Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 3

Carlos Gustavo Moreira

Aula 4

Números primos, números compostos e o Teorema Fundamental da Aritmética

1 O Teorema Fundamental da Aritmética

Estamos agora prontos para enunciar o teorema que caracteriza todo número natural em termos de seus "constituintes" primos.

Teorema 1 (Teorema Fundamental da Aritmética)**.** *Seja $n \geq 2$ um número natural. Podemos escrever n de uma única forma como um produto*

$$n = p_1 \cdots p_m$$

onde $m \geq 1$ é um natural e $p_1 \leq \ldots \leq p_m$ são primos.

Demonstração. Mostramos a existência da fatoração de n em primos por indução. Se n é primo não há o que provar (escrevemos $m = 1$, $p_1 = n$). Se n é composto podemos escrever $n = ab$, $a, b \in \mathbb{N}$, $1 < a < n$, $1 < b < n$. Por hipótese de indução, a e b se decompõem como produto de primos. Juntando as fatorações de a e b (e reordenando os fatores) obtemos uma fatoração de n.

Vamos agora mostrar a unicidade. Suponha por absurdo que n possui duas fatorações diferentes

$$n = p_1 \cdots p_m = q_1 \cdots q_{m'},$$

com $p_1 \leq \ldots \leq p_m$, $q_1 \leq \ldots \leq q_{m'}$ e que n é mínimo com tal propriedade. Como $p_1 \mid q_1 \cdots q_{m'}$ temos $p_1 \mid q_i$ para algum valor de i pelo corolário **??**. Logo, como q_i é primo, $p_1 = q_i$ e $p_1 \geq q_1$. Analogamente temos $q_1 \leq p_1$, e portanto $p_1 = q_1$. Mas

$$n/p_1 = p_2 \cdots p_m = q_2 \cdots q_{m'}$$

admite uma única fatoração, pela minimalidade de n, donde $m = m'$ e $p_i = q_i$ para todo i, o que contradiz o fato de n ter duas fatorações. □

Outra forma de escrever a fatoração acima é

$$n = p_1^{e_1} \ldots p_m^{e_m},$$

com $p_1 < \cdots < p_m$ e $e_i > 0$. Ainda outra formulação é escrever

$$n = 2^{e_2}3^{e_3}5^{e_5}\ldots p^{e_p}\ldots$$

onde o produto é tomado sobre *todos* os primos mas apenas um número finito de expoentes é maior do que zero. Vamos nos referir a qualquer destas expressões como a *fatoração canônica* de n em primos.

A fatoração única em primos se aplica em contextos mais gerais, como veremos mais tarde. Aqui, como aplicação imediata do Teorema Fundamental da Aritmética, vamos mostrar a prova atribuída a Euclides para a existência de infinitos primos (uma prova com mais de 2000 anos e que ainda funciona!).

Teorema 2 (Euclides). *Existem infinitos primos.*

Demonstração. Suponha por absurdo que $p_1, p_2, \ldots, p_m$ fossem *todos* os primos. O número $N = p_1p_2\ldots p_m + 1 > 1$ não seria divisível por nenhum primo p_i, o que contradiz o Teorema Fundamental da Aritmética. □

Observe que *não* provamos que $p_1p_2\ldots p_m+1$ é primo para algum conjunto finito de primos (por exemplo, os m primeiros primos). Aliás, $2{\cdot}3{\cdot}5{\cdot}7{\cdot}11{\cdot}13{+}1 = 30031 = 59 \cdot 509$ não é primo. Não se conhece nenhuma fórmula simples que gere sempre números primos.

Embora a quantidade de primos seja infinita, uma questão natural é saber o quão "raros" ou "frequentes" eles são. Na segunda parte do livro, discutiremos mais a fundo esta questão sobre a distribuição dos primos. Por outro lado, é interessante notar que existem cadeias arbitrariamente longas de números compostos consecutivos: na sequência

$$(k+1)!+2, (k+1)!+3, (k+1)!+4, \ldots, (k+1)!+(k+1),$$

nenhum termo é primo, pois eles admitem fatores próprios $2, 3, 4, \ldots, k+1$, respectivamente.

Uma interessante prova alternativa, devida a Erdős, de que existem infinitos primos é a seguinte:

Suponha, por contradição, que existe um número finito de primos, digamos $p_1, p_2, \ldots, p_k$. Seja n um número natural. Então podemos escrever qualquer número $m \leq n$ na forma $m = m_1^2m_2$, onde $m_1^2 \leq n$ e

$$m_2 = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k} \qquad \text{onde } a_k = 0 \text{ ou } 1 \text{ para cada } k.$$

Assim, considerando todas as possíveis maneiras de escrever os naturais $m \leq n$, temos: 2^k escolhas para m_2 e no máximo $\lfloor\sqrt{n}\rfloor$ escolhas para m_1. Ou seja, para todo n natural, vale que

$$n \leq 2^k\sqrt{n},$$

o que é absurdo, pois esta desigualdade não vale para n suficientemente grande. □

Exemplo 3 (OIbM1987). *A sequência p_n é definida da seguinte forma:*

(i) $p_1 = 2$.

