UNIVERSIDADE DE BRASÍLIA
DEPARTAMENTO DE MATEMÁTICA -IE

Brasília, setembro de 2004.

TEORIA DOS NÚMEROS

2º período de 2004

(Noturno)

Exercícios de treinamento

Observação: Os problemas que se seguem, marcados por * são tirados do livro de David M. Burton: Elementary Number Theory ©1980, 1976 by Allyn and Bacon, Inc., Boston.

1) Seja $S_n(m) = 1^m + 2^m + \ldots + n^m$, $(n \in \mathbb{N},\ m \in \mathbb{N}_0)$.

   a) Empreguem a nossa fórmula de recorrência

$$(m+1) \cdot S_n(m) = (n+1)^{m+1} - 1 - \sum_{k=0}^{m-1} \binom{m+1}{k} S_n(k)$$

   para determinar também $S_n(4)$ e $S_n(5)$.

   b) Verifiquem as fórmulas $S_n(4)$ e $S_n(5)$ obtidas em (a) também por indução sobre n.

*2) Verifiquem

$$1^2 + 3^2 + 5^2 + \ldots + (2n-1)^2 = \frac{n(4n^2-1)}{3}$$

para todo $n \in \mathbb{N}$.

3) Coloquemos $T_n(m) = 1^m + 3^m + 5^m + \ldots + (2n-1)^m$. Mostrar a fórmula de recorrência

$$2(m+1) \cdot T_n(m) = (2n+1)^{m+1} - 1 - 2^{m+1} \cdot \sum_{k=0}^{m-1} \binom{m+1}{k} \cdot 2^{-k} \cdot T_n(k).$$

Sugestão: Escrever $2x+1 = (2x-1)+2$ e desenvolver $\Big[(2x-1)+2\Big]^{m+1}$ pelo teorema binomial. Depois façam $x = 1, 2, \ldots, n$ e somem todas as n igualdades obtidas.

4) Determinar $T_n(0), T_n(1), T_n(2), T_n(3), \ldots$ pela fórmula de 3).

4') Mostrar diretamente: Para todos os $n \in I\!N$ e $m \in I\!N_0$ vale

$$T_n(m) = S_{2n}(m) - 2^m \cdot S_n(m) \ .$$

Determinar $T_n(0), T_n(1), T_n(2), T_n(3) \ , \ldots$ também por esta fórmula.

5) Verifiquem a identidade

$$x^n - 1 = (x-1)\left(1 + x + x^2 + \ \ \ldots \ \ + x^{n-1}\right)$$

onde n é um qualquer número natural, x é real.

6) Para todo x real e todo n natural *ímpar* vale:

$$x^n + 1 = (x+1)\left(1 - x + x^2 - x^3 \pm \ \ \ldots \ \ - x^{n-2} + x^{n-1}\right)$$

*7) Verifiquem

$$1 \cdot 2 + 2 \cdot 3 + \ \ \ldots \ \ + n(n+1) = \frac{n(n+1)(n+2)}{3}$$

para todo $n \in I\!N$

a) Por indução sobre n

b) Empregando-se as fórmulas $S_n(1)$ e $S_n(2)$.

*8) Dêem *exemplos que desprovem*

$$(mn)! = m!n! \quad \text{e} \quad (m+n)! = m! + n!$$

*9) Vale $n! > n^2$ para todo $n \geq 4$ e $n! > n^3$ para todo $n \geq 6$.

*10) Provar:

$$1 \cdot 1! \ + \ 2 \cdot 2! \ + \ 3 \cdot 3! \ + \ \ \ldots \ \ + \ n \cdot n! = (n+1)! - 1$$

para todo $n \in I\!N$.

*11) Provar: Para todo $n \geq 2$ vale

$$\binom{2}{2} + \binom{3}{2} + \ \ldots \ + \binom{n}{2} = \binom{n+1}{3}$$

(Comparar este resultado com 7)).

*12) Para todo $n \in I\!N$ provar o seguinte:

a) $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ \ldots \ + \binom{n}{n} = 2^n$.

Sugestão: Façam $a = b = 1$ no teorema binomial.

b) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - + \ \dots \ + (-1)^n\binom{n}{n} = 0$

c) $\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \ \dots \ + n\binom{n}{n} = n \cdot 2^{n-1}$

Sugestão: Expandir $n(1+b)^{n-1}$ pelo teorema binomial e colocar $b = 1$. Usem (e verifiquem) também a fórmula

$$n\binom{n-1}{k} = (k+1)\binom{n}{k+1}.$$

d) $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \ \dots \ = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \ \dots \ = 2^{n-1}$

e) $\binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \ \dots \ + 2^n\binom{n}{n} = 3^n$.

13) Admitindo que a fórmula para $S_n(2) = 1^2 + 2^2 + \ \dots \ + n^2$ deve ter a forma $S_n(2) = an^3 + bn^2 + cn + d$ com coeficientes a, b, c, d que independem de n, calcular os a, b, c, d, colocando-se $n = 1, 2, 3, 4$.

14) Mostrar: Para todo $n \in I\!N$, e todo k com $0 \le k \le n$,
os coeficientes binomiais $\binom{n}{k}$ *são números naturais*.

Sugestão: Indução sobre n; usem a fórmula $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$.

15) Mostrar: Para todo $k \in I\!N$, *o produto de quaisquer* k *números naturais consecutivos, é divisível por* $k!$.

*16) Mostrar: A soma de dois números triangulares consecutivos é um quadrado perfeito. Mais exatamente: $t_m + t_{m+1} = (m+1)^2$.

*17) Mostrar: Se $2n^2 \pm 1$ fôr um quadrado perfeito, digamos $2n^2 \pm 1 = m^2$, então $(nm)^2$ é um número triangular.

*18) Mostrar: Se n é um número triangular, então $9n+1$, $25n+3$ e $49n+6$ também são números triangulares (Euler 1775).
Mais exatamente: Se $n = t_m$, então $9t_m + 1 = t_{3m+1}$,
$25t_m + 3 = t_{5m+2}$ e $49t_m + 6 = t_{7m+3}$

19) Mostrar a seguinte generalização de 18):
Para todos os números $m, k \in I\!N$ vale:

$$(2k+1)^2 \cdot t_m + t_k = t_{(2k+1)m+k}$$

(Obs: 18) é obtido para $k = 1, 2, 3$).

