Terceira Lista de Preparação para a LVIII IMO
e XXVII Olimpíada Iberoamericana de Matemática
Nível III
Soluções

Prazo: 17/03/2017, 23:59 de Brasília

Álgebra

PROBLEMA 1

Defina a sequência $a_1, a_2, \ldots$ a partir de suas somas parciais $S_n = a_1 + a_2 + \cdots + a_n$ da seguinte forma:

$$S_1 = 1, \quad S_n = \frac{(2+S_{n-1})^2}{4+S_{n-1}}, \quad n \geq 2.$$

Prove que $a_n \geq \frac{4}{\sqrt{9n+7}}$ para todo n inteiro positivo.

Solução

Primeiro, veja que

$$S_n - S_{n-1} = \frac{4}{4+S_{n-1}} \iff a_n = \frac{4}{4+S_{n-1}} \iff S_{n-1} = \frac{4}{a_n} - 4 \iff a_n = \frac{4}{a_1 + \cdots + a_{n-1} + 4}.$$

Provaremos a desigualdade por indução. Para $n = 1$, temos $a_1 = S_1 = 1 = \frac{4}{\sqrt{9 \cdot 1 + 7}}$. O passo dá certo quando

$$S_{n-1} \leq \sqrt{9n+7} - 4.$$

Agora vamos provar, também por indução, que

$$S_n \leq \sqrt{9n+16} - 4.$$

Mas isso equivale a

$$S_{n-1} + 4 + \frac{4}{S_{n-1}+4} \leq \sqrt{9n+16}.$$

A função $f(x) = x + \frac{4}{x}$, para $x > 0$, atinge seu mínimo para $x = 2$, já que $f(x) \geq 2\sqrt{x \cdot \frac{4}{x}} = 4$ com igualdade para $x = 4/x \iff x = 2$. Além disso, para $x > y > 2$, $xy > 4 \iff 1 - 4/xy > 0$ e

$$f(x) - f(y) = x - y + \frac{4}{x} - \frac{4}{y} = (x-y)\left(1 - \frac{4}{xy}\right) > 0,$$

ou seja, f é crescente em $(2, \infty)$.

Assim, como indutivamente $S_n > 0$, $2 < S_{n-1} + 4 \leq \sqrt{9n+7}$, de modo que

$$S_{n-1} + 4 + \frac{4}{S_{n-1}+4} \leq \sqrt{9n+7} + \frac{4}{\sqrt{9n+7}}.$$

Logo basta que

$$\sqrt{9n+7} + \frac{4}{\sqrt{9n+7}} \leq \sqrt{9n+16} \iff \frac{4}{\sqrt{9n+7}} \leq \sqrt{9n+16} - \sqrt{9n+7} = \frac{9}{\sqrt{9n+7} + \sqrt{9n+16}}$$
$$\iff 4\sqrt{9n+16} \leq 5\sqrt{9n+7} \iff 16(9n+16) \leq 25(9n+7) \iff n \geq 1,$$

que é verdade, o que completa a demonstração.

PROBLEMA 2

O polinômio $x^3 - 21x + 35$ tem três raízes reais distintas r, s, t. Encontre um polinômio $P(x) = x^2 + ax + b$ tal que $P(r) = s$, $P(s) = t$ e $P(t) = r$.

Solução
Resposta: $P(x) = x^2 + 2x - 14$.

Temos

$$\left|\begin{aligned} &s = r^2 + ar + b \\ &t = s^2 + as + b \\ &r = t^2 + at + b \end{aligned}\right. \implies \left|\begin{aligned} &rs = r^3 + ar^2 + br \\ &st = s^3 + as^2 + bs \\ &rt = t^3 + at^2 + bt \end{aligned}\right. \implies rs + st + rt = r^3 + s^3 + t^3 + a(r^2 + s^2 + t^2) + b(r + s + t).$$

Temos $rs + st + rt = -21$, $r + s + t = 0$, $r^2 + s^2 + t^2 = (r + s + t)^2 - 2(rs + st + rt) = 42$, e sendo r, s, t raízes de $x^3 - 21x + 35 = 0$,

$$\left|\begin{aligned} &r^3 = 21r - 35 \\ &s^3 = 21s - 35 \\ &t^3 = 21t - 35 \end{aligned}\right. \implies r^3 + s^3 + t^3 = 21(r + s + t) - 105 = -105.$$

Logo

$$-21 = -105 + a \cdot 42 + 0 \iff a = 2.$$

Somando as três primeiras equações temos $r+s+t = r^2+s^2+t^2+a(r+s+t)+3b \iff 0 = 42+2\cdot 0+3b \iff b = -14$. Logo o polinômio pedido é $x^2 + 2x - 14$.

Pode-se provar que esse polinômio satisfaz as condições do enunciado verificando-se que

- $P(x) = x^3 - 21x + 35$ é irredutível e não tem raiz dupla;
- se r é raiz de $P(x)$ então $Q(r) = r^2 + 2r - 14$ também é;
- $Q(r) \neq r$;
- se $Q(r) = s$ e $Q(t) = s$ então s é racional, o que não é possível;
- $Q(r) = s$ e $Q(s) = r$ não é possível.

PROBLEMA 3
Encontre todas as funções $f\colon \mathbb{R} \to \mathbb{R}$ tais que

$$f(xf(y) - f(x)) = 2f(x) + xy$$

para todos x, y reais.

