CONTEÚDO

AOS LEITORES 2

XLIII OLIMPÍADA INTERNACIONAL DE MATEMÁTICA 3
Enunciados, Soluções e Resultado Brasileiro

XVII OLIMPÍADA IBEROAMERICANA DE MATEMÁTICA 15
Enunciados, Soluções e Resultado Brasileiro

ARTIGOS

A FÓRMULA DE CARDANO ALÉM DAS CÚBICAS 24
José Cloves Verde Saraiva, São Luis - MA

RECIPROCIDADE QUADRÁTICA 27
Carlos Gustavo T. de A. Moreira & Nicolau Corção Saldanha, Rio de Janeiro - RJ

APLICAÇÕES DE PLANOS PROJETIVOS EM TEORIA DOS NÚMEROS E COMBINATÓRIA 31
Carlos Yuzo Shine, São Paulo - SP

OLIMPÍADAS AO REDOR DO MUNDO 43

SOLUÇÕES DE PROBLEMAS PROPOSTOS 54

PROBLEMAS PROPOSTOS 59

COORDENADORES REGIONAIS 61

AOS LEITORES

Chegamos a esta última edição do ano 2002 muito contentes com o desempenho olímpico do Brasil: Pelo segundo ano consecutivo todos os integrantes da equipe brasileira ganharam medalha na Olimpíada Internacional de Matemática, e além disso tivemos excelentes resultados na Olimpíada de Matemática do Cone Sul e na Olimpíada Iberoamericana de Matemática, onde ganhamos a maioria das medalhas de ouro em disputa. Publicamos aqui as soluções dos problemas da IMO e da Ibero, sendo a maioria delas dos membros das equipes brasileiras.

Agradecemos mais uma vez a crescente colaboração dos leitores, enviando problemas propostos e soluções, e pedindo que publiquemos soluções de problemas de várias fontes, como das Olimpíadas ao Redor do Mundo.

Esse intercâmbio é fundamental para nós, e ajuda a manter a revista Eureka! viva e interessante.

Abraços e feliz 2003 para todos!

Os editores.

XLIII OLIMPÍADA INTERNACIONAL DE MATEMÁTICA

Enunciados, Soluções e Resultado Brasileiro

A XLIII Olimpíada Internacional de Matemática foi realizada na cidade de Glasgow, Reino Unido no período de 18 a 31 de julho de 2002.

A equipe brasileira foi liderada pelos professores Edmilson Motta (São Paulo – SP) e Ralph Costa Teixeira (Niterói – RJ).

O Resultado da Equipe Brasileira

BRA 1	**Alex Corrêa Abreu**	**Bronze**
BRA 2	**Larissa Cavalcante Queiroz de Lima**	**Prata**
BRA 3	**Guilherme Issao Camarinha Fujiwara**	**Bronze**
BRA 4	**Yuri Gomes Lima**	**Bronze**
BRA 5	**Davi Máximo Alexandrino Nogueira**	**Bronze**
BRA 6	**Thiago da Silva Sobral**	**Bronze**

PRIMEIRO DIA

DURAÇÃO: 4 horas e meia.

PROBLEMA 1

Seja n um inteiro positivo. Seja T o conjunto de pontos $(x; y)$ no plano onde x e y são inteiros não negativos e $x + y < n$. Cada ponto de T é pintado de vermelho ou azul. Se um ponto $(x; y)$ é vermelho, então todos os pontos $(x'; y')$ com $x' \le x$ e $y' \le y$ também são. Um conjunto X é um conjunto de n pontos azuis com abcissas todas distintas, e um conjunto Y é um conjunto de n pontos azuis com ordenadas todas distintas. Prove que o número de conjuntos X é igual ao número de conjuntos Y.

SOLUÇÃO DE GUILHERME FUJIWARA (SÃO PAULO – SP)

Primeiramente, seja $x(i)$ o número de pontos azuis cuja ordenada é i, e $y(i)$ o número de pontos azuis de abscissa i.

Veja que o número de *X-conjuntos* é $\prod_{i=0}^{n-1} y(i)$, e o número de *Y-conjuntos* é $\prod_{i=0}^{n-1} x(i)$.

Para provar que o número de *X-conjuntos* é igual ao número de *Y-conjuntos*, é suficiente provar que os números $x(0), x(1), x(2),...,x(n-1)$ são uma permutação dos números $y(0), y(1), y(2),..., y(n-1)$. Provaremos este lema por indução no n.

Se $n = 1$, temos que $x(0) = y(0) = 1$ ou 0 dependendo se (0; 0) é azul ou não.

Suponhamos que o lema é verdadeiro para $n < k$, provaremos para $n = k$.

Vamos olhar para a última diagonal de T (reta $x + y = k - 1$):

Se nela não houver pontos vermelhos, então tome T' como os conjuntos de pontos de

T que não estão na última diagonal. Temos que o lema vale para os $x'(i)$ e $y'(i)$ de T', e como $x(i) = x'(i) + 1$ e $y(i) = y'(i) + 1$, então $x'(a) = y'(b) \Leftrightarrow x(a) = y(b)$, e além disso $x(k-1) = y(k-1) = 1$, portanto o lema vale para T (vide fig. 1).

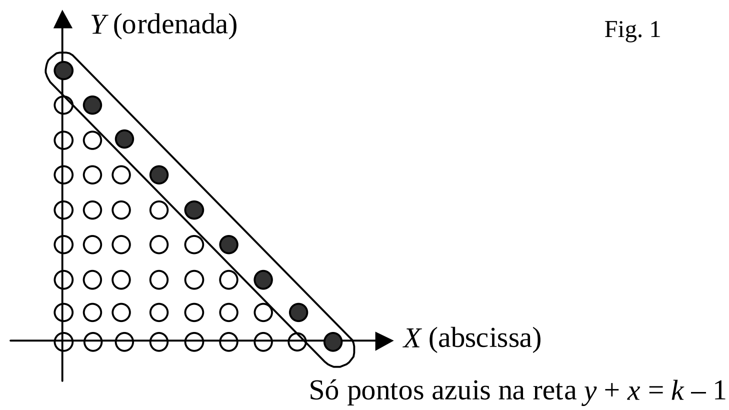


Fig. 1

Se nela houver algum ponto vermelho, digamos $(a; k-1-a)$, então aplicamos a hipótese de indução nos dois conjuntos T' formados acima e à direita de T, que são menores que T, e assim demonstramos o lema para T (vide fig. 2).

Provamos então o nosso lema e, como já foi visto anteriormente, segue o que é pedido no enunciado.

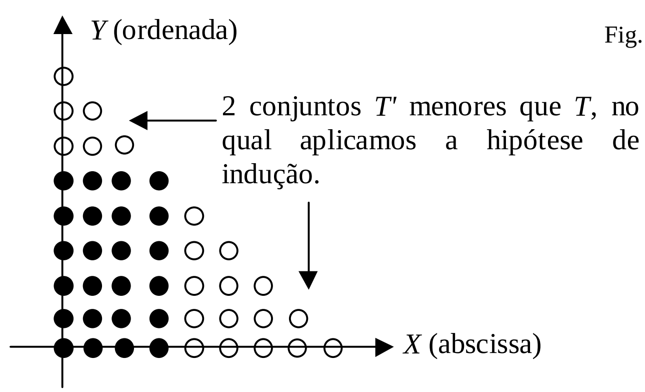


Fig. 2

PROBLEMA 2

Seja *BC* um diâmetro do círculo Γ de centro *O*. Seja *A* um ponto de Γ tal que $0^0 < \angle AOB < 120^0$. Seja *D* o ponto médio do arco *AB* que não contém *C*. A reta que passa por *O* e é paralela a *DA* encontra a reta *AC* em *J*. A mediatriz de *OA* corta Γ em *E* e *F*. Prove que *J* é o incentro do triângulo *CEF*.