20) Considera-se a sequência de LUCAS:

$$1, 3, 4, 7, 11, 18, 29, 47, 76\ , \ldots$$

definida por $a_1 = 1,\ a_2 = 3$ e $a_n = a_{n-1} + a_{n-2}$ para $n \geq 3$. Mostrar:

a) Para todo $n \geq 9$ vale a desigualdade

$$1,6180^n < a_n < 1,6181^n .$$

b) Para todo $n \geq 11$ vale a desigualdade

$$1,61803^n < a_n < 1,61804^n .$$

c) Admitindo-se que a seqüência $\left(\frac{a_n}{a_{n-1}}\right)_{n\in\mathbb{N}}$ converge, determinar

$$\lim_{n\to\infty} \frac{a_n}{a_{n-1}} \ .$$

21) Encontrar $r, q \in \mathbb{Z}$ de tal maneira que

$$-2347 = (-93)q + r \ \text{ com } \ 0 \leq r < 93 .$$

22) Sejam $a, b \in \mathbb{Z}$, $b \neq 0$ e seja n_0 um inteiro fixo. Mostrar a existência de *únicos* $q, r \in \mathbb{Z}$ *tais que*

$$a = bq + r \quad \text{e} \quad n_0 \leq r < n_0 + |b| .$$

23) Determinar (os únicos) $q, r \in \mathbb{Z}$ de tal maneira que

$$3100 = (-703)q + r \quad \text{e} \quad -512 \leq r < 191 .$$

24) Sejam $a, b \in \mathbb{Z}$, b ímpar. Existem únicos $q, r \in \mathbb{Z}$ tais que

$$a = bq + r \quad \text{e} \quad -\frac{|b|-1}{2} \leq r \leq \frac{|b|-1}{2} \ .$$

*25) Mostrar: Se um $n \in \mathbb{N}$ fôr simultâneamente um quadrado e um cubo, então n é da forma $7k + 1$ ou $7k$.

*26) Sejam $a \in \mathbb{Z}$, $n \in \mathbb{N}$. Mostrar: $\mathrm{mdc}(a, a+n) = \mathrm{mdc}(a, n)$.

*27) Sejam $0 \neq a, b, c \in \mathbb{Z}$. Mostrar:

a) Existem $x, y \in \mathbb{Z}$ tais que $ax + by = c$, se e somente se
$$\mathrm{mdc}(a, b) \,\big|\, c.$$

b) Se $x, y \in \mathbb{Z}$ são tais que $ax + by = \mathrm{mdc}(a, b)$, então
$$\mathrm{mdc}(x, y) = 1.$$

*28) Provar as seguintes afirmações:

a) Se $a \in \mathbb{Z}$ é ímpar, então $24 \,\big|\, a(a^2 - 1)$

b) Se $a, b \in \mathbb{Z}$ são ímpares, então $8 \,\big|\, (a^2 - b^2)$.

c) Se $a \in \mathbb{Z}$ não é divisível nem por 2 nem por 3, então $24 \,\big|\, (a^2 + 23)$.

Sugestão: Testar todas as possibilidades $a = 6k, 6k+1, \ldots, 6k+5$ com $k \in \mathbb{Z}$.

d) Para todo inteiro a vale: $360 \,\big|\, a^2(a^2 - 1)(a^2 - 4)$.

*29) Provar as seguintes propriedades do máximo divisor comum:

a) Se $\mathrm{mdc}(a, b) = 1$ e $\mathrm{mdc}(a, c) = 1$, então $\mathrm{mdc}(a, bc) = 1$.

b) Se $\mathrm{mdc}(a, b) = 1$ e $c \,\big|\, a$, então $\mathrm{mdc}(c, b) = 1$.

c) Se $\mathrm{mdc}(a, b) = 1$, então $\mathrm{mdc}(ac, b) = \mathrm{mdc}(c, b)$.

d) Se $\mathrm{mdc}(a, b) = 1$ e $c \,\big|\, a + b$, então $\mathrm{mdc}(a, c) = \mathrm{mdc}(b, c) = 1$.

*30) Encontrar $\mathrm{mdc}(143, 227)$, $\mathrm{mdc}(306, 657)$ e $\mathrm{mdc}(272, 1479)$
tal como $\mathrm{mmc}(143, 227)$, $\mathrm{mmc}(306, 657)$ e $\mathrm{mmc}(272, 1479)$.

*31) Usar o algoritmo Euclideano para se descobrir inteiros x, y tais que:

a) $\mathrm{mdc}(56, 72) = 56x + 72y$

b) $\mathrm{mdc}(24, 138) = 24x + 138y$

c) $\mathrm{mdc}(119, 272) = 119x + 272y$

d) $\mathrm{mdc}(1769, 2378) = 1769x + 2378y$

*32) Suponhamos $\mathrm{mdc}(a, b) = 1$. Mostrar o seguinte:

a) $\mathrm{mdc}(a + b, a - b) = 1$ ou 2

b) $\mathrm{mdc}(2a + b, a + 2b) = 1$ ou 3

c) $\mathrm{mdc}(a + b, a^2 + b^2) = 1$ ou 2

d) $\mathrm{mdc}(a + b, a^2 - ab + b^2) = 1$ ou 3.

*33) Mostrar: Para todos os $a, b, n \in I\!N$ valem

a) Se $\mathrm{mdc}(a,b) = 1$, então $\mathrm{mdc}(a^n, b^n) = 1$.

b) Se $a^n \big| b^n$, então $a \big| b$.

Sugestão: Seja $d = \mathrm{mdc}(a, b)$, $a = rd$, $b = sd$ com $\mathrm{mdc}(r, s) = 1$. Por a), $\mathrm{mdc}(r^n, s^n) = 1$. Mostrar $r = 1$ e daí $a = d$.

34) Determinar *todas as soluções* da equação DIOFANTina

$$84x - 49y = 91.$$

35) Determinar todas as *soluções positivas* da equação DIOFANTina

$$30x + 17y = 320$$

36) Um criador quer aplicar R\$ $2.000,00$ na *aquisição de bezerros* (R\$ $160,00$ cada) *e leitões* (R\$ $70,00$ cada). Quantos animais ele deve comprar?

