Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 3

Carlos Gustavo Moreira

Aula 16

Binomiais e Primos

Começamos lembrando a

Proposição 1 (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 $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$ para todo $k > \left\lfloor \frac{\log n}{\log p} \right\rfloor$.

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. □

Observação 2. *Se $n = (a_k a_{k-1} \ldots a_1 a_0)_p = \sum_{j=0}^{k} a_j p^j$ é a representação de n na base p, temos, para cada $j \geq 1$, $\left\lfloor \frac{n}{p^j} \right\rfloor = \sum_{i=0}^{k-j} a_{i+j} p^i$, e logo a proposição acima diz que*

$$\alpha = \sum_{j=1}^{k} \sum_{i=0}^{k-j} a_{i+j} p^i = \sum_{r=1}^{k} \sum_{j=1}^{r} a_r p^{r-j} = \sum_{r=1}^{k} a_r \frac{p^r - 1}{p-1} = \frac{n - \sum_{j=0}^{k} a_j}{p-1} = \frac{n - s_p(n)}{p-1},$$

onde $s_p(n)$ é a soma dos algarismos da representação de n na base p.

Podemos usar esse resultado para provar o seguinte teorema, devido a Kummer:

Teorema 3 (Teorema de Kummer). *Sejam p um primo, m e n inteiros com $0 \leq m \leq n$. Então a maior potência de p que divide $\binom{n}{m}$ é p^α onde α é o número de "vai-uns"quando somamos m e $n-m$ na base p.*

Demonstração. Como vimos, o expoente da maior potência de p que divide $n!$ é $\frac{n-s_p(n)}{p-1}$. Analogamente, os expoentes das maiores potências de p que dividem $m!$ e $(n-m)!$ respectivamente são $\frac{m-s_p(m)}{p-1}$ e $\frac{n-m-s_p(n-m)}{p-1}$. Assim, a maior potência de p que divide $\binom{n}{m} = \frac{n!}{m!(n-m)!}$ é

$$\frac{n-s_p(n)}{p-1} - \left(\frac{m-s_p(m)}{p-1} + \frac{n-m-s_p(n-m)}{p-1} \right) = \frac{s_p(m)+s_p(n-m)-s_p(n)}{p-1}.$$

Basta ver agora que $\frac{s_p(m)+s_p(n-m)-s_p(n)}{p-1}$ é igual ao número de "vai-uns"quando somamos m e $n-m$ na base p. Para isso, notamos que no algoritmo usual de soma, escrevendo $m = \sum j = 0^k b_j p^j$ e $n-m = \sum_{j=0}^{k} c_j p^j$, com $0 \leq b_j, c_j < p$ temos $n = \sum_{j=0}^{k} (b_j + c_j) p^k$ - se não houver "vai-um"', a soma dos algarismos nessa representação de n é igual a $s_p(m) + s_p(n-m)$; quando $b_j + c_j \geq p$, escrevemos $b_j + c_j = p + d_j$, onde $0 \leq d_j \leq p-2 < p$, e trocamos na soma acima $(b_j + c_j)p^j + (b_{j+1} + c_{j+1})p^{j+1}$ por $d_j p^j + (b_{j+1} + c_{j+1} + 1)p^{j+1}$ - esta é uma operação de "vai-um"', e repetimos o processo em ordem crescente dos j. Em cada operação de 'vai-um"', a soma dos algarismos diminui em $p-1$. Assim, ao final, obtemos que $s_p(m) + s_p(n-m) - s_p(n)$ é igual a $p-1$ vezes o número total de operações de "vai-um"necessárias, o que implica o resultado desejado. □

Uma consequência deste resultado, no caso $p = 2$, é o seguinte: os inteiros positivos n tais que $\binom{n}{k}$ é par para todo k com $1 \leq k \leq n-1$ são exatamente as potências de 2. De fato, se $n = 2^r$, a representação em base 2 de n é $(100...00)_2$, com r zeros, e logo não pode haver uma soma $k + (n-k) = n$ sem "vai-uns"na base 2, a menos que $k = 0$ ou $k = n$. Por outro lado, se n não é uma potência de 2, n tem algarismos iguais a 1 além do primeiro em sua representação na base 2, e logo há somas do tipo $k + (n-k) = n$ sem "vai-uns"na base 2 (verifique!).

