 1.
Sendo assim, $n^4 + 4$ é primo somente para $n = 1$.