37) *Decompor* os seguintes números n *em fatores primos*:

a) $n = 181\,429$ b) $n = 397\,703$ c) $n = 5\,609\,239$.

38) Mostrar: 2579 é um número primo.

39) Mostrar: $\big(2657, 2659\big)$ é um gêmeo de primos.

40) Mostrar: O único primo p da forma $n^5 - 1$ é $p = 31$.
O único primo p da forma $n^7 - 1$ é $p = 127$.
Não existe primo p da forma $n^{11} - 1$.

41) Sejam $2 < p \leq q$ números primos. Mostrar a equivalência das seguintes afirmações:

(i) $pq + 1$ é um quadrado perfeito

(ii) $\big(p, q\big)$ é um gêmeo de primos.

*42) Se $p \geq q \geq 5$ são dois primos, então $24 \big| p^2 - q^2$.

*43) Se $p \neq 5$ é um primo ímpar, então $p^2 - 1$ ou $p^2 + 1$ é divisível por 10.

44) Determinar a *decomposição primária* de $60!$.

*45) Mostrar: Se $n > 4$ é composto, então $n \big| (n-1)!$

*46) Para $n \geq 2$, todo inteiro da forma $n^4 + 4$ é composto.

47) Para $n \geq 2$, os números $n^4 + 4^n$ são compostos.

48) Mostrar: Um número $2 \leq n \in I\!N$ é um quadrado perfeito se e somente se na decomposição primária de n todos os expoentes são números pares.

49) Mostrar: Todo $n \in I\!N$ possui a forma $n = 2^k \cdot m$ onde $k \geq 0$ e m é um número ímpar.

49') Generalize 49): Seja $p \in I\!P$. Todo $n \in I\!N$ possui a forma $n = p^k \cdot m$ onde $k \geq 0$ e m é um número que não é divisível por p.

*50) Façam uma *tabela de todos os primos entre* 100 *e* 200.
Determinar $\pi(10k)$ para $k = 1, 2, \ldots, 20$.

51) Determinar $\pi(100k)$ por uma tabela de primos e *comparar*

$$\pi(100k) \quad \textit{com} \quad \frac{100k}{\ln 100k} \quad \textit{para} \quad k = 1, 2, \ldots, 20, \ldots .$$

*52) Sejam $p_1 = 2$, $p_2 = 3$, $p_3, \ldots, p_{25} = 97, \ldots, p_n, \ldots$ os primeiros n números primos. Mostrar:

$$N = p_1 \cdot p_2 \cdot \ \ldots \ \cdot p_n + 1 \ \textit{ jamais é um quadrado perfeito.}$$

52') Descubram, na seqüência $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $\ldots$ dos números primos, *o primeiro* p_k para o qual

$$N = p_1 \cdot p_2 \cdot \ \ldots \ \cdot p_k + 1 \ \textit{ não é primo.}$$

53) Mostrar: Para todo fator primo p de $n! + 1$ vale $p > n$. Usem este fato para mostrar a *infinitude do conjunto* $I\!P$ dos números primos.

54) Determinar a *decomposição primária de* $n! + 1$ para $1 \leq n \leq 12$.

55) Sejam $2 \leq a, n \in I\!N$. Mostrar:

a) Se $a^n - 1$ fôr primo, então $a = 2$ e n é primo (ver 40)).

b) Se $a^n + 1$ fôr primo, então n é uma potência de 2.

Sugestão para b): Escrever $n = 2^k \cdot m$ com m ímpar, $k \geq 0$.

56) Sejam $a, n, k \in I\!N$, $a \geq 2$. Mostrar:

$$a^k - 1 \ \textit{ divide } \ a^n - 1 \iff k \ \textit{ divide } \ n.$$

57) *Fatorar* os seguintes números n na forma

$$n = rs \quad \text{com} \quad 2 \le s \le r \le n-1:$$

a) $n = 2^{143} - 1$ b) $n = 6^{12} + 1$ c) $n = 2^{56} + 1$

58) Mostrar: Se $\big(p, p+2\big)$ é um gêmeo de primos com $p > 3$, então

a) 12 *divide* $p + (p+2)$ b) p é da forma $3k + 2$.

59) Mostrar: Para $n > 3$, um dos números $n, n+2, n+4$ é composto (divisível por 3).

*60) Se p e $p^2 + 8$ ambos são primos, então $p = 3$.

61) Seja $q = 2^{2n+1}$ com $n \in I\!N$. Mostrar: $(q^2+1)q^2(q-1)$ é divisível por 320 mas não por 60. Melhor: por $5 \cdot 4^{2n+1}$, mas não por 3.

*62) Mostrar: A função $f(n) = n^2 + n + 41$ assume valores primos para $n = 1, 2, \ldots, 39$. $f(40) = ?$, $f(41) = ?$

63) Escrever os seguintes números n como *diferença de dois quadrados* de todas as maneiras possíveis:

a) $n = 1997$ b) $n = 1991$

c) $n = 1729$ d) $n = 7735$

64) Escrever os números pares entre 100 e 200 como soma de dois primos. Escrever 120 como *soma de dois primos de todas as maneiras possíveis*.

*65) Mostrar:

a) Para todo $n \ge 2$ e p um primo, $\sqrt[n]{p}$ é irracional.

b) Se $a \in I\!N$ e $\sqrt[n]{a}$ é racional, então $\sqrt[n]{a}$ é inteiro.

c) Para $n \ge 2$, $\sqrt[n]{n}$ é irracional.

66) Mostrar: Se $\big(p, p+2\big)$ é um gêmeo de primos com $p > 3$, então p é da forma $p = 3k + 2$ $(k \in I\!N)$.

67) a) Se p é um primo e $p+1$ é um quadrado perfeito, então $p = 3$.

b) Se p é um primo e $p+1$ é um número triangular, então $p = 2$ ou $p = 5$.

c) Se p é primo e se $p + 1 = \dfrac{n(n+1)(2n+1)}{6}$, então $p = 13,\ 29$ ou 139.

