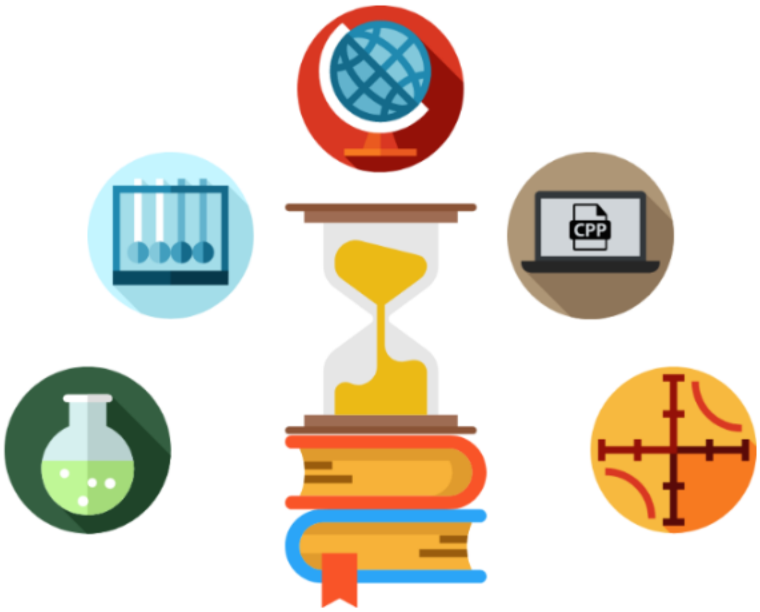
Funções Aritméticas Básicas

Roberto César Cucharero Peregrina



1 Função Soma dos Divisores

1.1 Função $\sigma(n)$

Definição : Soma dos divisores positivos de um certo número n
Exemplo : $\sigma(6) = 1+2+3+6 = 12$

1.1.1 Teorema 1

Se $n = p^k$, onde p é primo e $k \geq 1$, então a soma $\sigma(n)$ dos divisores é
$\sigma(n) = 1 + p + \cdots + p^k = \frac{p^{k+1}-1}{p-1}$

Prova: Se $n = p^k$, onde p é primo e $k \geq 1$, então os divisores positivos de n são $1, p, p^2, \ldots, p^k$. Assim $\sigma(n) = 1 + \cdots + p^k$ e os divisores forma uma progressão geométrica de razão p, então sua soma gera a soma dos divisores. $\sigma(n) = 1 + p + \cdots + p^k = \frac{p^{k+1}-1}{p-1}$

1.1.2 Teorema 2

Se $n = p_1^{k_1} \cdot p_2^{k_2}$ onde p_1 e p_2 são primos e $k_1, k_2 \geq 1$, então:

$$\sigma(n) = \sigma(p_1^{k_1})\sigma(p_2^{k_2}) = \frac{p_1^{k_1+1}-1}{p_1-1} \cdot \frac{p_2^{k_2+1}-1}{p_2-1}$$

Prova: Se $n = p_1^{k_1} \cdot p_2^{k_2}$, então os divisores positivos de n são da forma $n = p_1^{h_1} \cdot p_2^{h_2}$, onde $0 \leq h_1 \leq k_1$ e $0 \leq h_2 \leq k_2$.

Assim $\sigma(n) = 1 + p_1 + p_2 + \cdots + p_1^{k_1} \cdot p_2^{k_2}$ Fatorando : $\sigma(n) = (1 + p_1 + \cdots + p_1^{k_1}) \cdot (1 + p_2 + \cdots + p_2^{k_2})$

Portanto $\sigma(n) = \sigma(p_1^{k_1})\sigma(p_2^{k_2}) = \dfrac{p_1^{k_1+1}-1}{p_1-1} \cdot \dfrac{p_2^{k_2+1}-1}{p_2-1}$

1.1.3 Teorema 3

Seja n um inteiro positivo. Por $\sigma(n)$ indica-se a soma dos divisores positivos de n (inclusive 1 e n). Se $n = p_1^{k_1} \ldots p_r^{k_r}$ é a decomposição canônica do inteiro $n > 1$, então:

$$\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \cdots \frac{p_r^{k_r+1}-1}{p_r-1}$$

