Polos Olímpicos de Treinamento Intensivo (POTI)

Curso de Teoria dos Números - Nível 2

Aula 4 - Números Primos, MDC e MMC

Prof. Samuel Feitosa

Arquivo Original[1]

[1] **Documento:** "... gaia/educacional/matematica/pot2tn04/Aula04-MMC_MDC_e_os_Numeros_Primos.pdf".

Sumário

1 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, ..., p_n. Considere o número $X = p_1 p_2 \dots p_n + 1$. 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 $1001! + 2$, $1001! + 3$, ..., $1001! + 1001$. Veja $i | 1001! + i$ para todo $i = 2, 3, \dots, 1001$.

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, ..., 1000, temos 168 números primos (mas só usaremos o fato de que existem mais de dois primos nesse bloco). Comparando os blocos consecutivos $k + 1$, $k + 2$, ..., $k + 1000$ e $k + 2$, $k + 3$, ..., $k + 1001$, 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, ..., 1000 até $1001! + 2$, $1001! + 3$, ..., $1001! + 1001$, 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 $a|bc$ e $mdc(a,b) = 1$. Então, $a|c$.*

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

Em particular, se p é um número primo e $p|ab$, então $p|a$ ou $p|b$. 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 $k = 1, \ldots, 1995$, $\dfrac{a_{k-1}}{a_k}$ 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 $\dfrac{a_{k-1}}{a_k}$, 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:*

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

Então, $mdc(m,n) = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_k^{\gamma_k}$ e $mmc(m,n) = p_1^{\theta_1} p_2^{\theta_2} \ldots p_k^{\theta_k}$, 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 algum conjunto $\{a,b,c\}$ de inteiros positivos?*

Não. Suponha que $a + c$ e $b + c$ possuem algum divisor primo p. Como $p|mmc(a + c, b + c)$, caso existam tais inteiros, devemos ter que $p|mmc(a,b)$. 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:

$$\begin{aligned} a^4 + 4b^4 = &\quad a^4 + 4a^2b^2 + 4b^4 - 4a^2b^2 = (a^2 + 2b^2) - 4b^2b^2 \\ = &\quad (a^2 - 2ab + 2b^2)(a^2 + 2ab + 2b^2). \end{aligned}$$

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,

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

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, $a^{2^m} + 1 | a^{2^k} - 1$ 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:

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

temos o produto de pelo menos n inteiros primos entre si e consequentemente seus fatores primos são distintos. Para cada termo $\dfrac{(a^{2^i} + 1)}{2}$, 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, ..., 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, ..., 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 $a_{n+1} - a_n > c$.

1.1 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 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.*

1.2 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:

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

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 $p \neq 3$, $3|p^2+11$. Analogamente, se $p \neq 2$, $4|p^2+11$. Assim, exceto nesses dois casos, $12|p^2+11$ 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 $D_1 > D_2$.

1.3 Referências

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.