(ii) Para todo $n \geq 2$, p_n é o maior divisor primo da expressão

$$p_1 p_2 p_3 \cdots p_{n-1} + 1.$$

Demonstre que p_n é diferente de 5.

SOLUÇÃO: Dado que $p_1 = 2$, $p_2 = 3$, $p_3 = 7$, segue-se que para qualquer $n \geq 3$, $p_1 p_2 \cdots p_{n-1}$ é múltiplo de 2 e de 3, portanto $p_1 p_2 \cdots p_{n-1} + 1$ não é múltiplo nem de 2 nem de 3. Além disso, como $p_1 = 2$, então p_n é ímpar para todo $n \geq 2$, assim $p_1 p_2 \cdots p_{n-1}$ não é múltiplo de 4.

Suponhamos que exista n tal que $p_n = 5$, isto é, o maior divisor primo de $p_1 p_2 \cdots p_{n-1} + 1$ é 5. Como 2 e 3 não dividem $p_1 p_2 \cdots p_{n-1} + 1$, temos que

$$p_1 p_2 \cdots p_{n-1} + 1 = 5^k.$$

Portanto

$$p_1 p_2 \cdots p_{n-1} = 5^k - 1 = (5-1)(5^{k-1} + 5^{k-2} + \cdots + 5 + 1),$$

logo $4 \mid p_1 p_2 \cdots p_{n-1}$, o que é uma contradição. □

Exemplo 4. *Determine todas as ternas (a, b, c) de inteiros positivos tais que $a^2 = 2^b + c^4$.*

SOLUÇÃO: Como $a^2 = 2^b + c^4 \iff (a - c^2)(a + c^2) = 2^b$, pelo Teorema Fundamental da Aritmética existem dois naturais $m > n$ tais que $m + n = b$, $a - c^2 = 2^n$ e $a + c^2 = 2^m$. Subtraindo as duas últimas equações, obtemos que $2c^2 = 2^m - 2^n$, assim $c^2 = 2^{n-1}(2^{m-n} - 1)$. Como 2^{n-1} e $2^{m-n} - 1$ são primos entre si, e o seu produto é um quadrado perfeito (i.e. os expoentes das potências de primos distintos são pares), novamente pelo Teorema Fundamental da Aritmética 2^{n-1} e $2^{m-n} - 1$ devem ser quadrados perfeitos. Assim, $n - 1$ é par e $2^{m-n} - 1 = (2k-1)^2$ para algum inteiro positivo k. Como $2^{m-n} = (2k-1)^2 + 1 = 4k(k-1) + 2$ é divisível por 2 mas não por 4, temos $m - n = 1$. Assim, fazendo $n - 1 = 2t$, temos que todas as soluções são da forma $(a, b, c) = (3 \cdot 2^{2t}, 4t + 3, 2^t)$ com $t \in \mathbb{N}$ e é fácil verificar que todos os números desta forma são soluções. □

Do Teorema Fundamental da Aritmética, segue que todo divisor de $n = p_1^{e_1} \ldots p_m^{e_m}$ é da forma

$$p_1^{d_1} \ldots p_m^{d_m}$$

com $0 \leq d_i \leq e_i$. Assim, obtemos o outro algoritmo usual para calcular o mdc de dois números: fatoramos os dois números em primos e tomamos os fatores comuns com os menores expoentes. Este algoritmo é bem menos eficiente do que o de Euclides para inteiros grandes (que em geral não sabemos fatorar de forma eficiente computacionalmente) mas é instrutivo saber que os dois algoritmos dão o mesmo resultado. Além disso, este algoritmo tem consequências teóricas importantes, como por exemplo o

Corolário 5. *Se* $\mathrm{mdc}(a,n) = \mathrm{mdc}(b,n) = 1$*, então* $\mathrm{mdc}(ab,n) = 1$*.*

Demonstração. Evidente a partir do algoritmo descrito acima. □

Para encerrar esta seção, vejamos ainda algumas outras aplicações do Teorema Fundamental da Aritmética.