SOLUÇÃO DE YURI GOMES LIMA (FORTALEZA – CE)

Como *EF* é perpendicular ao raio *OA*, os arcos *EA* e *AF* são iguais, donde $\angle ECA = \angle ACF \Rightarrow \angle ECJ = \angle JCF$. Portanto, *J* já pertence à bissetriz de $\angle ECF$. Se mostrarmos então que *AJ* = *AE*, acabou (pois sabemos que o médio do arco *EF* eqüidista de *E*, de *F* e do incentro de *CEF*).

Mas, se *l* é a paralela a *DA* por *O*, temos que *l* // *DA* e *DO* // *AC* (pois $\angle DOB = \angle AOB/2 = \angle ACB$) $\Rightarrow$ *DAJO* paralelogramo $\Rightarrow$ *AJ* = *DO*. Também, sendo *EF* mediatriz de *OA*, segue que *EA* = *EO*. Mas *EO* = raio de Γ = *DO* , donde *AJ* = *EA* = *AF*.

OBS: é necessário $\angle AOB < 120°$, pois caso contrário teríamos $\angle AOC \le 60°$ e $\angle BOD \ge 60°$, o que implicaria $J = l \cap AC$ fora de Γ, não podendo então ser este o incentro de *CEF*.

PROBLEMA 3

Encontre todos os pares de inteiros *m*, $n \ge 3$ tais que há infinitos inteiros positivos *a* para os quais $\dfrac{a^m + a - 1}{a^n + a^2 - 1}$ é inteiro.

SOLUÇÃO DE ALEX CORRÊA ABREU (NITERÓI – RJ)

Seja $P = P(x) = x^m + x - 1$ e $Q(x) = x^n + x^2 - 1 \Rightarrow \exists T, R \in \mathbb{Z}[x]$ tq

$P(x) = T(x) \cdot Q(x) + R(x),$

com $\deg R < \deg Q$ ou $R \equiv 0 \Rightarrow \dfrac{P(a)}{Q(a)} = T(a) + \dfrac{R(a)}{Q(a)} \Rightarrow \dfrac{R(a)}{Q(a)} = \dfrac{P(a)}{Q(a)} - T(a)$ é inteiro

para infinitos *a*'s mas se $R \ne 0 \Rightarrow \exists n$ tq $|x| > n \Rightarrow 0 < \left|\dfrac{R(x)}{Q(x)}\right| < 1$ pois

$\deg R < \deg Q \Rightarrow \left|\dfrac{R(a)}{Q(a)}\right| < 1$ se $|a| > n \Rightarrow$ existe apenas um número finito de *a*'s tq

$\frac{R(a)}{Q(a)}$ é inteiro $\Rightarrow R \equiv 0 \Rightarrow P(x) = T(x) \cdot Q(x) \Rightarrow Q(x) | P(x) \Rightarrow Q(x) | P(x) \cdot (x+1) - Q(x) =$

$= x^{m+1} + x^m + x^2 - 1 - x^n - x^2 + 1 = x^n(x^{m-n+1} + x^{m-n} - 1)$; note que temos, $m \ge n$

(pois $Q(x) \mid P(x)$) mas $mdc(Q(x), x^n) = mdc(x^2 - 1, x^n) = 1 \Rightarrow Q(x) \mid x^{m-n+1} + x^{m-n} - 1 \Rightarrow$ por raciocínio análogo ao anterior, $m - n + 1 \geq n \Rightarrow 2n \leq m + 1 (I)$.

Agora, como $Q(0) = -1$, $Q(1) = 1 \Rightarrow \exists 0 < \alpha < 1$ tq $Q(\alpha) = 0 \Rightarrow P(\alpha) = T(\alpha)Q(\alpha) = 0$ $\Rightarrow \alpha^n + \alpha^2 - 1 = 0 = \alpha^m + \alpha - 1 (II) \Rightarrow$

de (*I*), $\alpha^{2n} \geq \alpha^{m+1} (III) \Rightarrow$ por (*II*), $(1 - \alpha^2)^2 \geq \alpha \cdot \alpha^m = \alpha(1 - \alpha) \Rightarrow$

$(1 - \alpha)^2 (1 + \alpha)^2 \geq \alpha(1 - \alpha) \Rightarrow (1 - \alpha)(1 + \alpha)^2 \geq \alpha$ pois $\alpha < 1 \Rightarrow$

$\alpha^3 + \alpha^2 - 1 \leq 0 \Rightarrow \alpha^3 \leq 1 - \alpha^2 = \alpha^n \Rightarrow n \leq 3$ mas $n \geq 3 \Rightarrow n = 3$ e a desigualdade só não é estrita em (*III*) se $m + 1 = 2n \Rightarrow m = 5$ logo se existir uma solução será (5, 3), que de fato é uma solução, pois obviamente

$$x^5 + x - 1 = (x^2 - x + 1)(x^3 + x^2 - 1) \Rightarrow P(x) = (x^2 - x + 1) \cdot Q(x).$$

SEGUNDO DIA

DURAÇÃO: 4 horas e meia.

PROBLEMA 4

Seja n inteiro maior que 1. Os divisores positivos de n são $d_1, d_2, \ldots, d_k$, onde

$$1 = d_1 < d_2 < \ldots < d_k = n$$

Seja $D = d_1d_2 + d_2d_3 + \ldots + d_{k-1}d_k$.

(a) Prove que $D < n^2$.

(b) Encontre todos os valores de n para os quais D é um divisor de n^2.

SOLUÇÃO DE THIAGO DA SILVA SOBRAL (FORTALEZA – CE)

Lema: $d_i = \dfrac{n}{d_{k+1-i}}$

Prova:

Observando que se d é divisor de n então n/d também o é, podemos agrupar os divisores aos pares, donde concluímos que $d_i d_{k+1-i} = n$, $0 \leq i \leq k$. Esse fato também vale para n sendo quadrado perfeito, pois $d_{\frac{k+1}{2}} = d_{k+1-\frac{k+1}{2}} = \sqrt{n}$

Corolário: $d_i \leq \dfrac{n}{k+1-i}$

Prova:

De fato, sendo d_{k+1-i} o (k + 1 – i)-ésimo divisor de n, temos $d_{k+1-i} \geq k+1-i$, e segue o resultado pelo lema.