Prova

Generalizando para n fatores primos: $s(n) = \sum p_1^{h_1} \ldots p_r^{h_r}, 0 \leq h_i \leq k_i$ para $0 \leq i \leq r \Rightarrow s(n) = (1 + \cdots + p_1^{k_1}) \cdot (1 + \cdots + p_r^{k_r}) \Rightarrow s(n) = s(p_1^{k_1} \cdots p_r^{k_r} = s(p_1^{k_1}) \ldots s(p_r^{k_r}) \Rightarrow s(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \cdots \frac{p_r^{k_r+1}-1}{p_r-1}$

Observação: a Expressão acima permite concluir que $\sigma(n)$ é uma função aritmética multiplicativa, uma vez que, se a e b forem primos entre si $mdc(a,b) = 1$, então $\sigma(a.b) = \sigma(a) \cdot \sigma(b)$

Exemplo : $\sigma(12) = \sigma(4) \cdot \sigma(3) = (1+2+4) \cdot (1+3) = 7 \cdot 4 = 28$

1.1.4 Números perfeitos

Um inteiro positivo n é perfeito se e somente se é igual à soma de todos os seus divisores positivos, exceto o divisor n. A soma de todos os divisores positivos de n, com exceção do próprio n é igual a $\sigma(n) - n$, logo para números perfeitos
$\sigma(n) = 2n$ **Exemplo**: $n = 28$ $s(28) = 1+2+4+7+14+28 = 56 = 2 \cdot 28 = 2 \cdot n$

1.1.5 Exemplo 1: Olímpiada da Catalunha

Um número natural possui 2 fatores primos e 8 divisores positivos. Calcule este número sabendo que a soma de seus divisores é 320.

Solução $n = p^a.q^b \Rightarrow d(n) = (a+1)\cdot(b+1) = 8$ Sendo $a \geq 1$ e $b \geq 1$ a única possibilidade a menos de ordem é $a = 1$ e $b = 3 \Rightarrow n = p \cdot q^3$

$s(n) = (p+1)\cdot(q^3+q^2+q+1) = (p+1)\cdot(q+1)\cdot(q^2+1) = 2^6\cdot 5$ Testando p e q primos : $p = 7$ e $q = 3 \Rightarrow n = 7\cdot 3^3 = 189$

2 Função Número de Divisores $\tau(n)$ e técnicas de contagem

Seja n um inteiro. O número de divisores positivos de n (inclusive 1 e n) indica-se por $\tau(n)$.

Exemplo: $\tau(12) = 6$: Divisores : $\{1,2,3,4,6,12\}$

Se $n = p_1^{k_1}\cdots p_r^{k_r}$ é a decomposição de $n > 1$, então $\tau(n) = (k_1+1)\cdots(k_r+1)$

Prova: Se $n = p_1^{k_1}...p_r^{k_r}$ é a fatoração em primos de $n > 1$, então os divisores de n são da forma : $p_1^{h_1}...p_r^{h_r}$, onde $0 \leq h_i \leq k_i$ $i = 1,2,\ldots,r$

Logo para cada h_i temos k_i+1 possibilidades. Como para cada h_i escolhido está associado um divisor diferente pelo principío multiplicativo $\tau(n) = (k_1+1)...(k_r+1)$.

Exemplo $\tau(-12) = 2.\tau(12) = 2.\tau(2^2\cdot 3) = 2\cdot(2+1)\cdot(1+1) = 2\cdot 3\cdot 2 = 12$. Quando temos números negativos basta dobrar a quantidade de divisores, pois a cada divisor positivo equivale o seu simétrico.

2.1 Quadrados Perfeitos

Prove que n é um quadrado perfeito se e somente se $\tau(n)$ é ímpar.