Proposição 6. *Seja* $n = p_1^{e_1} \dots p_m^{e_m}$ *a fatoração de* n *em potências de primos distintos* p_i *e seja* $\sigma_k(n) \stackrel{\text{def}}{=} \sum_{d|n,\, d>0} d^k$ *a soma das* k*-ésimas potências dos divisores positivos de* n*. Então*

$$\sigma_k(n) = \frac{p_1^{(e_1+1)k} - 1}{p_1^k - 1} \cdot \ldots \cdot \frac{p_m^{(e_m+1)k} - 1}{p_m^k - 1}.$$

Para $k = 0$*, a fórmula acima deve ser interpretada tomando-se o limite* $k \to 0$*, de modo que a quantidade de divisores positivos de* n *é* $\sigma_0(n) = (e_1+1)\cdots(e_m+1)$*.*

Demonstração. Como a soma na definição de $\sigma_k(n)$ percorre todos os números da forma $d^k = p_1^{d_1 k} \dots p_m^{d_m k}$ com $0 \le d_i \le e_i$, temos a seguinte fatoração:

$$\sigma_k(n) = (1 + p_1^k + p_1^{2k} + \cdots + p_1^{e_1 k}) \cdot \ldots \cdot (1 + p_m^k + p_m^{2k} + \cdots + p_m^{e_m k}).$$

Somando as progressões geométricas $1 + p_i^k + p_i^{2k} + \cdots + p_i^{e_i k} = \frac{p_i^{(e_i+1)k}-1}{p_i^k-1}$, o resultado segue. □

Proposição 7 (Fatores do Fatorial)**.** *Seja* p *um primo. Então a maior potência de* p *que divide* $n!$ *é* p^α *onde*

$$\alpha = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Observe que a soma acima é finita pois os termos $\left\lfloor \frac{n}{p^i} \right\rfloor$ são eventualmente zero.

Demonstração. No produto $n! = 1 \cdot 2 \cdot \ldots \cdot n$, apenas os múltiplos de p contribuem com um fator p. Há $\left\lfloor \frac{n}{p} \right\rfloor$ tais múltiplos entre 1 e n. Destes, os que são múltiplos de p^2 contribuem com um fator p extra e há $\left\lfloor \frac{n}{p^2} \right\rfloor$ tais fatores. Dentre estes últimos, os que são múltiplos de p^3 contribuem com mais um fator p e assim por diante, resultando na fórmula acima. □

Exemplo 8. *Determine com quantos zeros termina* 1000!*.*

Solução: O problema é equivalente a determinar qual a maior potência de 10 que divide 1000! e como há muito mais fatores 2 do que 5 em 1000!, o expoente desta potência coincide com o da maior potência de 5 que divide 1000!, ou seja,

$$\left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{5^2} \right\rfloor + \left\lfloor \frac{1000}{5^3} \right\rfloor + \left\lfloor \frac{1000}{5^4} \right\rfloor = 249.$$

Assim, 1000! termina com 249 zeros. □

Problemas Propostos

Problema 9. *Mostre que se n é um número natural composto, então n é divisível por um primo p com $p \leq \lfloor \sqrt{n} \rfloor$.*

Problema 10 (IMO1989). *Prove que, para todo inteiro positivo n, existem n inteiros positivos consecutivos, nenhum dos quais é potência de primo.*

Problema 11 (Chi1998). *Encontre todos os n para os quais $1 + \binom{n}{1} + \binom{n}{2} + \binom{n}{3}$ divide 2^{2000}.*

Problema 12 (IMO2002). *Sejam $d_1 < d_2 < \cdots < d_k$ os divisores positivos de um inteiro $n > 1$. Seja $d = d_1 d_2 + d_2 d_3 + \cdots + d_{k-1} d_k$. Mostre que $d < n^2$ e encontre todos os n para os quais $d \mid n^2$.*

Problema 13 (IMO1997). *Encontre todos os pares (x, y) de inteiros positivos tais que $x^{y^2} = y^x$.*

Problema 14. *Generalizar o resultado anterior para $x^{y^n} = y^x$, onde x e y são inteiros positivos.*

Problema 15 (IMO1984). *Sejam a, b, c, d inteiros ímpares tais que $0 < a < b < c < d$ e $ad = bc$. Demonstre que se $a + d = 2^k$ e $b + c = 2^m$ para inteiros k e m, então $a = 1$.*

Dicas e Soluções

10. Considere os inteiros $(n+1)!^2 + k, 2 \leq k \leq n+1$.

11. Note que $1 + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} = (n+1) \cdot \frac{n^2-n+6}{6} = (n+1) \cdot \frac{(n+1)^2-3(n+1)+8}{6}$.