67') Determinar todos os primos p para os quais

$$p + 253 \quad \text{é um número triangular .}$$

68) Mostrar: Para todo $n \in \mathbb{N}$ vale a fórmula

$$1 \cdot 3 \cdot 5 \cdot \ \ldots \ \cdot (2n-1) = \prod_{3 \le p \in \mathbb{P}} p^{b_p(n)}$$

onde $b_p(n) = \sum_{k=1}^{\infty} \left[\frac{2n-1+p^k}{2p^k}\right]$. Exemplo: $3 \cdot 5 \cdot 7 \cdot \ \ldots \ \cdot 71 = ?$

69) Descrever todos os pontos da circunferência unitária

$$x^2 + y^2 = 1$$

que têm suas duas *coordenadas racionais*.

70) Determinar *todos os triplos Pitagóricos primitivos* da forma

$$\big(120, \cdot\ , \ \cdot\ \big).$$

71) Seja p um primo ímpar. Determinem *todos os triplos Pitagóricos* da forma $\big(\ \cdot\ ,\ p^3\ ,\ \cdot\ \big)$.

*72) Pitágoras deu a seguinte fórmula para uma sequência infinita de triplos Pitagóricos primitivos:

$$\begin{aligned} x &= 2n^2 + 2n \\ y &= 2n + 1 \qquad\qquad (n \in \mathbb{N}) \\ z &= 2n^2 + 2n + 1 \end{aligned}$$

Como se enquadram estes triplos na nossa classificação completa dos triplos Pitagóricos? Comparar com 75).

*73) Seja $\big(x, y, z\big)$ um triplo Pitagórico primitivo. Mostrar: Exatamente um dos números ou x ou y é divisível por 3. xy é divisível por 12, xyz é divisível por 60.

*74) Triângulos Pitagóricos distintos podem ter a mesma área: Estudem os triplos $\big(20, 21, 29\big)$ e $\big(12, 35, 57\big)$.

*75) Determinem todos os triplos Pitagóricos primitivos $\big(x, y, x+1\big)$. Comparar com 72).

*76) Determinar todos os triplos Pitagóricos (necessariamente primitivos (porquê?)) da forma
$$\big(x, y, y+2\big) \;.$$

*77) a) Existem infinitos triplos Pitagóricos (necessariamente primitivos [porquê?]) da forma
$$\big(x, x+1, z\big) \;.$$
Sugestão: Se $\big(x, x+1, z\big)$ é um triplo Pitagórico, também $\big(3x+2z+1, 3x+2z+2, 4x+3z+2\big)$ é um.

b) Se $\big(x, x+1, z\big)$ é um triplo Pitagórico, então $\big(t_{2x}, t_{2x+1}, (2x+1)z\big)$ é um triplo Pitagórico. Logo existem infinitos triplos Pitagóricos nos quais x e y são números triangulares consecutivos.

*78) Se $\big(x, x+1, z\big)$ é um triplo Pitagórico, então, $\frac{u(u+1)}{2} = v^2$ onde $u = z - x - 1$, $v = x + \frac{1}{2}(1-z)$. Concluir daí que existem infinitos números triangulares que são também quadrados perfeitos.

79) Mostrar: Para $5 \le p < q < r$ primos e todos os $a, b, c \in I\!N$, o número $n = p^a \cdot q^b \cdot r^c$ é *deficiente*.

80) Mostrar: Os números das seguintes sequências são *abundantes*:

a) $2^k \cdot 5$ para todo $k \ge 2$.

b) $2^k \cdot 7$ para todo $k \ge 3$.

c) $2^k \cdot q$ para todo $k \ge \log_2(q+1)$. (q é um primo > 2).

d) $3^k \cdot 35$ para todo $k \ge 3$.

*81) Mostrar: *Todo número perfeito par é um número triangular*.

*82) Suponha que $n = 2^{k-1}(2^k - 1)$ seja perfeito. Mostrar: O produto dos divisores positivos de n é n^k. Em símbolos:
$$\prod_{d|n} d = n^k .$$

83) Se o número $n \ge 2$ é produto de primos de MERSENNE distintos, mostrar que $\sigma(n) = 2^k$ para algum k.
Exemplo: $n = 3 \cdot 7 \cdot 31$; $\sigma(n) = 4 \cdot 8 \cdot 32 = 2^{10}$.

84) Seja $2 \le m \in I\!N$.
Dar *exemplos de infinitos números* $n \in I\!N$ tais que $\tau(n) = m$.

85) Classificar todos os números $n \in \mathbb{N}$ para os quais $\tau(n)$ é:

a) um primo q b) o produto de dois primos qr $(q \leq r)$.

86) Seja $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}$ com primos distintos $p_1, \ldots, p_r$, $a_1, \ldots, a_r \in \mathbb{N}$. Mostrar a equivalência das afirmações:

a) $\tau(n) = 2^s$ para algum s.

b) Todos os expoentes $a_1, \ldots, a_r$ são números de MERSENNE.

87) Mostrar: Para todo $n \in \mathbb{N}$ vale:

$$\prod_{d|n} \frac{n}{d} = \prod_{d|n} d$$

tal como
$$\sum_{d|n} \frac{n}{d} = \sum_{d|n} d.$$

*88) Mostrar: Se $n \in \mathbb{N}$ é perfeito, então $\sum_{d|n} \frac{1}{d} = 2$.

DEFINIÇÃO: Dois números $m, n \in \mathbb{N}$ são ditos **amigáveis**, se $\sigma(m) = m + n = \sigma(n)$.

89) Seja $n \in \mathbb{N}$. Mostrar:

n é perfeito, se e somente se n é amigável com si mesmo.

*90) Mostrar que os seguintes pares de números são amigáveis:

a) 220 e 284 (PITÁGORAS)

b) 17 296 e 18 416 (FERMAT 1636)

c) $9\,363\,584 = 2^7 \cdot 191 \cdot 383$ e $9\,437\,056 = 2^7 \cdot 73\,727$ (DESCARTES 1638)

*91) Suponha que $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$ e $r = 9 \cdot 2^{2n-1} - 1$ sejam todos primos $(n \geq 2)$. Mostrar que $2^n pq$ e $2^n r$ formam um par de números amigáveis. Quais são os pares obtidos para $n = 2$, $n = 4$ e $n = 7$?