Resolução

Se $n = p_1^{a_1}...p_k^{a_k}$ é a fatoração em primos de n, então como é um quadrado perfeito $\{a_1,...a_k\}$ são pares, logo $\tau(n) = (a_1+1)\cdots(a_k+1)$ é um produto de fatores ímpares que resulta em $\tau(n)$ ímpar. A recíproca como o número de divisores é impar , ela é formada por fatores ímpares, oriundos de expoentes pares que formam um quadrado perfeito.

2.1.1 Exemplo 2 : Belarus 1999

Sejam a,b inteiros positivos tais que o produto de todos os divisores positivos de a é igual ao produto de todos os divisores positivos de b. Prove que $a = b$

Lema $\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$.

Prova. Se $1 = d_1 < ... < d_k = n$ são os divisores positivos de n, então $\frac{n}{d_k} < ... < \frac{n}{d_1}$ também são. Logo $d_1\cdot d_k = ... = d_k\cdot d_1 = n$ e multiplicando essas igualdades :
$(d_1\cdots d_k)^2 = n^k = n^{\tau(n)}$. Segue o resultado $\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$:

Por hipótese temos que $a^{\tau(a)} = b^{\tau(b)}$. Como consequência, a e b tem os mesmos fatores primos, $p_1,...p_k$. Seja $a = p_1^{x_1}\cdots p_k^{x_k}$ e $b = p_1^{y_1}\cdots p_k^{y_k}$, para inteiros $x_1,\ldots,x_k$ e $y_1,\ldots,y_k$. Da igualdade $a^{\tau(a)} = b^{\tau(b)}$ tiramos $x_i\tau(a) = y_i\tau(b)$ para todo i. Sejam
$u = \frac{\tau(a)}{mdc(\tau(a),\tau(b))}$ e $v = \frac{\tau(b)}{mdc(\tau(a),\tau(b))}$ sendo $mdc(u,v) = 1$ e $ux_i = vy_i$. Deduzimos que $y_i = uz_i$

e $x_i = vz_i$ para alguns inteiros positivos z_i. Assim
$a = (p_1^{z_1} \cdots p_k^{z_k})^u$, $b = (p_1^{z_1} \cdots p_k^{z_k})^v$
Claramente se $u > v$, então:
$\tau(a) = (1+uz_1)\cdots(1+uz_k) > (1+vz_1)\cdots(1+xz_k) = \tau(b)$
e portanto $a^{\tau(a)} > b^{\tau(b)}$. Analogamente , não podemo ter $u < v$, logo $u = v$, $x_i = y_i$ para todo i e , finalmente, $a = b$.

3 Função de Euler ($\phi(n)$) e Congruências

A função aritmética de Euler ($\phi(n)$), é definida para todo inteiro positivo para os números que não superem n e sejam primos com ele .

Exemplo $\phi(10) = 4$. Os números menores que 10 e primo com ele são 1, 3, 7 e 9

3.1 Cálculo de $\phi(n)$

Teorema : Se $n = p_1^{k_1} \cdots p_r^{k_r}$ é a decomposição canônica do inteiro positivo $n > 1$, então:
$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})\cdots(p_r^{k_r} - p_r^{k_r-1}) = n\cdot(1-\frac{1}{p_1})...(1-\frac{1}{p_r})$

Prova:. Como $p_1,\ldots,p_r$ são primos, o mdc entre esses primos é 1. Como $\phi(n)$ é uma função aritmética multiplicativa

$$\phi(n) = \phi(p_1^{k_1}\cdots p_r^{k_r}) = \phi(p_1^{k_1})\cdots\phi(p_r^{k_r}) = (p_1^{k_1} - p_1^{k_1-1})\cdots(p_r^{k_r} - p_r^{k_r-1}) = n\cdot(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_r})$$

3.2 Teorema de Euler

Teorema Se n é um inteiro positivo e o $mdc(a,n) = 1$, então $a^{\phi(n)} \equiv 1\ (mod\ n)$