Pelo corolário,

$$D = d_1d_2 + d_2d_3 + \ldots + d_{k-1}d_k \leq \frac{n}{k}\frac{n}{k-1} + \frac{n}{k-1}\frac{n}{k-2} + \ldots \frac{n}{2}\frac{n}{1} = n^2\sum_{j=1}^{k-1}\frac{1}{j}\frac{1}{j+1} =$$

$$= n^2\sum_{j=1}^{k-1}\left(\frac{1}{j} - \frac{1}{j+1}\right) = n^2\left(1 - \frac{1}{k}\right) < n^2$$

b) Veja que se n é primo, $D = 1 \times n$, e assim temos que $D \mid n^2$. Suponha n composto, e seja p o seu menor fator primo. Pelo lema, $D = d_1d_2 + d_2d_3 + \ldots + d_{k-1}d_k = 1 \times p + \ldots + \frac{n}{p} \times n > \frac{n^2}{p}$

Veja então que $\frac{n^2}{p} < D < n^2$, e como $\frac{n^2}{p}$ é o maior divisor de n^2 menor que n^2, concluímos que $D \nmid n^2$

Por fim, concluímos que $D \mid n^2 \Leftrightarrow n$ é primo.

PROBLEMA 5

Encontre todas as funções f de $\mathbb{R}$ em $\mathbb{R}$ tais que

$$(f(x) + f(z))(f(y) + f(t)) = f(xy - zt) + f(xt + yz)$$

para todo $x, y, z, t \in \mathbb{R}$.

SOLUÇÃO DE LARISSA CAVALCANTE QUEIROZ DE LIMA (FORTALEZA – CE)

$(f(x) + f(z))(f(y) + f(t)) = f(xy - zt) + f(xt + yz)$

$x, z, y, t \leftarrow 0 : (2 \cdot f(0)) \cdot (2 \cdot f(0)) = 2 \cdot f(0) \Rightarrow 2 \cdot f(0)^2 = f(0)$

$f(0) \neq 0 \Rightarrow 2 \cdot f(0) = 1 \Rightarrow f(0) = \frac{1}{2}$

$z, y, t \leftarrow 0 : (f(x) + f(0))(2 \cdot f(0)) = 2 \cdot f(0)$

se $f(0) \neq 0$ (ou seja $f(0) = \frac{1}{2}$), $f(x) + f(0) = 1 \Rightarrow f(x) = 1 - \frac{1}{2} = \frac{1}{2} \forall x \in \mathbb{R}$

$\Rightarrow$ Se $f(0) \neq 0$, então $f(0) = \dfrac{1}{2}$ e $f(x) = \dfrac{1}{2}, \forall x \in \mathbb{R}$ (o que é uma solução).

Suponha então $f(0) = 0$

$z \leftarrow y; t \leftarrow x \Rightarrow [f(x) + f(y)]^2 = f(xy - xy) + f(x^2 + y^2)$

$\Rightarrow [f(x) + f(y)]^2 = f(x^2 + y^2) = f(x)^2 + 2f(x)f(y) + f(y)^2$

$z \leftarrow x; t \leftarrow y \Rightarrow (2 \cdot f(x))(2 \cdot f(y)) = f(xy - xy) + f(xy + xy)$

$\Rightarrow 4f(x) \cdot f(y) = f(2xy)$

$t, z \leftarrow 0 \Rightarrow (f(x) + f(0))(f(y) + f(0)) = f(xy - 0) + f(0 + 0)$

$\Rightarrow f(x) \cdot f(y) = f(xy)$ ***f* é multiplicativa.**

$\Rightarrow 4 \cdot f(xy) = f(2xy)$

$y \leftarrow t; t \leftarrow y \Rightarrow (f(x) + f(z))(f(t) + f(y)) = f(xt - zy) + f(xy + tz)$

$\Rightarrow f(xt - zy) + f(xy + tz) = f(xt + zy) + f(xy - zt)$

Suponhamos que *f* não seja identicamente nula (note que $f(x) \equiv 0$ é uma solução).

Suponha $f(a) < 0$ e que $\exists x, y : x^2 + y^2 = a$

$\Rightarrow f(a) = f(x^2 + y^2) = [f(x) + f(y)]^2 \geq 0$, contradição!

Assim, $f(a) \geq 0, \quad \forall a \quad \geq 0$.

$z \leftarrow -z \Rightarrow (f(x) + f(-z))(f(y) + f(t)) = f(xy + zt) + f(xt - zy)$

$= (f(x) + f(z))(f(t) + f(y))$

$\Rightarrow f(x) + f(-z) = f(x) + f(z)$

$f(-z) = f(z)$

$f(-z) = f(-1) \cdot f(z) \Rightarrow f(-1) = 1 = f(1)$.

$z, y, t \leftarrow 1 : (f(x) + 1) \cdot 2 = f(x - 1) + f(x + 1)$

$\Rightarrow 2f(x) + 2 = f(x - 1) + f(x + 1)$.

$* 4 \cdot f(xy) = f(2xy) = f(2) \cdot f(xy) \Rightarrow f(2) = 4$.

* conjectura: $f(x) = x^2$

$(x^2 + z^2)(y^2 + t^2) = (xy - zt)^2 + (xt + yz)^2$

$\Leftrightarrow x^2y^2 + x^2t^2 + z^2y^2 + z^2t^2 = x^2y^2 + z^2t^2 - 2xyzt + x^2t^2 + 2xtyz + y^2z^2$

Ok!! A função $f(x) = x^2$ funciona!!!

$2f(x) + 2 = f(x - 1) + f(x + 1) \quad (f(1) = 1; \quad f(2) = 4)$

$f(m) = m^2 \quad \forall m \leq n, m \in \mathbb{N}$.

$2 \cdot f(n) + 2 = f(n - 1) + f(n + 1)$

$\Rightarrow f(n + 1) = 2 \cdot n^2 + 2 - (n - 1)^2 = n^2 + 2n + 1 = (n + 1)^2$

$\Rightarrow f(n)=n^2, \forall n \in \mathbb{N}$.

como $f(-n)=f(n)$; temos $f(z)=z^2, \forall z \in \mathbb{Z}$.

Tome $r \in \mathbb{Q}$; $r=\dfrac{p}{q}, mdc(p,q)=1; p,q \in \mathbb{Z}, q \neq 0$

$$f(r)=f\left(\frac{p}{q}\right)=f(p)\cdot f\left(\frac{1}{q}\right)=f(p)\cdot\frac{f(1)}{f(q)}=\frac{f(p)}{f(q)}=\frac{p^2}{q^2}=(r)^2$$

$\Rightarrow f(r)=r^2, \forall r \in \mathbb{Q}$.

$(f(x)+f(r))2\cdot f(r)=f(x\cdot r+r^2)+f(x\cdot r-r^2)$

$2f(x)f(r)+2f(r)^2=f(x\cdot r+r^2)+f(xr-r^2)$

$2f(xr)+2r^4=f(xr+r^2)+f(xr-r^2) \quad \forall x \in \mathbb{R}$,

$r \in \mathbb{Q} \Rightarrow 2f(y)+2r^4=f(y+r^2)+f(y-r^2), \forall y \in \mathbb{R}, r \in \mathbb{Q}.$

Suponha que $\exists y,r$ tais que $y \geq 0$, $r>0$ e

$f(y+r^2)<f(y)$

$\Rightarrow \left[f\left(\sqrt{y}\right)+f(r)\right]^2 < f\left(\sqrt{y}\right)^2$

$\Rightarrow f\left(\sqrt{y}\right)^2+\underbrace{2f\left(\sqrt{y}\right)}_{\geq 0}\cdot\underbrace{f(r)}_{>0}+\underbrace{f(r)^2}_{>0}<f\left(\sqrt{y}\right)^2$, Absurdo!!!