1 Algumas Estimativas sobre Primos

Vamos provar algumas estimativas sobre o crescimento dos primos. Seja $\pi(x)$ a quantidade de primos menores do que ou iguais a x. O seguinte argumento, devido a Erdős, mostra que $\pi(x) \geq \log x / \log 4$, para todo inteiro $x \geq 2$:

Sejam $n \geq 2$ natural, $k = \pi(n)$, e $p_1, p_2, \ldots, p_k$ os primos menores do que ou iguais a n. Então podemos escrever qualquer número $m \leq n$ na forma $m = m_1^2 m_2$, 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, temos

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

donde $n \leq 4^k$, e logo $\pi(n) = k \geq \log n / \log 4$.

Vamos ver a seguir como obter estimativas muito mais precisas sobre $\pi(n)$ usando propriedades de binomiais.

1.1 O Teorema de Chebyshev

Começamos com um

Lema 4. *Sejam n um número natural e p um número primo. Seja θ_p o inteiro tal que $p^{\theta_p} \leq 2n < p^{\theta_p+1}$. Então o expoente da maior potência de p que divide $\binom{2n}{n}$ é menor ou igual a θ_p. Em particular, se $p > \sqrt{2n}$ então o expoente desta máxima potência de p é menor do que ou igual a 1. Além disso, se $\frac{2}{3}n < p < n$ então p não divide $\binom{2n}{n}$.*

Demonstração. Sejam α e β os expoentes das maiores potências de p que dividem $(2n)!$ e $n!$ respectivamente. Sabemos da proposição 1 que

$$\alpha = \left\lfloor \frac{2n}{p} \right\rfloor + \left\lfloor \frac{2n}{p^2} \right\rfloor + \cdots \qquad \text{e} \qquad \beta = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots .$$

Portanto o expoente da máxima potência de p que divide $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ é

$$\alpha - 2\beta = \sum_{i=1}^{\theta_p} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor .$$

Mas como

$$\frac{2n}{p^i} \geq \left\lfloor \frac{2n}{p^i} \right\rfloor > \frac{2n}{p^i} - 1 \qquad \text{e} \qquad -2\left(\frac{n}{p^i} - 1\right) > -2 \left\lfloor \frac{n}{p^i} \right\rfloor \geq -2\frac{n}{p^i},$$

somando teremos que

$$2 > \left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor > -1.$$

Portanto esta última expressão só pode tomar os valores 1 e 0. Concluímos que

$$\alpha - 2\beta \leq \sum_{i=1}^{\theta_p} 1 = \theta_p.$$

Além disso, se $\frac{2n}{3} < p < n$ então $\alpha = 2$ e $\beta = 1$, logo $\alpha - 2\beta = 0$. □

Corolário 5. *Para todo inteiro positivo n, o mínimo múltiplo comum dos números $1, 2, \ldots, 2n$ é maior ou igual a $\binom{2n}{n}$.*

Podemos agora mostrar a seguinte

Proposição 6 (Chebyshev)**.** *Existem constantes positivas $c < C$ tais que*

$$c\frac{x}{\log x} < \pi(x) < C\frac{x}{\log x}$$

para todo $x \geq 2$.

Demonstração. Observemos inicialmente que $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ é múltiplo de todos os primos p que satisfazem $n < p \leq 2n$. Como

$$\binom{2n}{n} < \sum_{0 \leq k \leq 2n} \binom{2n}{k} = 2^{2n},$$

segue que o produto dos primos entre n e $2n$ é menor do que 2^{2n}. Como há $\pi(2n) - \pi(n)$ primos como esses segue que $n^{\pi(2n)-\pi(n)} < 2^{2n}$ (pois todos esses primos são maiores que n), donde $(\pi(2n) - \pi(n)) \log n < 2n \log 2$ e

$$\pi(2n) - \pi(n) < \frac{2n \log 2}{\log n}.$$

Isso implica facilmente, por indução, que

$$\pi(2^{k+1}) \leq \frac{5 \cdot 2^k}{k}$$

(começando com $k = 5$; até $k = 5$ segue de $\pi(n) \leq n/2$ para $n \geq 4$). Daí segue que se $2^k < x \leq 2^{k+1}$ então

$$\pi(x) \leq \frac{5 \cdot 2^k}{k} \leq \frac{5x \log 2}{\log x}$$

pois $f(x) = x \log 2 / \log x$ é uma função crescente para $x \geq 3$.