Demonstração

Sejam $a_1,...a_{\phi(n)}$ os números entre 1 e n primos com n. Temos que $a \cdot a_i$ é primo com n (nem a e nem a_i possui fatores comuns com n), onde $1xn$.
Suponha por absurdo, que x possui fatores comuns d com n então $a\cdot a_i \equiv x \pmod n$ e n divide $a\cdot a_i - x$, assim d divide $a\cdot a_i$ com um desses termos tendo fator comum a d. Absurdo pois são primos com n. Desta forma, x é primo com n e $1xn$, implicando $x = a_j$. Tomando os pares e multiplicando: $a^{\phi(n)}\cdot a_1\cdot a_\phi = a_{j_1}...a_{j_{\phi(n)}}$. Por fim devemos provar que $a_{j_m} \neq a_{j'_m}$, quando $m \neq m'$. Aqui supomos iguais e mostramos que $a\cdot a_m \equiv a\cdot a_{m'} \pmod n$ e chegamos na igualdade que implica na desigualdade. Assim $\{a_1,...,a_{\phi(n)}\} = \{a_{j_1},...,a_{j_{\phi(n)}}\}$ e $a^{\phi(n)}a_1...a_{\phi(n)} \equiv a_{j_1},...,a_{j_{\phi(n)}} \pmod n$ logo $a^{\phi(n)} \equiv 1 \pmod n$

3.2.1 Exemplo : Olímpiada da Rússia

Quais os possíveis resultados para os restos quando n^{100} é dividido por 125, quando n assume todos os valores inteiros positivos.

Solução: Se n for múltiplo de 5, 125 divide n^{100} e o resto é zero. Se $mdc(n,125) = 1$, temos $\phi(125) = 5^3\cdot(1-\frac{1}{5}) = 100$. Pelo Teorema de Euler, $n^{100} \equiv 1 \pmod n$. Assim o resto é 1.

4 Problemas para treinar

Questão 1
Determine todos os números naturais cuja soma dos divisores positivos é um número ímpar

Questão 2 - Putnam 1969 O inteiro positivo n é divisível por 24. Mostre que a soma de todos os divisores positivos de $n-1$ (incluindo 1 e $n-1$) também é divisível por 24.

Questão 3 - OBM - 1995 :
Quantos são os números inteiros que terminam com 1995 e que são múltiplos do número que se obtém quando estes últimos algarismos são eliminados ?

Questão 4 - China TST 2015 Para $n > 1$ defina
$f(n) = \tau(n!) - \tau((n-1)!)$
Prove que existem infinitos números compostos n tais que para todo $1 < m < n$ temos $f(m) < f(n)$

Questão 5 - China TST 1988 - IMO Defini-se $x_n = 3x_{n-1} + 2$ para todos os inteiros positivos n. Prove que um valor inteiro pode ser escolhido para x_0 tal que 1988 divide x_{100}:

Questão 6 - Komal A 240 Prove que , para todo $m, n \geq 1$,

$$\sum_{1 \leq k \leq n; mdc(k,m)=1} \frac{1}{k} \geq \frac{\phi(m)}{m} \sum_{k=1}^{n} \frac{1}{k}$$

5 Gabarito e Resolução

Questão 1 Seja n um número natural com s(n) ímpar. Escreva $n = 2^a.p$ com p ímpar e a um número não negativo. $\sigma(n) = (2^{a+1} - 1)\sigma(p)$ e $\sigma(p)$ deve ser ímpar Como p é impar, cada divisor de p deve ser ímpar e ele ter uma quantidade ímpar de divisores.

$d(p) = (k_1 + 1) \cdots (k_n + 1)$ para ser ímpar leva cada k_i a ser par

Logo p deve ser um quadrado perfeito, $p = m^2 \Rightarrow p = 2^b \cdot n^2$

Se a é par $n = (2^b \cdot m)^2$ Se a é ímpar $n = 2 \cdot (2^b \cdot m)^2$

Logo para que a soma dos divisores seja ímpar ou é um quadrado perfeito ou o dobro do quadrado de um número natural.

Questão 2

Seja $n = 24 \cdot m$. Se d é um divisor de $n - 1 = 24m - 1$, então $d^2 - 1$é divisível por 24. d não é múltiplo de 3 (n é) então deve dividir $d^2 - 1$. Além disso d deve ser ímpar (como $n - 1$) e $d - 1$ e $d + 1$ são pares consecutivos , com um deles múltiplo de 4 e seu produto $d^2 - 1$ múltiplo de 8.