Solução
Resposta: $f(x) = -x + 1$*, para todo* x *real.*

Note que não podemos ter $f(x) = 0$ para todo x real; de fato, fazendo $x = 1$ vemos que $f(f(y) - f(1)) = 2f(1) + y$, e sendo $g(y) = y + 2f(1)$ sobrejetora em $\mathbb{R}$, f é sobrejetora, e injetora, pois $f(x) = f(y) \implies f(f(x) - f(1)) = f(f(y) - f(1)) \iff 2f(1) + x = 2f(1) + y \iff x = y$. Ou seja, f é bijetora.

Vamos nos aproveitar disso, fazendo $2f(x) + xy = f(x) \iff y = -f(x)/x$, $x \neq 0$. Da bijetividade de f,

$$xf\left(-\frac{f(x)}{x}\right) - f(x) = x \iff f\left(-\frac{f(x)}{x}\right) = \frac{f(x)}{x} + 1.$$

Agora substitua $x \to 0$ na equação original. Temos $f(-f(0)) = 2f(0)$. Se $f(0) = 0$, temos, trocando $y \to 0$, $f(-f(x)) = 2f(x) \iff f(x) = -2x$ para todo x, já que f é sobrejetora, e vemos que essa função não dá certo: $f(xf(y) - f(x)) = f(-2xy + 2x) = 4xy - 4x$ e $2f(x) + xy = -4x + xy$. Assim, $f(0) \neq 0$ e podemos fazer $x \to -f(0)$ nessa última equação:

$$f\left(-\frac{f(-f(0))}{-f(0)}\right) = \frac{f(-f(0))}{-f(0)} + 1 \iff f(2) = -2 + 1 = -1.$$

Com essa nova informação, fazemos $y \to 2$ na equação original:

$$f(-x - f(x)) = 2(f(x) + x).$$

Já vimos que não é possível que $f(x) = -2x$ para todo x real, e por outro lado, acabamos de mostrar que existe a tal que $f(a) = -2a$. Se encontrarmos todos os valores de a terminamos o problema, pois isso se reduz a $-x - f(x) = a \iff f(x) = -x - a$, e substituímos todos os valores de a.

Troque agora y pela raiz r de f, ou seja, o único real r tal que $f(r) = 0$. Então

$$f(-f(x)) = 2f(x) + rx.$$

Escolhendo x tal que $f(x) = -a$ (existe pois f é sobrejetora), e lembrando que $f(0) \neq 0 \iff r \neq 0$, obtemos

$$f(a) = -2a + rx \iff rx = 0 \iff x = 0.$$

Assim, $a = -f(0)$ é único e obtemos $f(x) = -x + f(0)$. Sendo $f(0) = b$, substituindo na equação original obtemos

$$f(xf(y) - f(x)) = 2f(x) + xy \iff f(x(-y + b) - (-x + b)) = 2(-x + b) + xy$$
$$\iff (xy - xb - x + b) + b = xy - 2x + b \iff (b + 1)x = 2x,$$

e devemos ter $b = 1$. Logo a única solução é $f(x) = -x + 1$, para todo x real.

Combinatória

PROBLEMA 4

Seja $n \geq 2$ inteiro. Dizemos que duas permutações $(a_1, a_2, \ldots, a_n)$ e $(b_1, b_2, \ldots, b_n)$ de $\{1, 2, \ldots, n\}$ são *amiguinhas* se existe um inteiro $k \geq n$ tal que $b_i = a_{k+1-i}$ para $i = 1, \ldots, k$ e $b_i = a_i$ para $i = k + 1, \ldots, n$.

Prove que é possível colocar todas as permutações de $\{1, 2, \ldots, n\}$ em um círculo de modo que quaisquer duas permutações vizinhas são amiguinhas.

Solução

Denote por f_i a permutação que inverte os i primeiros termos, ou seja, troca $(x_1, x_2, \ldots, x_i, x_{i+1}, \ldots, x_n)$ por $(x_i, x_{i-1}, \ldots, x_1, x_{i+1}, \ldots, x_n)$; em particular, sempre existe um f_i que transforma uma permutação na sua vizinha.

Fazemos indução em n, de fato com hipótese fortalecida: começaremos com $P_1 = (1, 2, \ldots, n)$ e terminaremos com $P_{n!} = (n, n - 1, \ldots, 2, 1)$. Para $n = 1$ não há o que se fazer (e para $n = 2$ também não).

Agora, suponha que o resultado é válido para $n-1$ e provemos para n. Fazendo as permutações da hipótese de indução (isto é, sem mexer no último termo) obtemos $P_1 = (1, 2, \ldots, n-1, n)$ até $P_{(n-1)!} = (n-1, n-2, \ldots, 1, n)$. Nesse caso, obtemos todas as permutações que terminam com n. Aplicamos f_n e obtemos $(n, 1, 2, \ldots, n-1)$ (ou seja, permutamos ciclicamente). Fazemos de novo as permutações e obtemos todas as permutações com $n - 1$ no final, terminando em $(n-2, n-3, \ldots, 1, n, n-1)$; aplicamos novamente f_n e obtemos $(n-1, n, 1, \ldots, n-2)$ e prosseguimos. Note que a cada iteração fazemos uma permutação cíclica, e ao final de $n! - 1$ operações obtemos todas as permutações.

PROBLEMA 5

Considere um tabuleiro $n \times n$. Qual é a maior quantidade de casas que podemos escolher do tabuleiro de modo que não haja um paralelogramo cujos vértices são os centros de quatro das casas escolhidas?

Solução

Resposta: $2n - 1$.

Uma maneira de obter $2n - 1$ casas é ocupar a primeira linha e a primeira coluna do tabuleiro.

