Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 2

Prof. Samuel Feitosa

Aula 9

O Teorema de Euler

Nesta aula, obteremos uma generalização do teorema de Fermat.

Definição 1. *Dado $n \in \mathbb{N}$, denotaremos o número de naturais menores ou iguais a n e relativamente primos com n por $\phi(n)$.*

Segue imediatamente da definição de $\phi(n)$ que $\phi(1) = 1, \phi(2) = 1, \phi(3) = 2, \phi(5) = 4$ e $\phi(6) = 2$. Se p é primo, $\phi(p) = p - 1$.

Lema 2. *Se p é um número primo e k um número natural, então:*

$$\phi(p^k) = p^{k-1}(p-1).$$

Os únicos números do conjunto $\{1, 2, \ldots, p^k\}$ que não são relativamente primos com p^k são aqueles que são divisíveis por p. A quantidade de tais números é $\frac{p^k}{p} = p^{k-1}$. Sendo assim, $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

Nosso próximo objetivo será encontrar uma fórmula para calcular explicitamente $\phi(m)$ em função da fatoração em primos de m. Precisaremos relembrar um exemplo estudado na aula 6:

Lema 3. *Sejam m um número natural, l um número natural relativamente primo com m e r um inteiro arbitrário. Então, o conjunto:*

$$r, l + r, 2l + r, \ldots, (m-1)l + r;$$

é um sistema completo de restos módulo m.

Suponha, por absurdo, que existem dois inteiros i e j com $0 \leq i < j < m$ e para os quais tenhamos $r + il \equiv r + jl \pmod{m}$. Assim, $(j-i)l \equiv 0 \pmod{m}$. Como l é relativamente primo com m, devemos ter $j - i \equiv 0 \pmod{m}$. Obtemos um absurdo pois $0 < j - i < m$. Consequentemente, temos um conjunto de m inteiros todos incongruentes módulo m e, portanto, tal conjunto é um sistema completo de restos.

Teorema 4. *Se l e m são números naturais primos entre si, então:*

$$\phi(ml) = \phi(m)\phi(l).$$

Demonstração. Como $\phi(1) = 1$, o teorema anterior é valido quando $m = 1$ ou $n = 1$. Suponha então que $m, l > 1$. Façamos uma contagem dupla. Primeiramente, usando a definição, $\phi(mn)$ é o número de inteiros da tabela abaixo que são relativamente primos com ml.

$1,$	$2,$	$\ldots,$	$r,$	$\ldots,$	$l,$
$1+l,$	$l+2,$	$\ldots,$	$l+r,$	$\ldots,$	$2l,$
$21+l,$	$2l+2,$	$\ldots,$	$2l+r,$	$\ldots,$	$3l,$
$\ldots,$	$\ldots,$	$\ldots,$	$\ldots,$	$\ldots,$	$\ldots,$
$(m-1)1+l,$	$(m-1)l+2,$	$\ldots,$	$(m-1)l+r,$	$\ldots,$	$ml,$

Seja $r \leq m$ um número natural qualquer. Considerando a r-ésima coluna da tabela, se $mdc(r, l) > 1$, nenhum de seus elementos é relativamente primo com l. Então, se buscamos os elementos que não possuem nenhum fator em comum com ml, devemos nos ater às colunas com $mdc(r, l) = 1$. O número de tais colunas é $\phi(l)$. Considerando agora a r-ésima coluna e supondo que $mdc(r, l) = 1$, em virtude do lema anterior, sabemos que os restos de seus elementos na divisão por m formam exatamente o conjunto $\{0, 1, \ldots, m\}$ e dentre eles existem exatamente $\phi(m)$ números relativamente primos com m. Sendo assim, podemos contar os números relativamente primos com ml atráves do número de colunas "boas"e do número de "bons"elementos em cada uma delas, obtendo: $\phi(m)\phi(l)$.

Corolário 5. *Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ é a fatoração em primos de n, então:*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right)$$

De fato, pelo teorema anterior,

$$\begin{aligned}
\phi(n) &= \phi(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}) \\
&= \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})\ldots\phi(p_k^{\alpha_k}) \\
&= p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1)\ldots p_k^{\alpha_k - 1}(p_k - 1) \\
&= p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_k^{\alpha_k - 1}(p_1 - 1)(p_2 - 1)\ldots(p_k - 1) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right)
\end{aligned}$$

Exemplo 6. *Mostre que qualquer $n \geq 7$ pode ser escrito na forma $a + b$, com a e b naturais primos entre si, ambos maiores que 1.*

Podemos escrever $b = n - a$ e nosso objetivo é encontrar a com $1 < a < n - 1$ tal que $mdc(a, n - a) = 1$. Para isso, basta que $mdc(a, n) = 1$. Pelo corolário anterior,

$$\phi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_k^{\alpha_k - 1}(p_1 - 1)(p_2 - 1)\ldots(p_k - 1)$$

Se a expressão anterior é igual à 2, necessariamente devemos ter $\alpha_i = 1$ e $p_i = 2$ ou 3 para todo i. Sendo assim, $n \leq 6$. Logo, $\phi(n) > 2$ e existe pelo menos outro número natural diferente de 1 e $n-1$ que é relativamente primo com n.