*92) Se m e n são números amigáveis, mostrar que

$$\frac{1}{\sum_{d|m} \frac{1}{d}} + \frac{1}{\sum_{d|n} \frac{1}{d}} = 1$$

*93) Para todo $n \in \mathbb{N}$, a **média harmônica** $H(n)$ dos divisores de n é definida como sendo

$$\frac{1}{H(n)} = \frac{1}{\tau(n)} \cdot \sum_{d|n} \frac{1}{d}\,. \qquad \text{Mostrar:}$$

a) $H(n) = n \cdot \tau(n)/\sigma(n)$.

b) Se $\mathrm{mdc}(m, n) = 1$, então $H(mn) = H(m)H(n)$

c) Se n fôr um número perfeito, então $H(n)$ é um inteiro.

*94) Mostrar: Para todo $n \in \mathbb{N}$ vale $\prod_{d|n} d = n^{\tau(n)/2}$.

*95) Um $n \in \mathbb{N}$ é dito **multiplicativamente perfeito,** se

$$n^2 = \prod_{d|n} d.$$

Classificar todos os números que são multiplicativamente perfeitos.

96) Sejam $b_1, \ldots, b_n$ n números tais que $b_i \not\equiv b_j \mod n$ para todo $1 \le i \ne j \le n$. Então $\{b_1, \ldots, b_n\}$ é um sistema completo de resíduos $\mod n$.

97) Seja $\{a_0, a_1, \ldots, a_{n-1}\}$ um sistema completo de resíduos $\mod n$ e seja $b \in \mathbb{Z}$ com $\mathrm{mdc}(b, n) = 1$. Mostrar: $\{ba_0, ba_1, \ldots, ba_{n-1}\}$ também é um sistema completo de resíduos $\mod n$.

98) Seja $\mathrm{mdc}(a, n) = 1$ $(n \in \mathbb{N},\ a \in \mathbb{Z})$. Mostrar: Para qualquer $c \in \mathbb{Z}$, os números

$$c,\ c + a,\ c + 2a,\ c + 3a, \ldots,\ c + (n-1)a$$

formam um sistema completo de resíduos $\mod n$.

99) Quaisquer n números consecutivos formam um sistema completo de resíduos $\mod n$.

100) O produto de quaisquer n números consecutivos é divisível por n.

Observação: A afirmação de 100) é fraca. Comparar isso com o resultado bem mais forte que já vimos em 15) onde se afirma que até $n!$ divide tal produto!

101) Mostrar: $\{-76, 2, 2^2, 2^3, \ldots, 2^{18}\}$ é um sistema completo de resíduos $\mod 19$.

102) Mostrar as seguintes *relações de divisibilidade*:

a) $2 \cdot 251 + 1 = 503 \,\big|\, M_{251} = 2^{251} - 1$ tal como
$216 \cdot 251 + 1 = 54217 \,\big|\, M_{251}$.

b) $17 \,\big|\, M_{89} + 2 = 2^{89} + 1$

c) $479 \,\big|\, M_{239}$

d) $83 \,\big|\, M_{41} + 2$

103) *Decompor em fatores primos* os seguintes números:

a) M_{48}

b) M_{22}

c) $M_{13} + 2$

d) $(M_{17})^2 - 4$

104) *Decompor em fatores primos* os seguintes números:

a) $n = 111$ b) $n = 1111$

c) $n = 11111$ d) $n = 111111$

e) $n = 1111111$ f) $n = 11111111$

*105) Para quem dispuser de uma calculadora de pelo menos 9 dígitos, mostrar

$$2 \cdot 1445580 \cdot 67 + 1 = 193707721 \,\big|\, M_{67} \qquad (\text{F. N. Cole}, 1903).$$

*106) Se $x \equiv a \mod n$, provar que

$$x \equiv a \mod 2n \text{ ou } x \equiv a + n \mod 2n\,.$$

*107) Explique a seguinte curiosidade:

$$\begin{array}{rcccl}
1 \cdot 9 & + & 2 & = & 11 \\
12 \cdot 9 & + & 3 & = & 111 \\
123 \cdot 9 & + & 4 & = & 1111 \\
1234 \cdot 9 & + & 5 & = & 11111 \\
12345 \cdot 9 & + & 6 & = & 111111 \\
123456 \cdot 9 & + & 7 & = & 1111111 \\
1234567 \cdot 9 & + & 8 & = & 11111111 \\
12345678 \cdot 9 & + & 9 & = & 111111111 \\
123456789 \cdot 9 & + & 10 & = & 1111111111
\end{array}$$

Sugestão: Provar a fórmula

$$(10^{n-1} + 2 \cdot 10^{n-2} + 3 \cdot 10^{n-3} + \ \ldots \ + (n-1) \cdot 10 + n)(10 - 1) + (n+1) = (10^{n+1} - 1)/9\,.$$

108) Determinar os *últimos quatro dígitos* de

$$1! + 2! + 3! + \ \ldots \ + n! \qquad \text{para}$$

a) $n \geq 19$ b) $n = 17$ c) $n = 11$.

109) Qual é o resto r $(0 \leq r \leq 196)$ quando 51^{125} é dividido por 197?

*110) Mostrar: Se $a \equiv b \mod n_1$ e $a \equiv b \mod n_2$, então

$$a \equiv b \mod m \ \text{ onde } \ m = \mathrm{mmc}(n_1, n_2).$$

Se $\mathrm{mdc}(n_1, n_2) = 1$, então $a \equiv b \mod n_1 n_2$.

*111) Se $a \equiv b \mod n_1$ e $a \equiv c \mod n_2$, então $b \equiv c \mod d$ onde $d = \mathrm{mdc}(n_1, n_2)$.

*112) Se $a \equiv b \mod n$, mostrar que $\mathrm{mdc}(a, n) = \mathrm{mdc}(b, n)$.

*113) Um número de MERSENNE $M_n = 2^n - 1$ $(n \geq 2)$ jamais é um quadrado perfeito.