12. Temos $d = \frac{n^2}{d_k d_{k-1}} + \frac{n^2}{d_{k-1} d_{k-2}} + \cdots + \frac{n^2}{d_2 d_1} < n^2 \cdot (\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots) = n^2 \cdot (\frac{1}{1} - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \frac{1}{3} - \frac{1}{4} + \cdots) = n^2$. Por outro lado, se p é o menor primo que divide n^2, temos que $d \geq d_{k-1} d_k = \frac{n^2}{p}$. Como $\frac{n^2}{p}$ é o maior divisor próprio de n^2 e $d > d_{k-1} d_k$ se $k > 2$, temos que $d \mid n^2$ se, e somente se, $n = p$ é primo.

13. Sejam $x = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ e $y = p_1^{\beta_1} \ldots p_n^{\beta_n}$ as fatorações canônicas de x e y. Temos $\alpha_j = \frac{p}{q} \cdot \beta_j$ e $x = y^{p/q}$ onde $\frac{p}{q} = \frac{x}{y^2} \in \mathbb{Q}$, com p, q inteiros positivos e $\mathrm{mdc}(p, q) = 1$. Assim, $p \mid \alpha_j$ e $q \mid \beta_j$ para todo j, donde $x = a^p$ e $y = a^q$, para um certo inteiro positivo a. Se $a = 1$, temos $x = y = 1$, o que é uma solução. Suponhamos que $a > 1$. A igualdade $x^{y^2} = y^x$ pode ser escrita como $(a^p)^{y^2} = (a^q)^x$, que equivale a $py^2 = qx$, ou seja, $pa^{2q} = qa^p$. Se $2q \geq p$, temos $\frac{q}{p} = a^{2q-p} \in \mathbb{N}$, donde $p = 1$ e $a^{2q-1} = a^{2q-p} = q$, absurdo, pois para todo $a \geq 2$ e $q \geq 1$, $a^{2q-1} \geq 2q - 1 + 1 = 2q > q$. Se, por outro lado, $2q < p$, teremos $\frac{p}{q} = a^{p-2q} \in \mathbb{N}$, donde $q = 1$ e $a^{p-2} = a^{p-2q} = p$.

Como $2^{n-2} > n, \forall n \geq 5$, $3^{n-2} > n, \forall n \geq 4$ e $a^{n-2} > n, \forall a \geq 4, n \geq 3$, temos que as únicas possibilidades são $(a, p) = (2, 4)$ e $(a, p) = (3, 3)$, o que nos dá as soluções $x = 16, y = 2$ e $x = 27, y = 3$, que, junto com a solução $x = y = 1$, constituem todas as soluções do problema.

15. Note que $2^k - 2^m = a + d - (b + c) = \frac{bc}{d} + d - (b + c) = (d - b)(d - c)/d > 0$. Assim, se $k > m$. De $ad = bc$, segue que $a(2^k - a) = b(2^m - b)$, o que equivale a $(b - a)(b + a) = b^2 - a^2 = 2^m(b - 2^{k-m}a)$. Como a e b são ímpares, $b - a$ e $b + a$ são pares, mas um deles não é múltiplo de 4. Assim, temos duas possibilidades: $b - a = 2^{m-1}t$ e $b + a = 2s$, com t e s ímpares ou $b - a = 2t$ e $b + a = 2^{m-1}s$, com t e s ímpares.

    Se $b - a = 2^{m-1}t$ e $b + a = 2s$, com t e s ímpares, temos em particular $b = a + 2^{m-1}t > 2^{m-1}$, absurdo, pois $b + c = 2^m$ e $b < c$, donde $b < 2^{m-1}$.

    Se $b - a = 2t$ e $b + a = 2^{m-1}s$, com t e s ímpares, temos $b = t + 2^{m-2}s$ e $a = 2^{m-2}s - t$, e, de $2^m st = (b - a)(b + a) = 2^m(b - 2^{k-m}a)$, temos $st = b - 2^{k-m}a = (2^{k-m} + 1)t - 2^{m-2}(2^{k-m} - 1)s = 2t - (2^{k-m} - 1)(2^{m-2}s - t) < 2t$ (pois $2^{m-2}s - t = a > 0$). Assim, $s < 2$, donde $s = 1$, e logo $t = st = (2^{k-m} + 1)t - 2^{m-2}(2^{k-m} - 1)s = (2^{k-m} + 1)t - 2^{m-2}(2^{k-m} - 1)$, donde $2^{m-2}(2^{k-m} - 1) = 2^{k-m}t$. Daí segue que $m - 2 = k - m$ e $t = 2^{k-m} - 1 = 2^{m-2} - 1$, donde $a = 2^{m-2}s - t = 2^{m-2} - t = 1$.

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.