Exemplo 7. *Prove que existem infinitos inteiros positivos n tais que*

$$\phi(n) = \frac{n}{3}.$$

Basta tomar $n = 2 \cdot 3^m$, onde m é um inteiro positivo. Então:

$$\phi(n) = \phi(2 \cdot 3^m) = \phi(2)\phi(3^m) = 2 \cdot 3^{m-1} = \frac{n}{3}.$$

Exemplo 8. *Se n é um inteiro positivo composto, então*

$$\phi(n) \leq n - \sqrt{n}$$

Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, usando que n é composto, podemos garantir que existe um fator primo p_i tal que $p_i \leq \sqrt{n}$. Assim,

$$\begin{aligned}
\phi(n) &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right) \\
&\leq n\left(1 - \frac{1}{p_i}\right) \\
&\leq n\left(1 - \frac{1}{\sqrt{n}}\right) \\
&= n - \sqrt{n}
\end{aligned}$$

Teorema 9. *(Teorema de Euler) Se $mdc(a, m) = 1$, então*

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Demonstração. A prova deste teorema será muito similar à prova do teorema de Fermat. Sejam $r_1, r_2, \ldots, r_{\phi(m)}$ os restos em $\{0, 1, 2, \ldots, m-1\}$ que são relativamente primos com m. Considere o conjunto $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$. Se dois de seus membros deixam o mesmo resto por m, digamos:

$$ar_i \equiv ar_j \pmod{m};$$

temos $r_i \equiv r_j \pmod{m}$ pois $mdc(a, m) = 1$. Claramente isso é uma contradição. Além disso, $mdc(ar_i, m) = mdc(m, r_i) = 1$. Analisando os restos na divisão por m dos membros desse novo conjunto, podemos concluir que tal conjunto coincide com o conjunto dos restos iniciais. Assim,

$$\begin{aligned}
r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)} &\equiv ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\phi(m)} \\
&\equiv a^{\phi(m)} r_1 \cdot r_2 \ldots \cdot r_{\phi(m)}
\end{aligned}$$

Como $mdc(r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)}, m) = 1$, podemos cancelar esse termo em ambos os membros da congruência anterior obtendo assim o teorema de Euler.

Exemplo 10. *Encontre os últimos três dígitos de* 7^{9999}

Como $\phi(1000) = 400$, usando o Teorema de Euler, obtemos:

$$\begin{aligned} 7^{10000} &= (7^{400})^{25} \\ &\equiv 1 \pmod{1000} \end{aligned}$$

Note que $7 \cdot 143 = 1001 \equiv 1 \pmod{1000}$. Assim,

$$\begin{aligned} 7^{9999} &\equiv 7^{9999} \cdot 7 \cdot 143 \\ &\equiv 7^{10000} \cdot 143 \\ &\equiv 143 \pmod{1000} \end{aligned}$$

Logo, 7^{9999} termina em 143.

Exemplo 11. *(Putnam 1972) Prove que não existe um inteiro* $n > 1$ *tal que* $n|2^n - 1$.

Se existem tais inteiros positivos, denotemos por m o menor deles. Claramente m é ímpar, pelo teorema de Euler, podemos garantir que:

$$m \mid 2^{\phi(m)} - 1.$$

Seja $d = mdc(m, \phi(m))$. Pelo problema 27 da aula 3, temos $2^d - 1 = mdc(2^m - 1, 2^{\phi(m)} - 1)$. Como $m \mid mdc(2^m - 1, 2^{\phi(m)} - 1)$, $d > 1$. Além disso, $d \leq \phi(m) < m$ e $d \mid 2^d - 1$. Isso é um absurdo pois m é o menor inteiro maior que 1 com tal propriedade.