Vamos agora provar a outra desigualdade. Se $\binom{2n}{n} = \prod_{p<2n} p^{\alpha_p}$ é a fatoração canônica de $\binom{2n}{n}$ então pelo lema 4 temos $p^{\alpha_p} \leq 2n \iff \alpha_p \log p \leq \log 2n$ e portanto

$$\log \binom{2n}{n} = \sum_{p<2n} \alpha_p \log p \leq \pi(2n) \log(2n),$$

donde

$$\pi(2n) \geq \frac{\log \binom{2n}{n}}{\log(2n)} \geq \frac{n \log 2}{\log(2n)}$$

pois

$$\binom{2n}{n} = \frac{2n}{n} \cdot \frac{2n-1}{n-1} \cdots \frac{n+1}{1} \geq 2^n,$$

assim,

$$\pi(x) \geq \frac{x \log 2}{2 \log x}$$

para todo x par, o que implica na mesma estimativa para todo x inteiro, pois $\pi(2k-1) = \pi(2k)$. □

Corolário 7. *Seja p_n o n-ésimo número primo. Existem constantes $C' > c' > 0$ tais que*

$$c' n \log n < p_n < C' n \log n$$

para todo $n \geq 2$.

Demonstração. Se $\limsup_{n\to\infty} \frac{p_n}{n\log n} > C'$, então

$$\begin{aligned}\liminf_{x\to\infty} \frac{\pi(x)}{x/\log x} &\leq \liminf_{n\to\infty} \frac{\pi(p_n)}{p_n/\log p_n} \\ &\leq \liminf_{n\to\infty} \frac{n(\log C' + \log n + \log\log n)}{C' n \log n} = \frac{1}{C'}\end{aligned}$$

já que $x/\log x$ é crescente para $x \geq 3$. Assim, como $\liminf_{x\to\infty} \frac{\pi(x)}{x/\log x} > 0$ pelo teorema anterior, temos que existe C' tal que $p_n < C' n \log n$ para todo $n \geq 2$. Analogamente se prova a existência de c'. □

1.2 O Teorema dos Números Primos

Já vimos que existem infinitos primos; o teorema dos números primos dá uma estimativa de quantos primos existem até um inteiro x, ou seja, descreve a distribuição dos primos. Defina $\pi(x)$ como sendo o número de primos p com $2 \leq p \leq x$. Já sabemos pelo teorema de Chebyshev 6 que $\pi(x)$ está entre $cx/\log x$ e $Cx/\log x$ para duas constantes $c < C$. Na verdade, temos um resultado muito mais preciso:

Teorema 8 (Teorema dos Números Primos)**.**

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

Este resultado foi conjecturado por vários matemáticos, inclusive por Legendre e Gauß, mas a demonstração completa só foi encontrada em 1896, por de la Vallée Poussin e Hadamard (independentemente). Não demonstraremos este teorema aqui: as demonstrações elementares conhecidas são todas bastante difíceis (lembramos que uma demonstração é dita *elementar* quando não usa ferramentas avançadas: muitas demonstrações elementares são longas e sofisticadas).

Problemas Propostos

Problema 9. *a) Sejam x inteiro e p um divisor primo de $20x^2-1$. Prove que $p \equiv \pm 1 \pmod{10}$.*
b) Mostrar que existem infinitos primos que terminam no dígito 9.

Problema 10. *Mostrar que existe um intervalo de 1000 números inteiros positivos consecutivos contendo exatamente cinco números primos.*

Problema 11. *Mostrar que não existem polinômios P e Q tais que $\pi(x) = \frac{P(x)}{Q(x)}$ para todo $x \in \mathbb{N}$.*

Problema 12. *Mostrar que existem dois quadrados consecutivos tais que existem ao menos 1000 primos entre eles.*

Problema 13. *Mostrar que não existem 11 primos, todos menores que* 20000 *e em progressão aritmética.*

Problema 14. *Prove que numa progressão aritmética formada por n primos, a razão deve ser um múltiplo de $(n-1)\#$, e, a menos que n seja primo e o menor termo da progressão seja n, sua razão deve ser um múltiplo de $n\#$.*
Obs.: *Lembramos que $m\#$ denota o produto dos primos menores do que ou iguais a m.*

Problema 15. *Mostrar que para cada primo p no intervalo $\left(n, \frac{4n}{3}\right]$, p divide*

$$\sum_{j=0}^{n} \binom{n}{j}^4.$$

Dicas e Soluções

Em breve

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.