Agora considere $2n$ casas do tabuleiro e considere as linhas. Se existem duas linhas com duas peças com a mesma distância entre si, obtemos um paralelogramo; e é claro que há $n - 1$ possíveis distâncias. Sendo $a_1, a_2, \ldots, a_m$ as quantidades de peças nas linhas, $a_i > 0$ (ou seja, $m \leq n$), há pelo menos $a_i - 1$ distâncias distintas possíveis (use a casa mais à esquerda como referência e faça as distâncias até essa casa). Com isso, há pelo menos $a_1 + a_2 + \cdots + a_m - m$ distâncias. Se $a_1 + \cdots + a_m \geq 2n$, há pelo menos $2n - m \geq 2n - n = n$ distâncias possíveis, e por casa dos pombos duas distâncias se repetem; como tomamos o cuidado de não ter distâncias repetidas na mesma linha, elas são em linhas diferentes, e o problema acabou.

PROBLEMA 6

Colorado e Colorina participam de um jogo. Eles alternadamente pintam uma aresta de uma pirâmide cuja base é um 2017-ágono usando uma de k cores, de modo que arestas com um vértice comum tenha cores diferentes. Não é permitido pintar uma aresta que já foi pintada. Colorado começa o jogo e Colorina quer pintar todas as arestas. Qual é o menor valor de k para o qual Colorina sempre consegue pintar todas as arestas da pirâmide?

Solução

Resposta: 2017.

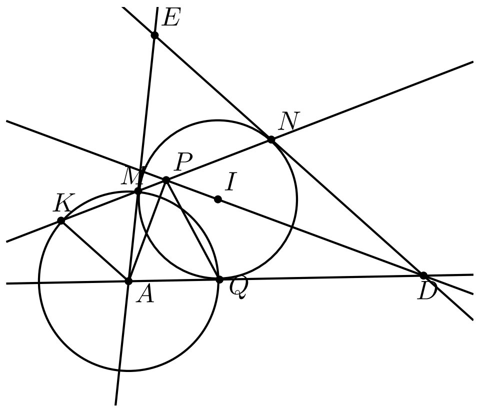
Primeiro, é imediato que $k \geq 2017$, pois o vértice da pirâmide tem grau 2017.

Para $k = 2017$, adote a estratégia de simetria; se Colorado pintar uma aresta a da cor i, pinte a aresta a' a a simétrica em relação à altura pirâmide (que podemos supor sem perdas ser regular) com a cor $2018 - i$. Com isso, Colorina tem sempre uma aresta para pintar.

Geometria

PROBLEMA 7
Seja $ABCD$ um quadrilátero circunscrito no círculo ω, que tem centro I. Suponha que $\angle BAD + \angle ADC < \pi$. Sejam M e N os pontos de tangência de ω em AB e CD, respectivamente. O ponto $K \neq M$ está sobre a reta MN e satisfaz $AK = AM$. Prove que a reta ID corta o segmento de reta KN em seu ponto médio.

Solução
A condição $\angle BAD + \angle ADC < \pi$ serve para mostrarmos que as retas AB e CD se intersectam em um ponto E tal que ω é incírculo de ADE. A partir daqui, podemos ignorar os pontos B e C, e temos um problema no triângulo ADE.



Sejam P o ponto de interseção de DI e MN e Q o ponto de tangência de ω em AD. Como $DN = DQ$, DP é comum e $\angle IDN = \angle IDQ$, os triângulos DQP e DNP são congruentes pelo caso LAL, e $PQ = PN$. Então basta provar que $PQ = PK$, ou seja, PQK é isósceles.

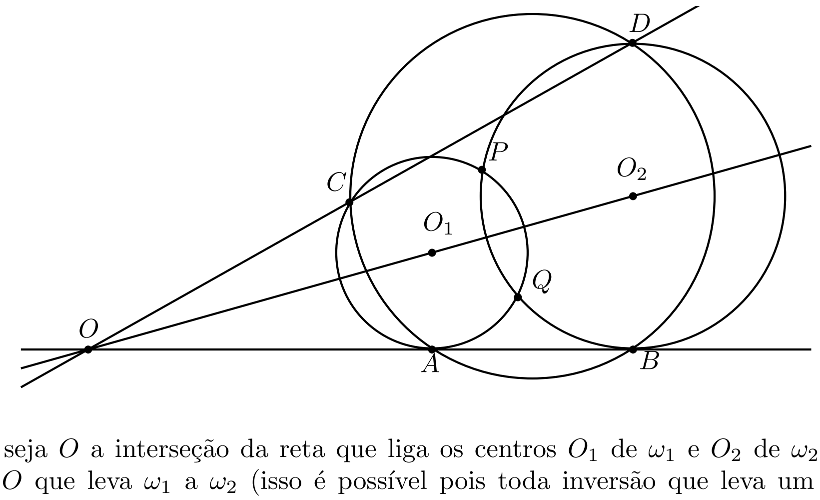
Mas da mesma congruência, agora com ângulos externos e considerando que $EN = EM$ e $AM = AK$, $\angle PQA = \angle PNE = \angle NME = \angle KMA = \angle AKM = \angle AKP < 90°$, $AQ = AM = AK$ e AP é comum. Assim, pela lei dos senos

$$\frac{AQ}{\operatorname{sen}\angle APQ} = \frac{AP}{\operatorname{sen}\angle AQP} = \frac{AP}{\operatorname{sen}\angle AKP} = \frac{AK}{\operatorname{sen}\angle APK},$$

de modo que $\operatorname{sen}\angle APQ = \operatorname{sen}\angle APK$, ou seja, $\angle APQ$ e $\angle APK$ são iguais ou suplementares. Mas $\angle APQ + \angle APK < \pi$, logo $\angle APQ = \angle APK$, e os triângulos AKP e AQP são congruentes pelo caso ALA, e $PQ = PK$, como queríamos demonstrar.