Agora $24m - 1$ não pode ser quadrado perfeito, pois estes deixam resto 0 ou 1 na divisão por 4, e seus divisores vem em pares d, $\dfrac{24m-1}{d}$. Mas $d + \dfrac{24m-1}{d}$ é divisível por 24, pois $d^2 - 1$ e $24m$ são e nenhum fator de 24 pode dividir d. Portanto, a soma de todos os divisores de $n - 1$ é divisível por 24.

Questão 3

Seja $N = a_1 \ldots a_k 1995$, onde $a_1, \ldots, a_k$ representam os primeiros digitos de N. Escreva $N = A \cdot 10^4 + 1995$. Pelo enunciado $1995 = N - A \cdot 10^4$, como A divide N, então ele deve dividir 1995. Fatorando 1995, temos $1995 = 3 \cdot 5 \cdot 7 \cdot 19$. $\tau(1995) = 16$, que são os possíveis valores assumidos por A. Assim temos 16 números possíveis.

Questão 4

Testamos $n = 2p$ com $p > 2$ e primo. Vamos provar que todos eles satisfazem o problema. $f(2p) = \tau((2p)!) - \tau((2p-1)!)$. Como $(2p-1)!$ é divisível por p exatmente uma vez, então $(2p-1)! = px$, com x coprimo de p. $(2p)! = 2p^2x$

$f(2p) = \tau(2p^2x) - \tau(px) = \tau(p^2)\tau(2x) - \tau(p)\tau(x) > 3\tau(x) - 2\tau(x) = \tau(x)$, consequência de $\tau(2x) > \tau(x)$
Assim é suficiente mostrar que para cada $m \in \{2, 3, ..., 2p-1\}$ temos $f(m) \leq \tau(x)$. Sabemos $f(m) \leq \frac{\tau(m!)}{2} \leq \frac{\tau((2p-1)!)}{2} = \frac{\tau(px)}{2} = \tau(x)$, assim terminamos a prova.

Questão 5 $x_n = 3x_{n-1} + 2 \Rightarrow (x_n + 1) = 3 \cdot (x_{n-1} + 1)$. Isto é uma progressão geométrica de razão 3 e primeiro termo $x_0 + 1$
Logo $x_n = (x_0 + 1) \cdot 3^n - 1$. Portanto $x_{100} = (x_0 + 1) \cdot 3^{100} - 1$. De 1988 = $2^2 \cdot 7 \cdot 71$ e o fato dele ser primo com 3, o Teorema de Euler nos dá $\phi(1988) = 340$ e $3^{340} \equiv 1 \pmod{1988} \Rightarrow (3^{740}) \cdot (3^{100}) \equiv 1 \pmod{1988}$. Logo, fazendo $x_0 = 3^{740} - 1$ teremos x_{100} múltiplo de 1988.

Questão 6 Sejam $p_1, \ldots, p_s$ fatores primos de m sem contar as multiplicações.
$\prod_{i=1}^{s} \frac{1}{1 - \frac{1}{p_i}} \sum_{1 \leq k \leq n; mdc(k,m)=1} \frac{1}{k} \geq \sum_{k=1}^{n} \frac{1}{k}$ ou $\prod_{i=1}^{s} (1 + \frac{1}{p_1} + \frac{1}{p_i^2 + \ldots}) \sum_{1 \leq k \leq n; mdc(k,m)=1} \frac{1}{k} \geq \sum_{k=1}^{n} \frac{1}{k}$. Expandindo temos uma soma infinita, entre cujos termos temos todos $\frac{1}{p_1^{k_1} \cdots p_s^{k_s} \cdot r}$ com $k_i \geq 0$ e $1 \leq r \leq n$, $mdc(r, m) = 1$. Como qualquer número k entre 1 e n pode ser escrito como $k = p_1^{k_1} \cdots p_s^{k_s} \cdot r$ com k_i e r, como acima segue o resultado.