$\Rightarrow f(y+r^2)>f(y) \quad \forall y \in \mathbb{R} \Rightarrow f$ é crescente em $\mathbb{R}^+$.

Vamos mostrar que f é contínua em $\mathbb{R}^+$: note que se y, $r \geq 0$, $f(y+r^2)-f(y)=$

$\Rightarrow f(\sqrt{y})^2+2f(\sqrt{y})f(r)+f(r)^2-f(y)=f(r)(2f(\sqrt{y})+f(r))=r^2(2f(\sqrt{y})+r^2)$,

se $r \in \mathbb{Q}$. Assim, dado $\varepsilon>0$, para $r_0 \in \mathbb{Q}$ suficientemente pequeno, temos

$f(y+r_0^2)-f(y)<\varepsilon.$

e se $r<r_0$, temos $f(y+r^2)-f(y)<f(y+r_0^2)-f(y)<\varepsilon$

$\Rightarrow$ se $x-y<r_0^2$ temos $f(x)-f(y)<\varepsilon (x>y)$.

* $f(y)-f(y-r_0^2)=f(y+r_0^2)-f(y)-2r_0^4<\varepsilon-2r_0^4<\varepsilon$

Se $r<r_0$ então $y-r^2>y-r_0^2 \Rightarrow f(y-r^2)>f(y-r_0^2)$

$\Rightarrow f(y)-f(y-r^2)<f(y)-f(y-r_0^2)<\varepsilon$

$\Rightarrow$ para $|x-y|<r_0^2$ temos $|f(x)-f(y)|<\varepsilon$

portanto f é contínua.

Suponha $f(w)=w^2+\theta, \theta \neq 0$

1) $\theta > 0$

Temos que $\exists r_0 > 0$ tal que

$|x - w| < r_0^2 \Rightarrow |f(x) - f(w)| < \theta$

ou seja $\left|x^2 - w^2 - \theta\right| < \theta$ caso $x \in \mathbb{Q}$

mas se $x < w$ temos $x^2 < w^2$ e portanto $w^2 - x^2 > 0$

$\Rightarrow \left|x^2 - w^2 - \theta\right| = w^2 + \theta - x^2 = \left(w^2 - x^2\right) + \theta > \theta$, contradição!!

(existe $x \in \mathbb{Q}$ tal que $0 < w - x < r_0^2$).

2) $\theta < 0 \Rightarrow f(w) = w^2 - |\theta|$

temos que $\exists r_0 > 0$ tal que

$|x - w| < r_0^2 \Rightarrow |f(x) - f(w)| < |\theta|$

ou seja $\left|x^2 - w^2 + |\theta|\right| < |\theta|$ caso $x \in \mathbb{Q}$

Note que $\exists x \in \mathbb{Q}$ tal que $0 < x - w < r_0^2$

$\Rightarrow x > w \Rightarrow x^2 > w^2 \Rightarrow \left|x^2 - w^2 + |\theta|\right| = x^2 - w^2 + |\theta| > |\theta|$ contradição!!

$\Rightarrow f(x) = x^2, \forall x \in \mathbb{R}$.

As únicas funções são:

$f(x) \equiv \frac{1}{2}$; $f(x) \equiv 0$ ou $f(x) = x^2$, $\forall x \in \mathbb{R}$.

PROBLEMA 6

Sejam $\Gamma_1, \Gamma_2, ..., \Gamma_n$ círculos de raio 1 no plano, onde $n \geq 3$. Seus centros são O_1, $O_2, \ldots, O_n$, respectivamente.

Suponha que não exista reta que intercepte mais que dois dos círculos. Prove que

$$\sum_{1 \le i < j \le n} \frac{1}{O_i O_j} \le \frac{(n-1)\pi}{4}.$$

SOLUÇÃO DE LUCIANO GUIMARÃES CASTRO (RIO DE JANEIRO – RJ)

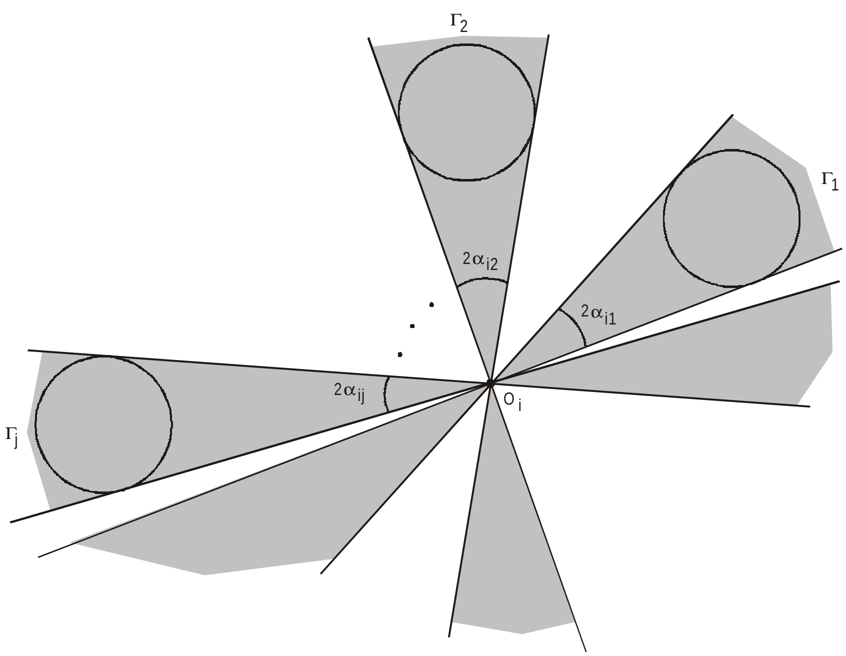
Seja α_{ij} a medida, em radianos, do ângulo agudo formado pela reta O_iO_j com uma reta tangente a Γ_j passando por O_i. As circunferências têm raio 1, e $\operatorname{sen} \alpha_{ij} \le \alpha_{ij}$, $\forall i, j \in \{1, 2, \ldots, n\}$. Assim,

$$\sum_{1 \le i < j \le n} \frac{1}{O_i O_j} = \sum_{1 \le i < j \le n} \operatorname{sen} \alpha_{ij} \le \sum_{1 \le i < j \le n} \alpha_{ij} .$$

É suficiente, portanto, provar que $\sum_{1\le i<j\le n} \alpha_{ij} \le \frac{(n-1)\pi}{4}$, o que parece menos assustador que o enunciado original.