PROBLEMA 8
Os círculos ω_1 e ω_2 se cortam em P e Q. Uma reta é tangente a ω_1 em A e a ω_2 em B. Um círculo passa por A e B e corta ω_1 em $C \neq A$ e ω_2 em $D \neq B$. Prove que $\frac{CP}{CQ} = \frac{DP}{DQ}$.

Solução
Se ω_1 e ω_2 têm o mesmo raio, a figura toda é simétrica com relação a PQ, e a relação é imediata.



Caso contrário, seja O a interseção da reta que liga os centros O_1 de ω_1 e O_2 de ω_2 e AB. Considere a inversão de centro O que leva ω_1 a ω_2 (isso é possível pois toda inversão que leva um círculo a outro tem centro no centro de homotetia direta entre os dois círculos). Ela leva A a B, e sendo C' a imagem de C, sendo $OA \cdot OB = OC \cdot OC'$, A, B, C e C' são concíclicos e, como C pertence a ω_1, C' pertence a ω_2. Logo $D = C'$. Note também que P e Q são fixados pois interseções são levadas a interseções.

Deste modo, usando a fórmula $X'Y' = \frac{XY}{OX \cdot OY} r^2$, em que r é o raio de inversão, como $OP = OQ = r$,

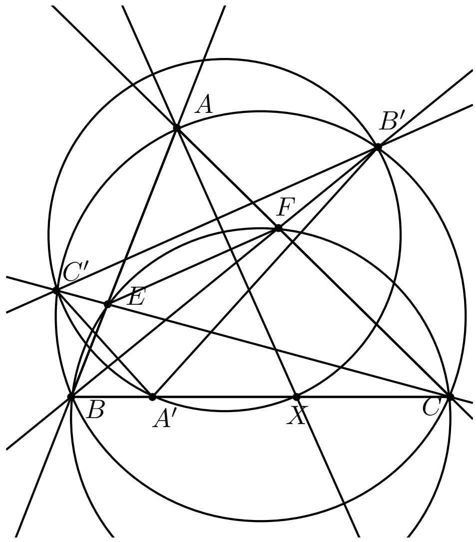
$$\frac{DP}{DQ} = \frac{C'P'}{C'Q'} = \frac{CP \cdot r^2}{OP \cdot OC} \cdot \frac{OQ \cdot OC}{CQ \cdot r^2} = \frac{CP}{CQ}.$$

PROBLEMA 9

No triângulo ABC, ω é um círculo que passa por B e C e corta o lado AB em E e o lado AC em F. As retas BF e CE cortam o circuncírculo de ABC novamente em B' e C', respectivamente. Seja A' o ponto sobre BC tal que $\angle C'A'B = \angle B'A'C$.

Prove que, ao variar ω, os circuncírculos dos triângulos $A'B'C'$ passam um ponto comum.

Solução



Seja $X \neq A'$ a interseção do circuncírculo de $A'B'C'$ com BC. Então, no quadrilátero cíclico $A'C'B'X$, $\angle XB'C' = \angle BA'C' = \angle CA'B' = \angle B'C'X$, ou seja, $XB'C'$ é isósceles. Isso quer dizer que X pertence à mediatriz de $B'C'$.

Por outro lado, $\angle C'CA = \angle ECF = \angle EBF = \angle ABB'$, e os arcos AC' e AB' são congruentes. Ou seja, $AC' = AB'$, e A também pertence à mediatriz de $B'C'$. Sendo $B'C'$ uma corda do circuncírculo de ABC, essa mediatriz também passa pelo circuncentro O de ABC. Portanto X é a interseção de AO com BC, e é o ponto comum a todos os circuncírculos de $A'B'C'$.

Teoria dos Números

PROBLEMA 10

Seja n um inteiro positivo. Suponha que seus divisores possam ser particionados em pares de modo que a soma de cada par de divisores é um primo. Prove que esses primos são todos distintos e que nenhum desses primos é divisor de n.

Solução

Sejam d_1, d_2 um dos pares do problema. Se $p \mid d_1$ e $p \mid d_2$, então $p \mid d_1 + d_2$ e $d_1 + d_2 > p$, de modo que $d_1 + d_2$ não é primo. Portanto $\mathrm{mdc}(d_1, d_2) = 1$, e $d_1 d_2 \mid n$. Em particular, $d_1 d_2 \leq n$. Multiplicando tudo, temos que o produto de todos os $2t$ divisores é menor ou igual a n^t. Por outro lado, podemos formar pares $\{d, n/d\}$ de divisores, e o produto dos divisores é $(d \cdot n/d)^t = n^t$. Com isso, ocorre igualdade, e todos os pares são da forma $\{d, n/d\}$, e mais ainda, $\mathrm{mdc}(d, n/d) = 1$.

Agora podemos provar os fatos do problema. Primeiro note que $f(d) = d + n/d$ é decrescente em $[0, \sqrt{n}]$, logo os primos são distintos. Finalmente, se p é um primo que divide n então p divide exatamente um dos números $d, n/d$, já que $\mathrm{mdc}(d, n/d) = 1$. Logo $p \nmid d + n/d$, e $\mathrm{mdc}(n, d + n/d) = 1$, ou seja, $d + n/d$ não pode ser divisor de n.

PROBLEMA 11

Sejam $c, d \geq 2$ inteiros. Defina $a_1 = c$ e $a_n = a_{n-1}^d + c$, $n \geq 2$. Prove que, para todo $n \geq 2$, existe um primo p que divide a_n e nenhum dos números $a_1, a_2, \ldots, a_{n-1}$.