114) Resolver as congruências:

a) $5x \equiv 2 \mod 26$ b) $36x \equiv 8 \mod 102$

c) $34x \equiv 60 \mod 98$ d) $140x \equiv 133 \mod 301$

115) Resolver o sistema de *congruências simultâneas*:

$$x \equiv 3 \mod 19, \quad x \equiv 5 \mod 18, \quad x \equiv 12 \mod 17.$$

*116) Quando se remove ovos de um cesto, 2, 3, 4, 5, 6 de uma vez, sobram respectivamente, 1, 2, 3, 4, 5 ovos. Removendo-os em 7 de uma vez, nenhum sobra. *Quantos ovos (no mínimo) encontram-se no cesto*?

117) Um certo inteiro ≤ 3000 deixa os restos 4, 5, 1, 7 quando dividido, respectivamente, por 5, 7, 8, 9. *Determinar este inteiro*.

*118) Resolver a congruência $23x \equiv 37 \mod 1386$, tendo em vista que $1386 = 9 \cdot 11 \cdot 14$. Logo, a congruência é equivalente às 3 congruências

$$23x \equiv 37 \mod 9, \quad 23x \equiv 37 \mod 11, \quad 23x \equiv 37 \mod 14.$$

*119) Mostrar as seguintes afirmações:

a) Se $a \equiv b \mod n$ e $m \big| n$, então $a \equiv b \mod m$.

b) Se $a \equiv b \mod n$ e $c > 0$, então $ca \equiv cb \mod cn$.

c) Se $a \equiv b \mod n$ e se d divide todos os a, b, n, então

$$\frac{a}{d} \equiv \frac{b}{d} \mod \frac{n}{d}.$$

*120) Seja $a \in I\!N$. Mostrar:

a) a^2 termina em 0,1,4,5,6 ou 9.

b) a^3 pode terminar em qualquer um dos dígitos $0, 1, \ldots, 9$.

c) a^4 termina em 0,1,5 ou 6

d) um número triangular termina em 0,1,3,5,6 ou 8.

*121) Seja $a \in I\!N$. Mostrar:

a) Se a é ímpar, então $a^2 \equiv 1 \mod 8$

b) Sempre $a^3 \equiv 0, 1$ ou $8 \mod 9$

c) Sempre $a^3 \equiv a \mod 6$

d) Se $2 \dagger a$ e $3 \dagger a$, então $a^2 \equiv 1 \mod 24$

e) Se a é tanto um quadrado quanto um cubo perfeitos, então $a \equiv 0, 1, 9$ ou $28 \mod 36$.

*122) Provar por indução: Para todo a ímpar vale a congruência

$$a^{2^n} \equiv 1 \mod 2^{n+2} \qquad (n \in I\!N).$$

123) Seja $p = 23$, $a = -6$. Mostrar: Os números

$$(-6) \cdot 1, (-6) \cdot 2, \ldots, (-6) \cdot 21, (-6) \cdot 22$$

são, em alguma ordem, congruentes $\mod 23$ aos números $1, 2, \ldots, 22$.

124) Seja $p = 29$. Escrever o conjunto $\{2, 3, \ldots, 27\}$ na forma $\{a_1, b_1, a_2, b_2, \ldots, a_{13}, b_{13}\}$ com $a_i b_i \equiv 1 \mod 29$ $(1 \leq i \leq 13)$.

125) Determinar os restos quadráticos e os restos não-quadráticos $\mod p$ para todos os primos $3 \leq p \leq 31$.

126) Seja $p = 17$, $a = 14$. Escrever o conjunto $\{1, 2, \ldots, 16\}$ como $\{c_1, c_1', c_2, c_2', \ldots, c_8, c_8'\}$ tal que $c_i c_i' \equiv 14 \mod 17$ para todo $i = 1, 2, \ldots, 8$.

127) Resolver todas as congruências $x^2 \equiv -1 \mod p$ para os primos $p \equiv 1 \mod 4$ $(100 \leq p \leq 200)$.

*128) Mostrar as seguintes congruências para todo $a \in \mathbb{Z}$:

i) $a^{21} \equiv a \mod 15$

ii) $a^7 \equiv a \mod 42$

iii) $a^{13} \equiv a \mod 3 \cdot 7 \cdot 13$

*129) Para todo $a \in \mathbb{Z}$, mostrar que a^5 e a *têm o mesmo dígito final.*

*130) Sejam $a, b \in \mathbb{Z}$ não divisíveis pelo primo p. Mostrar:

a) Se $a^p \equiv b^p \mod p$, então $a \equiv b \mod p$.

b) Se $a^p \equiv b^p \mod p$, então $a^p \equiv b^p \mod p^2$.

*131) Para p um primo ímpar, mostrar o seguinte:

a) $1^{p-1} + 2^{p-1} + 3^{p-1} + \ \dots \ + (p-1)^{p-1} \equiv -1 \mod p$

b) $1^p + 2^p + 3^p + \ \dots \ + (p-1)^p \equiv 0 \mod p$

*132) Seja p um primo ímpar, $1 \leq k \leq p-1$. Então o coeficiente binomial

$$\binom{p-1}{k} \equiv (-1)^k \mod p.$$

133) Qual é o resto de divisão de 27! por 29? Em geral:
Seja p um primo ímpar $(p-2)! \equiv \ ? \mod p$.

134) Para todo primo $p > 2$ vale: $2 \cdot (p-3)! \equiv -1 \mod p$.
Exemplo: Qual é o resto de divisão de $2 \cdot 38!$ por 41?

135) Mostrar: $n > 1$ é primo, se e somente se $(n-2)! \equiv 1 \mod n$.

*136) Para todo primo ímpar p vale:

$$1^2 \cdot 3^2 \cdot 5^2 \cdot \ \dots \ \cdot (p-2)^2 \equiv \big(-1\big)^{(p+1)/2} \mod p.$$

*137) Para todo primo $p \equiv 3 \mod 4$ vale:

$$\text{ou} \quad \Big(\frac{p-1}{2}\Big)! \equiv 1 \qquad \text{ou} \quad \Big(\frac{p-1}{2}\Big)! \equiv -1 \mod p.$$

*138) Seja $p \equiv 3 \mod 4$ um primo, $a, b \in \mathbb{Z}$. Mostrar:
$a^2 + b^2 \equiv 0 \mod p$ implica em $a \equiv b \equiv 0 \mod p$.

139) Mostrar: M_{131} não é primo; M_{3023} não é primo.