Vejamos de que maneira a condição de nenhuma reta cortar mais de duas circunferências limita a soma dos α_{ij}. Fixemos i. Para cada j, a união de todas as retas que passam por O_i e cortam a circunferência Γ_j forma dois ângulos opostos pelo vértice O_i, cada um medindo $2\alpha_{ij}$. Como essas retas não cortam outra circunferência além de Γ_i e Γ_j, variando j obtemos ângulos disjuntos com vértice O_i, de forma que a soma de suas medidas não pode ultrapassar 2π, ou seja,

$$\sum_{\substack{1\le j\le n\\ j\ne i}} 4\alpha_{ij} \le 2\pi\,. \qquad (1)$$



Agora, somando estas desigualdades para $i \in \{1, 2, \ldots, n\}$ e observando que $\alpha_{ij} = \alpha_{ji}$, obtemos

$$\sum_{1\le i\le n} \sum_{\substack{1\le j\le n\\ j\ne i}} 4\alpha_{ij} \le \sum_{1\le i\le n} 2\pi \iff 2\sum_{1\le i<j\le n} 4\alpha_{ij} \le 2n\pi \iff \sum_{1\le i<j\le n} \alpha_{ij} \le \frac{n\pi}{4}.$$

Hummmm... quase! De fato, este resultado já é assintoticamente equivalente ao desejado. Apesar de que conseguir um $n - 1$ no lugar daquele n é a parte difícil deste problema, você vai perceber que se trata apenas de ir adaptando esta primeira idéia.

Intuitivamente, o que acabamos de fazer foi "girar" uma reta 180º em torno de cada ponto O_i, sabendo que neste percurso ela cortará todas as outras circunferências, mas nunca duas ao mesmo tempo. Para melhorar a estimativa, precisamos encontrar uma forma de girar menos que 180º e, ainda assim, encontrar todas as demais circunferências. Isto não é possível para todos os O_i, mas podemos fazê-lo com os "mais afastados".

Mais precisamente, nossa idéia é trabalhar com o fecho convexo do conjunto $\{O_1, O_2, ..., O_n\}$, ou seja, o menor conjunto convexo que contém $\{O_1, O_2, ..., O_n\}$. Sem perda de generalidade, podemos supor que esse fecho convexo é o polígono $O_1O_2O_{3...}\ O_m\ (m \le n)$. Desta forma, os pontos O_{m+1}, O_{m+2}, ..., O_n são interiores ao polígono.

Vamos separar a soma $\sum_{1\le i<j\le n} \alpha_{ij}$ em quatro partes:

$L = \sum_{1\le i\le m-1} \alpha_{i,i+1} + \alpha_{1m}$ (soma dos α_{ij} tais que O_iO_j é lado do polígono);

$D = \sum_{1\le i<j\le m} \alpha_{ij} - L$ (soma dos α_{ij} tais que O_iO_j é diagonal do polígono);

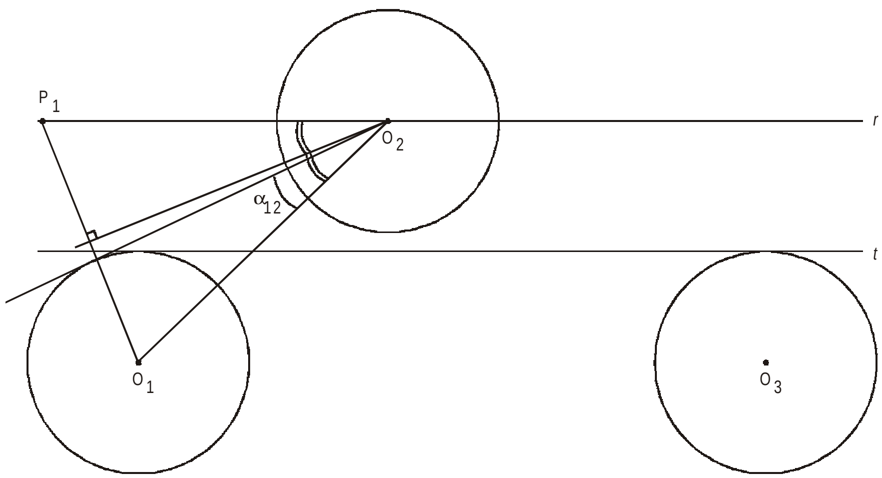
$T = \sum_{\substack{1\le i\le m \\ m<j\le n}} \alpha_{ij}$ (soma dos α_{ij} tais que O_i é vértice do polígono e O_j é interior);

$I = \sum_{m<i<j\le n} \alpha_{ij}$ (soma dos α_{ij} tais que O_i e O_j são interiores ao polígono).

Observe que $L + D + T + I = \sum_{1\le i<j\le n} \alpha_{ij}$.

Vamos usar os ângulos externos do polígono para limitar L. Sejam a_i e e_i, respectivamente, as medidas dos ângulos interno e externo do polígono no vértice O_i. Para simplificar a notação, trabalharemos com o vértice O_2. Seja t a tangente comum exterior a Γ_1 e Γ_3, mais próxima de Γ_2. Então Γ_2 está totalmente contida no semiplano determinado por t que não contém Γ_1 e Γ_3 (caso contrário existiria uma reta cortando Γ_1, Γ_2 e Γ_3). Sejam r a paralela a t por O_2 e P_1 o ponto de r tal que $\angle P_1O_2O_1$ é agudo e sua bissetriz é perpendicular à reta O_1P_1. Então a distância de O_1 a essa bissetriz é igual a $\frac{O_1P_1}{2}$. Esta distância é maior que 1, pois P_1 pertence a r e a distância de O_1 a r é maior que 2. Isto significa que a bissetriz de $\angle P_1O_2O_1$ é exterior a Γ_1, do que concluímos que $\alpha_{12} < \dfrac{m(\angle P_1O_2O_1)}{2}$. Procedendo de forma análoga com a circunferência Γ_3 e somando as duas desigualdades, temos

$$\alpha_{12} + \alpha_{23} < \frac{\pi - a_2}{2} = \frac{e_2}{2}.$$



Fazendo o mesmo para os demais vértices do polígono e somando as desigualdades obtidas, concluímos que

$$2L < \sum_{1 \le i \le m} \frac{e_i}{2} \iff 2L < \pi. \qquad (2)$$

Agora utilizaremos os ângulos internos do polígono em um procedimento parecido ao que fizemos para descobrir a desigualdade (1). Salvo Γ_1, Γ_2 e Γ_3, todas as demais circunferências estão completamente contidas no ângulo interno $\hat{O}_2 = \angle O_1O_2O_3$. Para cada $j \neq 2$, considere o conjunto união das semi-retas com origem O_2, interiores a $\hat{O}_2$, que cortam a circunferência Γ_j. Este conjunto forma um ângulo de medida α_{2j}, para $j = 1$ e $j = 3$, e um ângulo de medida $2\alpha_{2j}$ para os demais valores de j. Como cada semi-reta pode cortar apenas uma circunferência além de Γ_2, os conjuntos correspondentes a distintos valores de j são disjuntos. Assim,

$$\alpha_{12} + \alpha_{23} + 2\sum_{4 \le i \le n} \alpha_{2j} \le a_2.$$

Procedendo de forma análoga com os demais vértices do polígono e somando as desigualdades obtidas concluímos que

$$2L + 4D + 2T \le \sum_{1 \le i \le m} a_i = (m-2)\pi. \qquad (3)$$

Para concluir, seja O_i um ponto interior ao polígono, ou seja, $i > m$. Já provamos a desigualdade (1): $\sum_{\substack{1\le j\le n \\ j\ne i}} 4\alpha_{ij} \le 2\pi$.