Solução
Primeiro, é fácil ver por indução de $c \mid a_i$ para todo i, então seja $b_i = a_i/c$. Com isso, $b_1 = 1$ e $b_n = c^{d-1}b_{n-1}^d + 1$. Com isso, $\text{mdc}(b_n, c) = 1$. Começaremos provando que $\text{mdc}(b_n, b_m) = b_{\text{mdc}(n,m)}$.

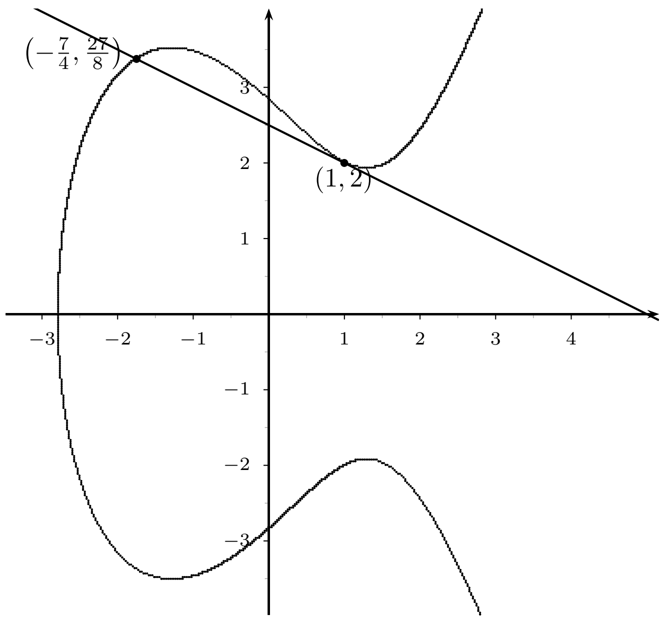
Para isso, provaremos que $b_n \equiv b_{n-m} \pmod{b_m}$ para $n > m$, por indução em n. Para $n = m+1$, $b_{m+1} = c^{d-1}b_m^d + 1 \equiv 1 = b_1 \pmod{b_m}$. Para $n > m+1$, $b_n = c^{d-1}b_{n-1}^d + 1 \equiv c^{d-1}b_{n-m-1}^d + 1 = b_{n-m} \pmod{b_m}$. Com isso, $\text{mdc}(b_n, b_m) = \text{mdc}(b_{n-m}, b_m)$ e usamos o algoritmo de Euclides, obtendo o resultado.

Isso ainda não resolve o problema, pois b_n pode ser grande sem ter fatores primos novos. Para ajeitar isso, vamos comparar os fatores primos p de b_n. Para isso, mostraremos que se $p^k \mid b_n$ então $p^{kd} \mid b_{mn} - b_n$. Para isso, note que $b_{n+1} = c^{d-1}b_n^d + 1 \equiv 1 = b_1 \pmod{p^{dk}}$, e a mesma indução que a acima mostra que $b_{n+t} \equiv b_t \pmod{p^{dk}}$ para todo t. Em particular, $b_{mn} \equiv b_n \pmod{p^{dk}}$. A consequência imediata disso é que se $p \mid b_n$ então $\nu_p(b_n) = \nu_p(b_t)$ para todo divisor t de n, pois se $k = \nu_p(a_t)$ então $p^{dk} \mid a_n - a_t$ e, sendo $d > 1$, $a_n \equiv a_t \not\equiv 0 \pmod{p^{k+1}}$ e $p^k \mid a_n$.

Agora, se b_n não tem fator primo novo então b_n tem todos os seus fatores em b_t, t divisor de n, de modo que $b_1 b_2 \ldots b_{n-1} \geq b_n > b_{n-1}^d \implies b_1 b_2 \ldots b_{n-2} > b_{n-1}^{d-1} > b_{n-2}^{d(d-1)} \implies b_1 \ldots b_{n-3} > b_{n-2}^{d(d-1)-1}$, e assim por diante, até que obtemos $b_1 > b_1$, um absurdo. Com isso, b_n tem fator primo novo.

PROBLEMA 12
Prove que existem infinitos pares de racionais (x, y) tais que $y^2 = x^3 - 5x + 8$.

Solução
Primeiro, note que $(1, 2)$ é uma solução da equação diofantina dada. Agora, considerando o gráfico da relação $y^2 = x^3 - 5x + 8$, trace a reta que passa por $(1, 2)$ e é tangente a essa curva, ou seja, escolha racionais a e b tais que a reta é $y = ax + b$. Assim, $2 = a \cdot 1 + b$ e $(ax+b)^2 = x^3 - 5x + 8$ tem 1 como raiz dupla. Logo $(ax + 2 - a)^2 = x^3 - 5x + 8$ e, pelas relações entre coeficientes e raízes, sendo r a outra raiz, $a^2 = 1 + 1 + r$ e $a^2 - 4a - 4 = r$, de modo que $a^2 = r + 2$ e $r + 2 - 4a - 4 = r \iff a = -1/2$. Com isso, $r = a^2 - 2 = -7/4$, e $b = 2 - a = 5/2$. logo $y = -x/2 + 5/2$ é a reta tangente, para $x = -7/4$ obtemos $y = 27/8$ e obtemos outra solução racional $(-7/4, 27/8)$.