Exemplo 12. *(Olimpíada de Matemática Argentina) Demostre que para cada número natural* n*, existe uma potência de 2 cuja expansão decimal tem entre seus últimos* n *dígitos (da direita) mais de* $\frac{2n}{3}$ *dígitos que são iguais a 0.*

Se 2^k tiver um resto muito pequeno módulo 10^n, poderemos garantir que existirão muitos zeros consecutivos entre seus últimos dígitos. Para obtermos a equação $2^k \equiv r \pmod{10^n}$ com r pequeno, é interessante começarmos analisando $2^k \pmod{5^n}$ uma vez que $mdc(2, 5^n) = 1$. Façamos isso. Pelo teorema de Euler, temos:

$$\begin{aligned} 2^{\phi(n)} &\equiv 1 \pmod{5^n} \Rightarrow \\ 2^{\phi(n)+n} &\equiv 2^n \pmod{10^n}. \end{aligned}$$

Como $2^n = 8^{n/3} < 10^{n/3}$, podemos concluir que 2^n possui menos que $\frac{n}{3}$ dígitos e, consequentemente, entre os últimos n dígitos de $2^{\phi(n)+n}$ existem pelo menos $n - \frac{n}{3} = \frac{2n}{3}$ dígitos consecutivos iguais à zero.

Exemplo 13. *(IMO 1971) Prove que a sequência* $2^n - 3 (n > 1)$ *contém uma subsequência de números primos entre si dois a dois.*

Uma boa estratégia é construir uma sequência recursivamente. Suponha que já tenhamos escolhido os termos $a_1, a_2, \ldots, a_k$ na sequência de modo que $mdc(a_i, a_j) = 1$. Como poderemos escolher o próximo termo a_{k+1} da forma $2^n - 3$? Claramente $mdc(2, a_i) = 1$. Desde que $\phi(a_i) \mid n$, poderemos usar o teorema de Euler para obter:

$$\begin{aligned} 2^n - 3 &\equiv 1 - 3 \\ &\not\equiv 0 \pmod{a_i} \end{aligned}$$

Sendo assim, pelo teorema 4, basta escolhermos:

$$n = \phi(a_1 \cdot a_2 \cdot \ldots \cdot a_k) = \phi(a_1)\phi(a_2)\ldots\phi(a_k);$$

que naturalmente será um múltiplo de cada $\phi(a_i)$. Logo, podemos definir

$$a_{k+1} = 2^{\phi(a_1 \cdot a_2 \cdot \ldots \cdot a_k)} - 3$$

e assim temos uma sequência de termos infita satisfazendo as condições do enunciado.

Problemas Propostos

Problema 14. *Encontre todos os números naturais n para os quais $\phi(n)$ não é divisível por 4.*

Problema 15. *Prove que se $p > 2$ e $2p + 1$ são ambos números primos, então para $n = 4p$ vale que*

$$\phi(n + 2) = \phi(n) + 2.$$

Problema 16. *Encontre todas as soluções nos números naturais da equação $\phi(n) = \phi(2n)$.*

Problema 17. *Encontre todas as soluções nos números naturais da equação $\phi(2n) = \phi(3n)$.*

Problema 18. *Se n possui k fatores primos distintos, prove que $2^k \mid \phi(n)$.*

Problema 19. *Prove que para qualquer número natural k, existe pelo menos um número natural n tal que*

$$\phi(n + k) = \phi(n).$$

Dica: Considere o menor divisor primo p que não é um divisor de k e estude o número $n = (p - 1)k$.

Problema 20. *Mostre que se a e b são inteiros primos entre si, então existem inteiros m e n tais que $a^m + b^n \equiv 1 \pmod{ab}$.*

Problema 21. *(Alemanha) Se n é um número natural tal que $4^n + 2^n + 1$ é primo, prove que n é potência de 3.*

Problema 22. *(USAMO 1991) Mostre que para qualquer inteiro fixo $n \geq 1$, a sequência*

$$2, 2^2, 2^{2^2}, 2^{2^{2^2}}, \ldots \pmod{n};$$

é eventualmente constante, isto é, a partir de um certo termo da sequência todos os restos obtidos na divisão por n serão iguais.

Dica: Tente considerar os casos em que n é par ou n é ímpar em separado e use indução.

Problema 23. *Encontre os últimos 8 dígitos da expansão binária de* 27^{1986}

Problema 24. *Mostre que, para qualquer inteiro positivo n com* $n \neq 2$ *e* $n \neq 6$ *temos:*

$$\phi(n) \geq \sqrt{n}.$$

Referências

[1] F. E. Brochero Martinez, C. G. Moreira, N. C. Saldanha, E. Tengan - Teoria dos Números ? um passeio com primos e outros números familiares pelo mundo inteiro, Projeto Euclides, IMPA, 2010.

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

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

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

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

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