*140) Seja p um primo, $a \in \mathbb{Z}$, $p \dagger a$. Mostrar: $x \equiv a^{p-2} \cdot b$ é uma solução da congruência $ax \equiv b \mod p$

*141) Sejam p, q dois primos distintos. Mostrar:

$$p^{q-1} + q^{p-1} \equiv 1 \mod pq$$

*142) Sejam p, q dois primos distintos, $a \in \mathbb{Z}$ tal que $a^p \equiv a \mod q$ e $a^q \equiv a \mod p$. Mostrar que

$$a^{pq} \equiv a \mod pq .$$

*143) Seja p um primo, $a, b \in \mathbb{Z}$ tais que $p \dagger a$ e $p \dagger b$.
Mostrar: Das três congruências

$$x^2 \equiv a \mod p, \quad x^2 \equiv b \mod p, \quad x^2 \equiv ab \mod p$$

ou exatamente uma ou todas as três são solúveis.

144) Seja p um primo. Se ambos $a, b \in \mathbb{Z}$ são restos quadráticos (não-quadráticos) $\mod p$, mostrar que ab é um resto quadrático $\mod p$. Se um dos dois é resto quadrático, o outro é resto não-quadrático $\mod p$, mostrar que ab é resto não-quadrático $\mod p$.

145) Seja $p = 19$, $a = -87$. Determinar $t_1, t_2, \ldots, t_9$ $(1 \leq t_k \leq 18)$ tais que $t_k \equiv (-87)k \mod 19$ $(k = 1, 2, \ldots, 9)$.
Escrever $\{t_1, \ldots, t_9\}$ na forma

$$\{r_1, \ldots, r_m, 19 - s_1, \ldots, 19 - s_n\} = \{1, 2, \ldots, 9\} .$$

Qual é a paridade de n ? -87 é um quadrado ou um não-quadrado $\mod 19$?

146) Completar a seguinte tabela:

q	$n = \frac{q-1}{2}$	$n \equiv ? \mod 4$	**Observação**
5	2	2	$5 \mid M_2 + 2$
7	3	3	$7 \mid M_3$
11	5	1	$11 \mid M_5 + 2$
13	6	2	$13 \mid M_6 + 2$
17	8	0	$17 \mid M_8$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
59	29	1	$59 \mid M_{29} + 2$
61	30	2	$61 \mid M_{30} + 2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
97	48	0	$97 \mid M_{48}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

147) Resolver as congruências quadráticas

a) $x^2 - 33x + 24 \equiv 0 \mod 41$ b) $x^2 - 205x + 406 \equiv 0 \mod 547$

148) Resolver a congruência cúbica

$$x^3 - 190x^2 + 188x - 147 \equiv 0 \mod 211 .$$

149) Seja $p = 4679$. Mostrar que p é primo. Qual é o valor dos símbolos de LEGENDRE $\left(\frac{a}{p}\right)$ quando $-630 \le a \le -620$?

150) Façam uma tabela dos números primos $p \le 200$ que são

a) $\equiv \pm 1 \mod 8$ e resolvam as congruências $x^2 \equiv 2 \mod p$.

b) $\equiv 1$ ou $3 \mod 8$ e resolvam as congruências $x^2 \equiv -2 \mod p$.

c) $\equiv \pm 1 \mod 12$ e resolvam as congruências $x^2 \equiv 3 \mod p$.

d) $\equiv \pm 1 \mod 10$ e resolvam as congruências $x^2 \equiv 5 \mod p$.

151) Mostrar:

a) $\left(\frac{11}{p}\right) = +1$ se e somente se $p = \pm 1,\ \pm 5,\ \pm 9,\ \pm 25,\ \pm 37 \mod 44$.

b) $\left(\frac{17}{p}\right) = +1$ se e somente se $p = \pm 1,\ \pm 9,\ \pm 13,\ \pm 15 \mod 34$.

152) a) Quais são os menores primos p que são congruentes $\mod 44$ com $\pm 1,\ \pm 5,\ \pm 9,\ \pm 25,\ \pm 37$? Resolver as congruências $x^2 \equiv 11 \mod p$ para estes valores de p.

b) Quais são os menores primos que são congruentes $\mod 34$ com $\pm 1,\ \pm 9,\ \pm 13,\ \pm 15$? Resolver as congruências $x^2 \equiv 17 \mod p$ para estes valores de p.

153) Estabeleçam *condições necessárias e suficientes sobre* p para que se tenha

a) $\left(\frac{13}{p}\right) = +1$ b) $\left(\frac{19}{p}\right) = +1$ c) $\left(\frac{15}{p}\right) = +1$

d) $\left(\frac{10}{p}\right) = +1$ e) $\left(\frac{14}{p}\right) = +1$ f) $\left(\frac{21}{p}\right) = +1$.

154) Mostrar: Se $p, p+2$ são primos gêmeos, então

$$\left(\frac{p}{p+2}\right) = \left(\frac{p+2}{p}\right) = \big(-1\big)^{\frac{p^2-1}{8}} .$$

155) Sejam p e $p+8$ ambos primos. Mostrar:

$$\left(\frac{p}{p+8}\right) = \big(-1\big)^{(p^2+4p-5)/8}\ .$$

156) Estabeleçam regras sobre:

a) $\left(\frac{-3}{p}\right)$ b) $\left(\frac{-5}{p}\right)$

c) $\left(\frac{-6}{p}\right)$ d) $\left(\frac{-7}{p}\right)$.

157) Mostrar que os seguintes números p são primos $\equiv 1 \mod 4$. Escrevam-nos como *soma de dois quadrados*:

a) $p = 977$ b) $p = 2\,593$.

158) Escrever o número $n = 205\,193$ como *soma de dois quadrados de duas maneiras essencialmente distintas*.

159) Escrever os números n da forma

$$n = 4^k(8m+7) \quad (7 \le n \le 200;\ k, m \in I\!N_0\ )$$

como *soma de* 4 *quadrados*.

160) Escrever os números $n \le 100$ como *soma de quadrados com um número mínimo de somandos*.

161) Calcular: $\varphi(1\,001)$, $\varphi(5\,040)$, $\varphi(36\,000)$ e $\varphi(3^{28}-1)$.