Vamos generalizar essa ideia: sendo $P = (x_0, y_0)$ um ponto com coordenadas racionais sobre a curva, traçamos a reta $y - y_0 = a(x - x_0)$ que passa por P e é tangente à curva em P. Com isso,

$$(a(x - x_0) + y_0)^2 = x^3 - 5x + 8,$$

e, sendo r a outra raiz, temos $a^2 = 2x_0 + r$, $x_0^2 r = -8 + (ax_0 + y_0)^2 = -8 + a^2x_0^2 - 2ax_0y_0 + y_0^2 = -8 + (2x_0 + r)x_0^2 - 2ax_0y_0 + (x_0^3 - 5x_0 + 8) = 3x_0^3 + rx_0^2 - 2ax_0y_0 - 5x_0 \iff a = \frac{3x_0^2 - 5}{2y_0}$, que é racional. Com isso, o novo ponto tem coordenada x dada por $r = a^2 - 2x_0$, que também é racional e a coordenada y dada por $y = a(r - x_0) + y_0$, que também é racional. Com isso, obtemos sempre um novo ponto racional ao traçar a tangente... a não ser que obtenhamos um ciclo. Provemos que isso não acontece.

Note que se $x_0 = m/n$, $\text{mdc}(m, n) = 1$, então $a = \frac{3m^2 - 5n^2}{2mn}$. Seja $\nu_2(n)$ a quantidade de fatores 2 em n. No que seria a segunda iteração, $x_0 = -7/4$, e obtemos $\nu_2(n) = 2$. Suponha que $\nu_2(n) > 0$. Então $\nu_2(m) = 0$ e $3m^2 - 5n^2$ é ímpar, ou seja, nenhum fator 2 cancela. Com isso, o denominador de a tem $\nu(n) + 1$ fatores 2, ou seja, sempre aumenta. Finalmente, $r = a^2 - 2x_0$ tem $2\nu_2(n) + 2$ fatores 2 no denominador, pois $2x_0 = -2m/n$ soma um número par no numerador de r, e não cortamos fatores 2. Com isso, como os denominadores dos novos pontos têm mais fatores 2 do que o ponto anterior, os pontos não podem se repetir.

Observação: curvas do tipo $y^2 = x^3 + Ax + B$ são curvas elípticas, e são bastante usadas em teoria dos números moderna. A quantidade de pontos com coordenadas racionais sobre curvas elípticas pode ser finita nula, finita não nula – por exemplo, $y^2 = x^3 + px$, p primo congruente a 9 ou 13 módulo 16 – ou infinita, como no nosso problema. Sabe-se que a quantidade de pontos com coordenadas inteiras, no caso em que $x^3 + Ax + B$ não tem raiz dupla nem tripla, é finita.

Problemas gerais

PROBLEMA 13

Seja P um ponto no interior do triângulo ABC tal que

$$\frac{AP+BP}{AB} = \frac{BP+CP}{BC} = \frac{CP+AP}{CA}.$$

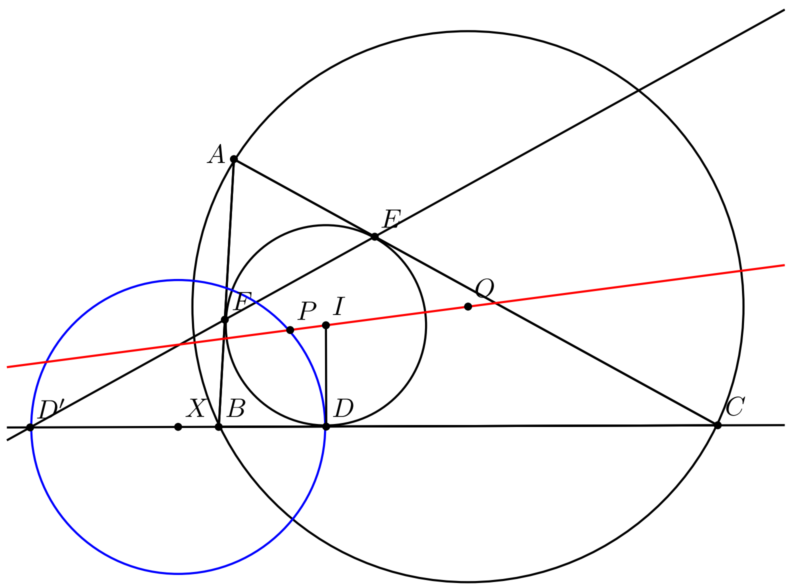
As retas AP, BP, CP cortam o circuncírculo de ABC novamente em A', B', C'. Prove que os incírculos dos triângulos ABC e $A'B'C'$ coincidem.

Solução

Primeiro note que, sendo $2p = AB + BC + CA$,

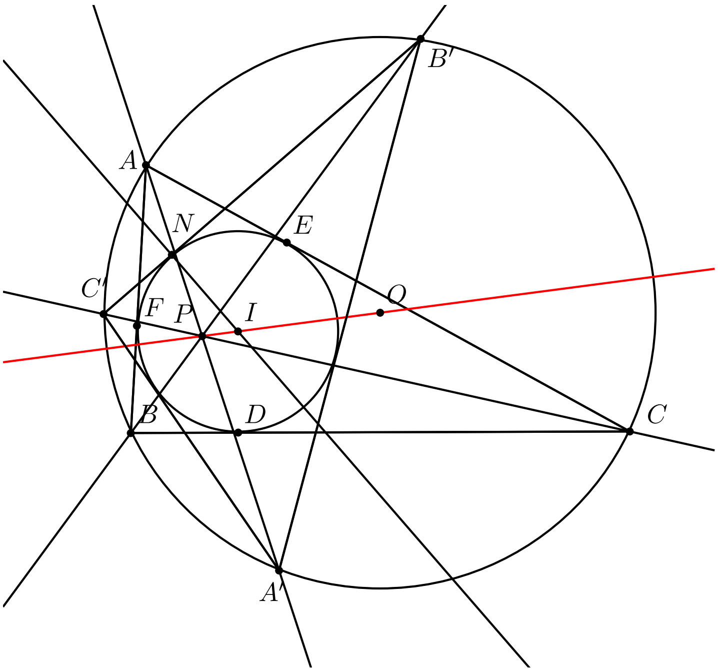
$$\frac{AP+BP}{AB} = \frac{BP+CP}{BC} = \frac{CP+AP}{CA} = \frac{2(AP+BP+CP)}{2p} = \frac{AP+BP+CP}{p}$$
$$\iff AP : BP : CP = (p-a) : (p-b) : (p-c).$$

Em outras palavras, P é a interseção dos círculos de Apolônio correspondentes aos pontos de tangência D sobre BC, E sobre CA e f sobre AB do incírculo no triângulo ABC.