Somando essas desigualdades para todos os pontos O_i interiores temos

$$\sum_{m<i\le n} \sum_{\substack{1\le j\le n \\ j\ne i}} 4\alpha_{ij} \le \sum_{m<i\le n} 2\pi \iff 4T + 8I \le (n-m)2\pi \iff 2T + 4I \le (n-m)\pi . \qquad (4)$$

Agora basta somar as desigualdades (2), (3) e (4), obtendo

$$2L + 2L + 4D + 2T + 2T + 4I \le \pi + (m-2)\pi + (n-m)\pi$$

$$\iff 4L + 4D + 4T + 4I \le (n-1)\pi \iff L + D + T + I \le \frac{(n-1)\pi}{4} .$$

Portanto

$$\sum_{1\le i<j\le n} \frac{1}{O_iO_j} = \sum_{1\le i<j\le n} \operatorname{sen}\alpha_{ij} \le \sum_{1\le i<j\le n} \alpha_{ij} = L + D + T + I \le \frac{(n-1)\pi}{4},$$

como queríamos demonstrar.

XVII OLIMPÍADA IBEROAMERICANA DE MATEMÁTICA

Enunciados, Soluções e Resultado Brasileiro

A XVII Olimpíada Iberoamericana de Matemática foi realizada na cidade de São Salvador, El Salvador no período de 30 de setembro a 5 de outubro de 2002.

A equipe brasileira foi liderada pelos professores Eduardo Wagner (Rio de Janeiro – RJ) e Onofre da Silva Farias (Fortaleza – CE).

O Resultado da Equipe Brasileira

BRA 1	Guilherme Camarinha Fujiwara	Ouro
BRA 2	Humberto Silva Naves	Ouro
BRA 3	Larissa Cavalcante Queiroz de Lima	Ouro
BRA 4	Yuri Gomes Lima	Prata

PRIMEIRO DIA

DURAÇÃO: 4 horas e meia.

PROBLEMA 1

Os números inteiros desde 1 até 2002, ambos incluídos, escrevem-se num quadro por ordem crescente 1, 2,..., 2001, 2002. Em seguida apagam-se os que ocupam o primeiro lugar, quarto lugar, sétimo lugar, etc, ou seja, os que ocupam os lugares da forma $3k + 1$.

Na nova lista apagam-se os números que estão nos lugares da forma $3k + 1$. Repete-se este processo até que se apagam todos os números da lista. Qual foi o último número que se apagou?

SOLUÇÃO DE GUILHERME CAMARINHA FUJIWARA (SÃO PAULO - SP)

Considere uma sequência infinita ao invés de uma sequência até 2002. Seja então $R(k)$ o primeiro número a ser apagado na k-ésima seção de apagamento.

Temos então $R(1) = 1$, $R(2) = 2$, $R(3) = 3$, $R(4) = 5$, $R(5) = 8$, $R(6) = 12$.

Queremos então achar o maior $R(k)$ menor ou igual à 2002.

Vamos provar que $R(k + 1) = \left\lceil \frac{3}{2} \cdot R(k) \right\rceil$ (onde $\lceil k \rceil$ é o menor inteiro maior ou igual a x).

Para tal, basta ver que se considerarmos a seqüência que sobra após a primeira série de apagamentos, teremos que o $R(k)$-ésimo termo será o primeiro a ser apagado na k-ésima próxima série de apagamento. Considerando também o primeiro apagamento, temos que o $R(k)$-ésimo número dessa lista sérá o primeiro a ser apagado na $(k + 1)$-ésima série de apagamento, logo será o $R(k + 1)$.

É fácil ver que o n-ésimo termo da sequência que sobra após a primeira série de apagamentos será o $\left\lceil \frac{3}{2} \cdot n \right\rceil$ (basta ver os dois casos de paridade de n), logo temos que $R(k+1) = \left\lceil \frac{3}{2} \cdot R(k) \right\rceil$.

Fazendo as contas, temos então $R(6) = 12$, $R(7) = 18$, $R(8) = 27$, $R(9) = 41$, $R(10) = 62$, $R(11) = 93$, $R(12) = 140$, $R(13) = 210$, $R(14) = 315$, $R(15) = 473$, $R(16) = 710$, $R(17) = 1065$, $R(18) = 1598$ e finalmente $R(19) = 2397$.

Como $R(18) = 1598$ e $2002 < R(19) = 2397$, então o último número apagado foi 1598.

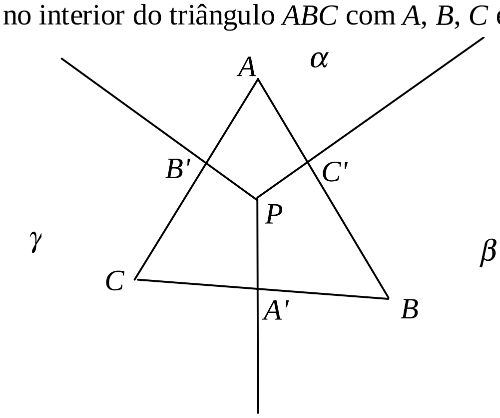
PROBLEMA 2

Dado qualquer conjunto de 9 pontos no plano entre os quais não existem três colineares, demonstre que para cada ponto P do conjunto, o número de triângulos que têm como vértices três dos oito pontos restantes e P no seu interior é par.

SOLUÇÃO DE HUMBERTO SILVA NAVES (SÃO JOSÉ DOS CAMPOS - SP)

Seja S o conjunto dos 9 pontos.

Se um ponto P está no interior do triângulo ABC com A, B, C e $P \in S$, temos:



Sejam $A' = AP \cap BC$; $B' = BP \cap AC$ e $C' = CP \cap AB$. As semi-retas PA', PB' e PC' dividem o plano em três regiões: α, β e γ ($A \in \alpha$, $B \in \beta$ e $C \in \gamma$).

Vamos construir um grafo G cujos vértices representam os triângulos (com vértices em S) com o ponto P em seu interior. Ligaremos 2 vértices deste grafo se e somente se os triângulos correspondentes tiverem um lado em comum. Vamos agora provar que o grau de cada vértice é 5.

Seja $Q \in S - \{A ; B ; C ; P\}$. Temos 3 possibilidades:

1) Se $Q \in \alpha$: Temos que o ponto P está no triângulo QBC, logo $\Delta QBC \in V(G)$. Como os triângulos ΔABC e ΔQBC tem um lado em comum, eles estão ligados por uma aresta em G. Obs.: Claro que P não está no ΔQAB e nem no ΔQAC.

2) Se $Q \in \beta$: $\Delta QAC \in V(G)$ e está ligado à ΔABC em G.