*162) a) Se n é ímpar, então $\varphi(2n) = \varphi(n)$.

b) Se n é par, então $\varphi(2n) = 2\cdot\varphi(n)$.

c) $\varphi(3n) = 3\cdot\varphi(n)$, se e somente se $3\,\big|\,n$.

d) $\varphi(3n) = 2\cdot\varphi(n)$, se e somente se $3\dagger n$.

e) $\varphi(n) = n/2$ se e somente se $n = 2^k$ para algum $k \ge 1$.

163) Seja p um primo e $k \in I\!N$. Mostrar:

$$\varphi(p^k) \quad \text{é} \quad \tfrac{p-1}{p}\cdot 100\% \quad \text{de} \quad p^k\ .$$

Particularmente: $\varphi(2^k) = 50\%$ de 2^k e $\varphi(5^k)$ é 80% de 5^k.

*164) Se p e $2p-1$ são ambos primos, então, para $n = 2(2p-1)$ será satisfeito $\varphi(n) = \varphi(n+2)$.

165) Mostrar: se n possui r fatores primos distintos ímpares, então $2^r \,\big|\, \varphi(n)$.

*166) a) Se p e $p+2$ são primos gêmeos, então $\varphi(p+2) = \varphi(p) + 2$.

b) Se p e $2p+1$ são ambos primos, então $n = 4p$ satisfaz
$$\varphi(n+2) = \varphi(n) + 2.$$

*167) Suponhamos que todo primo que divide n também divide m.
Mostrar que
$$\varphi(nm) = n \cdot \varphi(m) \ ,$$
particularmente, $\varphi(n^2) = n \cdot \varphi(n)$ para todo $n \in I\!N$.

*168) Se $\varphi(n) \,\big|\, n-1$, mostrar que $n = p_1 \cdot p_2 \cdot \ \ldots \ \cdot p_r$ com primos distintos $p_1 \ , \ldots , \ p_r$, i. e. n é um número livre de quadrados.

*169) Mostrar: Se $d \,\big|\, n$ então $\varphi(d) \,\big|\, \varphi(n)$.

170) Encontrar as soluções das equações $\varphi(n) = 16$ e $\varphi(n) = 24$.

*171) Se p é primo e $2p+1$ é composto, então a equação $\varphi(n) = 2p$ não admite solução.
Mostrar que $\varphi(n) = 14$ não tem solução e 14 é o menor número natural par com esta propriedade.

*172) Se p é um primo e $k \geq 2$, mostrar $\varphi\left(\varphi(p^k)\right) = p^{k-2}(p-1) \cdot \varphi(p-1)$.

*173) Sejam $n \in I\!N$, $a \in Z\!\!\!Z$ tal que $\mathrm{mdc}(n,a) = \mathrm{mdc}(n, a-1) = 1$.
Mostrar:
$$1 + a + a^2 + \ \ldots \ + a^{\varphi(n)-1} \equiv 0 \mod n.$$

*174) Se $m, n \in Z\!\!\!Z$ são primos entre si, mostrar que
$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \mod mn.$$

*175) Se $\mathrm{mdc}(a,n) = 1$, mostrar que a congruência $ax \equiv b \mod n$ possui a solução $x = b \cdot a^{\varphi(n)-1} \mod n$. Resolver as congruências
$3x \equiv 5 \mod 26$, $13x \equiv 2 \mod 40$ e $10x \equiv 21 \mod 49$.

176) Mostrar: Os inteiros $-31, \ -16, \ -8, \ 13, \ 25, \ 80$ formam um sistema reduzido de restos $\mod 9$. Os inteiros $3, \ 3^2, \ 3^3, \ 3^4, \ 3^5, \ 3^6$ formam um sistema reduzido de restos $\mod 14$.

177) Façam uma tabela para $\mathbf{o}_n(a)$ quando $1 \leq n \leq 20$, $\mathrm{mdc}(a,n) = 1$.

178) Determinar $\mathbf{o}_n(2)$ para todos os $n \equiv 1 \mod 2, \quad 1 \leq n \leq 30$.

179) Determinar as ordens $\mathbf{o}_p(2),\ \mathbf{o}_p(3),\ \mathbf{o}_p(5)$ para todo primo $p \leq 100$ para o qual o símbolo está definido.

180) Quais são os números $n, \quad 1 \leq n \leq 100,$ para os quais *existe uma raíz primitiva* $\mod n$.

181) Determinar *as menores raízes primitivas* $r \mod p$ e a quantidade das raízes primitivas incongruentes $\mod p$ quando p é um primo ≤ 100.

*182) Mostrar: $\varphi(2^n - 1)$ é múltiplo de n para todo $n \geq 1$.
Sugestão: Qual é a ordem de $2 \mod 2^n - 1$?

*183) a) Se $\mathbf{o}_n(a) = hk,$ então $\mathbf{o}_n(a^h) = k$.
b) Se $\mathbf{o}_p(a) = 2k,$ então $a^k \equiv -1 \mod p$; p é um primo ímpar.
c) Se $\mathbf{o}_n(a) = n - 1,$ então n é um primo.

184) Mostrar (por indução):

a) Para todo $k \geq 3$ temos

$$5^{2^{k-3}} \equiv 1 + 2^{k-1} \not\equiv 1 \mod 2^k .$$

b) Para todo $k \geq 4$ temos

$$5^{2^{k-3}} \equiv 3^{2^{k-3}} \equiv 1 + 2^{k-1} \not\equiv 1 \mod 2^k .$$

c) Para todo $k \geq 3$ temos

$$\mathbf{o}_{2^k}(3) = \mathbf{o}_{2^k}(5) = 2^{k-2} .$$

Lembrar que $a^{2^{k-2}} = a^{\frac{\varphi(2^k)}{2}} \equiv 1 \mod 2^k$ para todo $k \geq 3$ e todo a ímpar. Comparar com *122). Logo,

$$\mathbf{o}_{2^k}(3) = \mathbf{o}_{2^k}(5) = \frac{\varphi(2^k)}{2} \text{ para todo } k \geq 3 .$$

Como não existe raíz primitiva modulo 2^k, isto significa que 3 e 5 possuem modulo 2^k as máximas ordens possíveis.