Seja DD' o diâmetro e X o centro do círculo de Apolônio correspondente. Inverta a figura por esse círculo. Então B é levado em C, e concluímos que $XP^2 = XB \cdot XC = XD^2$, ou seja, as potências de X com relação ao ponto P, ao circuncírculo e ao incírculo são iguais. Isso também vale para os centros Y e Z dos outros dois círculos de Apolônio, logo XYZ é o eixo radical desses três círculos, e além disso os três centros P, I (incentro) e O (circuncentro) são colineares.

Consideremos agora a figura toda:



Agora vejamos a semelhança entre BPC e $C'PB'$. Ela leva a projeção de P no lado BC à projeção de P sobre $B'C'$, e leva o ponto médio de BC ao ponto médio de $B'C'$; esses pontos médios são projeções de O sobre esses lados. Com isso, as projeções de I sobre BC e $B'C'$ são correspondentes. Sendo N a projeção de I sobre $B'C'$, temos também da semelhança $\angle INP = \angle IDP$. Além disso, considerando o círculo de Apolônio, PD é bissetriz de $\angle BPC$ e, da semelhança, PN é bissetriz de $\angle C'PB'$, e assim D, P e N são colineares, ou seja, $\angle IPN$ e $\angle IPD$ são suplementares, e têm o mesmo seno. Assim, pela lei dos senos,

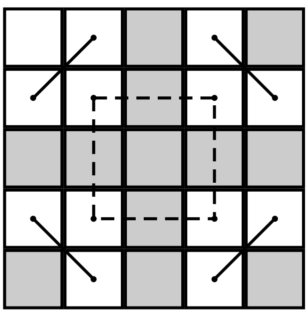
$$\frac{IN}{\operatorname{sen}\angle IPN} = \frac{IP}{\operatorname{sen}\angle INP} = \frac{IP}{\operatorname{sen}\angle IDP} = \frac{ID}{\operatorname{sen}\angle IPD} \implies IN = ID.$$

Logo o lado $B'C'$ é tangente ao incírculo, e analogamente os lados $A'B'$ e $A'C'$ também, e o problema terminou.

PROBLEMA 14
Suponha que as casas de um tabuleiro $n \times n$ são pintadas de preto e branco de modo que cada casa preta tem uma quantidade par de casas vizinhas (lado comum) brancas. Prove que é possível pintar todas as casas brancas de vermelho ou azul de modo que cada casa preta tenha uma quantidade igual de casas vizinhas azuis e vermelhas.

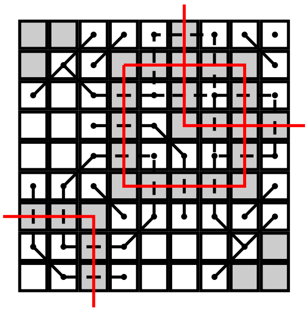
Solução
Considere o grafo G cujos vértices são as casas brancas com alguma casa preta vizinha e ligue duas casas se elas têm exatamente um vértice em comum. Note que cada casa preta com quatro brancas vizinhas tem todas as casas brancas ligadas em ciclo.

Agora, considere uma casa preta com exatamente duas brancas vizinhas. Essas duas casas brancas ou estão ligadas em G ou são opostas. Construa o grafo H colocando em G arestas tracejadas correspondentes a essas casas brancas opostas. Note que o problema é equivalente que podemos pintar H de duas cores, vermelho e azul, de modo que vértices ligados por aresta tenha cores diferentes. Em outras palavras, H deve ter número cromático 2. Isso é equivalente a provar que H é bipartido (se H é bipartido, basta pintar cada classe de uma cor; se dá para pintar, considere as cores dos vértices, e o grafo com classes de cada cor é bipartido).



Cada aresta corresponde a mudar a paridade das coordenadas das duas casas. O grafo G é bipartido, pois se há ciclo, precisamos mudar a paridade uma quantidade par de vezes, e a quantidade de arestas (e portanto vértices) é par. Agora vamos ajeitar H. Para isso basta provar que todo ciclo tem uma quantidade par de arestas tracejadas.

Note que cada aresta tracejada está associada a uma única casa preta. Vamos fazer uma sequência de casas pretas, a partir de uma casa preta com aresta tracejada. Essa casa não pode estar no canto do tabuleiro. Como ela tem duas casas brancas vizinhas, ela também tem pelo menos uma casa preta vizinha. Vá para essa casa; se ela não está na borda do tabuleiro, ela tem mais uma casa preta vizinha; e caso a casa preta em que estamos tenha todas as vizinhas pretas, continue na mesma direção; continue esse procedimento até chegar ao bordo do tabuleiro ou completar um ciclo de casas pretas. Repita o procedimento com toda aresta tracejada. Como toda casa preta tirando as da borda têm uma quantidade par de vizinhas pretas, podemos dividir o tabuleiro em várias regiões com essas linhas pretas; de fato, suponha que duas dessas linhas se cruzem: para isso acontecer, a casa preta deve ter todas as vizinhas pretas, e aí elas se cruzam.