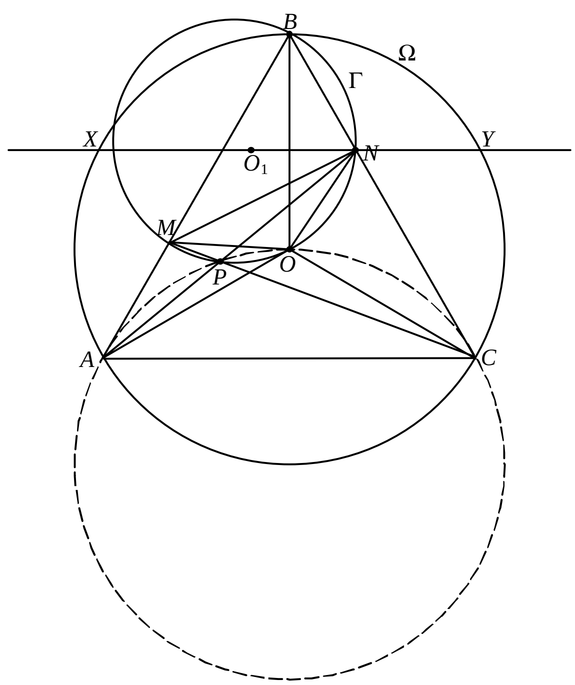
3) Se $Q \in \gamma$: $\Delta QAB \in V(G)$ e está ligado à ΔABC em G.

Logo deg $(\Delta ABC) = \#(S - \{A\ ;\ B\ ;\ C\ ;\ P\}) = 5$. E como $\Sigma\ \deg(\Delta) = 2 \times \#E(G)$
$\Rightarrow\ \#V(G)$ é par. Portanto o número de triângulos com P em seu interior é par.

PROBLEMA 3

Um ponto P é interior ao triângulo equilátero ABC e é tal que $\angle APC = 120°$. Sejam M a intersecção de CP com AB e N a intersecção de AP com BC. Encontrar o lugar geométrico do circuncentro do triângulo MBN quando P varia.

SOLUÇÃO DE YURI GOMES LIMA (FORTALEZA – CE)



Vamos mostrar que tal L.G. está contido na reta ℓ mediatriz do raio $\overline{BO}$, onde O é o centro de ABC. Para isso, seja O_1 o circuncentro de BMN. Daí, como $A\hat{P}C = 120°$, temos $N\hat{P}M = 120° \Rightarrow BNPM$ inscritível. Para O_1 pertencer a ℓ, devemos ter $\overline{BO_1} = \overline{OO_1}$, ou seja, O também deve pertencer à circunferência Γ circunscrita em $BMPN$. Vamos mostrar que O é o médio do arco MN.

Agora, veja que, como $A\hat{P}C = 120°$, temos então que $B\hat{A}N = 60° - N\hat{A}C = A\hat{C}M$. Assim, $\Delta ABN \equiv \Delta CAM$. Logo, a rotação com centro em O e ângulo $120°$ que leva B em A e A em C também leva N em M.

Assim, $N\hat{O}M = 120°$ e $\overline{NO} = \overline{MO}$. Mas sendo $N\hat{O}M = 120°$, segue que $BMON$ é inscritível. Assim, provamos o que queríamos e $O_1 \in \ell$.

Mas o LG não é a reta toda. De fato, devemos ter $O_1\hat{B}N < 90°$, pois ΔO_1BN é isósceles, daí, se X e Y são os pontos de interseção de ℓ com a circunferência Ω circunscrita a ABC, teremos que O_1 pertence ao INTERIOR do segmento $\overline{XY}$, pois $X\hat{B}C = Y\hat{B}A = 90°$ (para ver isto, observe que $XBYO$ é losango com $\overline{XO} = \overline{BO} \Rightarrow X\hat{O}B = 60° \Rightarrow X$ é o médio do arco AB).

Agora, dado O_1 pertencente ao interior do segmento $\overline{XY}$, trace a circunferência de centro O_1 e raio $\overline{O_1B}$ (que passa por O).

Ela determinará dois pontos M e N sobre $\overline{AB}$, $\overline{BC}$ tais que $O\hat{M}N = O\hat{B}N = O\hat{B}M = O\hat{N}M$ e $M\hat{O}N = 120°$. Daí, a mesma rotação considerada antes levará N em M, levando então o ΔABN no $\Delta CAM \Rightarrow \overline{AN} = \overline{CM}$ e $B\hat{A}N = A\hat{C}M \Rightarrow 60° - B\hat{A}N = 60° - A\hat{C}M \Rightarrow P\hat{A}C + A\hat{C}P = 60°$, onde $P = \overline{AN} \cap \overline{CM}$, donde $A\hat{P}C = 120°$.

Logo, o L.G. procurado é o interior do segmento $\overline{XY}$.

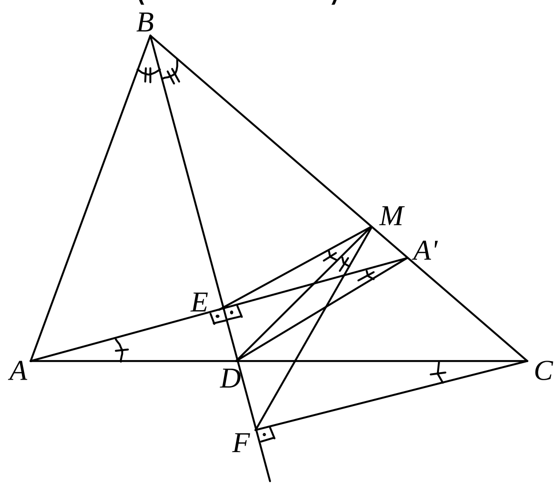
SEGUNDO DIA

DURAÇÃO: 4 horas e meia.

PROBLEMA 4

Num triângulo escaleno ABC traça-se a bissectriz interna BD, com D sobre AC. Sejam E e F, respectivamente, os pés das perpendiculares traçadas desde A e C até à recta BD, e seja M o ponto sobre o lado BC tal que DM é perpendicular a BC. Demonstre que $\angle EMD = \angle DMF$.

SOLUÇÃO DE YURI GOMES LIMA (FORTALEZA – CE)



Seja A' a interseção de $\overline{AE}$ com $\overline{BC}$. Então, como BE é bissetriz, segue que $\overline{AE} = \overline{EA'}$. Mas então os triângulos ADE e $A'DE$ são congruentes, donde $D\hat{A}E = D\hat{A}'E$ (I). Como $\overline{AE}$ e $\overline{CF}$ são perpendiculares a $\overline{BD}$, então $\overline{AE} // \overline{CF} \Rightarrow E\hat{A}D = D\hat{C}F$ (II)

Também:

$D\hat{F}C = D\hat{M}C = 90° \Rightarrow$ o quadrilátero $MCFD$ é inscritível $\Rightarrow D\hat{C}F = D\hat{M}F$.

$A'\hat{M}D = A'\hat{E}D = 90° \Rightarrow$ o quadrilátero $A'MED$ é inscritível $\Rightarrow E\hat{M}D = E\hat{A}'D$.

Mas, por (I) e (II), temos que $E\hat{A}'D = D\hat{C}F \Rightarrow$

$\Rightarrow E\hat{M}D = D\hat{M}F$.

Obs. Por ABC ser escaleno, temos que $\overline{BD}$ não é perpendicular a $\overline{AC}$, i.e,
$E \neq D \neq F \neq E$.

PROBLEMA 5

A sucessão de números reais $a_1, a_2, ...$ define-se como:

$$a_1 = 56 \quad \text{e} \quad a_{n+1} = a_n - \frac{1}{a_n} \text{ para cada inteiro } n \geq 1.$$

Demonstre que existe um inteiro $k, 1 \leq k \leq 2002,$ tal que $a_k < 0$.