Agora vamos mostrar que é possível pintar as regiões de duas cores com indução sobre as linhas. Se só tem uma linha, só há duas regiões, e é só pintá-las de cores diferentes; se há mais, retire uma linha, pinte (o que é possível pela hipótese de indução), coloque a linha de volta, dividindo o tabuleiro (inteiro) em duas regiões; mantenha as cores de uma região e troque todas as cores da outra região – por hipótese de indução não há problemas dentro de cada região e, como trocamos as cores, na nova linha as cores são diferentes.

Como cada aresta tracejada liga duas regiões diferentes, e pintamos as regiões de duas cores diferentes, a quantidade de arestas tracejadas é par, e o problema acabou.

PROBLEMA 15

Sejam $A = A(x, y)$ e $B = B(x, y)$ polinômios de duas variáveis com coeficientes reais. Suponha que $A(x, y)/B(x, y)$ é um polinômio em x para infinitos valores de y e é um polinômio em y para infinitos valores de x. Prove que B divide A, ou seja, existe um polinômio C de coeficientes reais tal que $A = B \cdot C$.

Solução

Primeiro considere A e B como polinômios em x, e divida A por B, obtendo $A = B \cdot Q + R$, com o grau em x de R menor do que o grau em x de B (sendo mais específico, escrevemos $A = \sum_{k=0}^{n} A_k(y)x^k$, $B = \sum_{k=0}^{m} B_k(y)x^k$; os polinômios Q e R são somas de produtos de funções racionais de y com x^k. Temos $A/B = Q + R/B$. Como A/B e Q são polinômios em x para infinitos valores de y, R/B também o é. Suponha, por absurdo que R não é nulo.

Agora, considere o coeficiente líder de B, um polinômio $B_m(y)$ em y. Há infinitos valores de y que tornam R/B polinômio em x, e, tirando possivelmente os que zeram $B_m(y)$, sobram infinitos valores de y para os quais R/B é um polinômio em x, mas o coeficiente líder de B não some. Mas o grau de R é menor do que o de B, então para R/B poder ser polinômio R deve ser nulo.

Com isso, $A = B \cdot Q$, em que Q é um polinômio em x cujos coeficientes são funções racionais em y. Ou seja, $Q = F(x, y)/U(y)$. Trocando x por y, obtemos $A = B \cdot P$ com $P = G(x, y)/V(x)$. Logo, como $P = Q = A/B$,

$$\frac{F(x,y)}{U(y)} = \frac{G(x,y)}{V(x)} \iff F(x,y)V(x) = G(x,y)U(y).$$

Como $U(y)$ e $V(x)$ não têm fatores comuns, $U(y)$ divide $F(x, y)$, de modo que $Q = F/U$ é um polinômio de duas variáveis, completando a demonstração.

PROBLEMA 16

Para m inteiro maior do que 1, dizemos que a é *m-poderoso* se $\text{mdc}(a, m) = 1$ e existe x inteiro positivo tal que $x^x - a$ é múltiplo de m. Prove que se a é n^n-poderoso, então também é $n^{(n^n)}$-poderoso.

Solução

Sejam $p_1 < p_2 < \ldots < p_k$ os fatores primos de n. Provaremos que se existe x tal que $x^x \equiv a \pmod{p_1^r \ldots p_k^r}$ com $p_1^r \geq p_k$ então existe y tal que $y^y \equiv a \pmod{p_1^{r+1} \ldots p_k^{r+1}}$. Ou seja, indutivamente obtemos $z^z \equiv a \pmod{p_1^N \ldots p_k^N}$ para todo $N \geq r$, e escolhendo N suficientemente grande obtemos $z^z \equiv a \pmod{n^{n^n}}$. Como n^n implica $r \geq n$, a hipótese é verdadeira, e o problema acabaria.

Vamos provar o fato então. Seja $M = \text{mmc}((p_i - 1)p_i^r, 1 \le i \le k)$ o mmc dos $\phi(p^{r+1})$. Começamos escolhendo $y = x + tM$, para manter a conta módulo $p_1^r \dots p_k^r$. De fato, $y^y = (x+tM)^x (x+tM)^{tM} \equiv (x+tM)^x \pmod{p_1^{r+1} \dots p_k^{r+1}}$. Note que $M^2 \equiv 0 \pmod{p_1^{r+1} \dots p_k^{r+1}}$, logo abrindo com o binômio de Newton temos

$$y^y \equiv x^x + \binom{x}{1} x^{x-1} tM = x^x(1 + tM) \pmod{p_1^{r+1} \dots p_k^{r+1}}.$$

Agora é só ajeitar t para obter $x^x(1 + tM) \equiv a \pmod{p_1^{r+1} \dots p_k^{r+1}}$. Mas já temos $x^x = a + up_1^r \dots p_k^r$, e fazendo a conta temos

$$a + taM + up_1^r \dots p_k^r + uaMp_1^r \dots p_k^r \equiv a \pmod{p_1^{r+1} \dots p_k^{r+1}}.$$

Mas M é múltiplo de $p_1^r p_2^r \dots p_k^r$, e como $p_i - 1 < p_k \le p_j^r$, o mmc não tem mais do que r de cada fator p_i, e $M/(p_1^r \dots p_k^r) = v$ com $\text{mdc}(v, p_1 \dots p_k) = 1$. Com isso, cortando $p_1^r \dots p_k^r$ temos

$$tav + u \equiv 0 \pmod{p_1 \dots p_k} \iff t \equiv -u(av)^{-1} \pmod{p_1 \dots p_k},$$

o que é possível, completando a solução.