SOLUÇÃO DE LARISSA CAVALCANTE QUEIROZ DE LIMA (FORTALEZA – CE)

Lema: $a_k < m; m, a_k > 0$

$\Rightarrow a_{k+1} < m - \frac{1}{m}$

Prova: $a_k < m \Rightarrow \frac{1}{m} < \frac{1}{a_k} \Rightarrow -\frac{1}{a_k} < -\frac{1}{m}$

$\Rightarrow a_k - \frac{1}{a_k} < m - \frac{1}{m} \therefore a_{k+1} < m - \frac{1}{m}$

$* \, a_{k+1} = a_k - \frac{1}{a_k} \Rightarrow a_{k+1}^2 = a_k^2 - 2a_k \cdot \frac{1}{a_k} + \frac{1}{a_k^2}$

$\Rightarrow a_{k+1}^2 = a_k^2 + \frac{1}{a_k^2} - 2$

Soma telescópica

$* \; a_2^2 = a_1^2 + \frac{1}{a_1^2} - 2$

$a_3^2 = a_2^2 + \frac{1}{a_2^2} - 2$

$(+) \; a_{k+1}^2 = a_k^2 + \frac{1}{a_k^2} - 2$

$\Rightarrow a_{k+1}^2 = a_1^2 + \frac{1}{a_1^2} + \frac{1}{a_2^2} + \ldots + \frac{1}{a_k^2} - 2 \cdot k$

1) Suponha que $\exists \; i \le 1999$ tal que $a_i < 2 (a_i > 0)$

Isso implica: $a_{i+1} < 2 - \frac{1}{2} = \frac{3}{2}$. Caso $a_{i+1} > 0$, $a_{i+2} < \frac{3}{2} - \frac{2}{3} = \frac{9-4}{6} = \frac{5}{6} < 1.$

Se $a_{i+2} > 0 \Rightarrow a_{i+3} < 1 - \frac{1}{1} = 0; i + 3 \le 1999 + 3 = 2002$

$\Rightarrow \exists k, 1 \le k \le 2002$ tal que $a_k < 0.$

2) Suponha que $\nexists \; i \le 1999$ tal que $a_i < 2$

$\Rightarrow a_i \ge 2 \;\; \forall \; 1 \le i \le 1999 \Rightarrow \frac{1}{2} \ge \frac{1}{a_i} \Rightarrow \frac{1}{4} \ge \frac{1}{a_i^2}$

$$\Rightarrow a_{2000}{}^2 = 56^2 + \frac{1}{a_1{}^2} + \ldots + \frac{1}{a_{1999}{}^2} - 2(1999) \le 56^2 + 1999 \cdot \frac{1}{4} - 2 \cdot 1999$$

$$\Rightarrow a_{2000}{}^2 \le 56^2 - 1999\left(2 - \frac{1}{4}\right) = 3136 - (2000-1)\frac{7}{4} = 3136 - 3500 + \frac{7}{4} < 0$$

Absurdo!

Portanto $\exists\, i \le 1999$ tal que $a_i < 2$

$\Rightarrow$ temos que a_i, a_{i+1}, a_{i+2} ou a_{i+3} é menor que zero (por 1)

$\therefore \exists k, 1 \le k \le 2002$ tal que $a_k < 0$.

PROBLEMA 6

Um polícia tenta capturar um ladrão num tabuleiro de 2001×2001. Eles jogam alternadamente. Cada jogador, na sua vez, deve mover-se uma casa num dos três seguintes sentidos:

$\downarrow$ (abaixo); $\longrightarrow$ (direita); $\nwarrow$ (diagonal superior esquerda).

Se o polícia se encontra na casa da esquina inferior direita, pode usar a sua jogada para passar directamente para a casa da esquina superior esquerda (o ladrão não pode fazer esta jogada). Inicialmente o polícia está na casa central e o ladrão está na casa vizinha diagonal superior direita do polícia. O polícia começa o jogo.

Demonstre que:

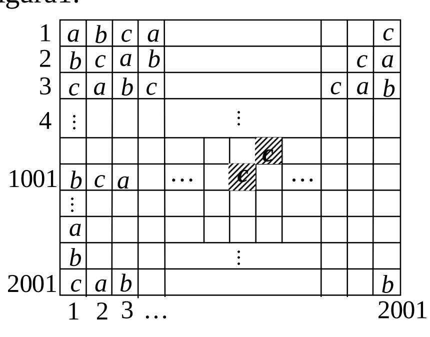
a) O ladrão consegue mover-se pelo menos 10000 vezes sem ser capturado.

b) O polícia possui uma estratégia para capturar o ladrão.

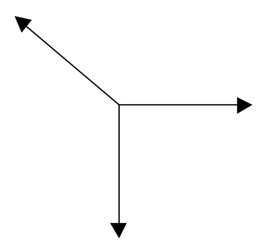
Nota: O polícia captura o ladrão quando entra na casa em que está o ladrão. Se o ladrão entra na casa do polícia, não há captura.

SOLUÇÃO OFICIAL: Pinte o tabuleiro com 3 cores da seguinte forma:

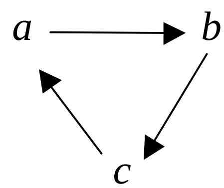
Figura1:



Movimentos



Observe que os movimentos nos dão o seguinte ciclo:



Quer dizer: de uma casa a só se vai para b, de uma b só se vai para c e de uma c só se vai para a.

Inicialmente o polícia começa numa casa c e o ladrão também.
(casas hachuradas na figura)
Assim teremos as seqüências
Polícia: $c \to a \to b \to c$

O polícia nunca poderia entrar numa casa de mesma cor do ladrão.

Ladrão: $c \to a \to b \to c$
Para sua sorte existe o túnel.
Se pensarmos um pouco, veremos que o polícia deve atravessar o túnel 2 vezes para poder tornar compatível seu ciclo com o do ladrão, ou seja, jogar e cair numa casa de mesma cor do ladrão (podendo pegá-lo).
Seja X = casa superior esquerda
Y = casa inferior direita.
Logo o polícia precisa de 2000 movimentos para chegar até Y, cruza o túnel (1 movimento), mais 4000 para chegar de novo até Y, cruza o túnel (1 movimento). Neste momento o ladrão deve estar próximo de Y e o polícia precisará de mais 3999 movimentos (pelo menos) para capturar o ladrão (que ficará rodando no quadrado 2×2 inferior esquerdo, totalizando
$2000 + 4000 + 3999 + 2 = 10001$ movimentos do polícia, ou seja, 10000 movimentos do ladrão.
b) Vejamos agora uma estratégia para que o polícia prenda o ladrão.
Suponha que ele já tenha passado 2 vezes pelo túnel.
Numere as linhas do tabuleiro de 1 a 2001, de cima para baixo e as colunas de 1 a 2001, da esquerda para a direita.
Após sair do túnel, o polícia se encontra na casa da linha 1 e coluna 1.
A estratégia é a seguinte:

i) O polícia deve se mover para a direita até que o ladrão fique na mesma diagonal (inferior direita) do polícia ou uma casa à direita.
ii) Em seguida, o polícia deve fazer o seguinte movimento:

iii) O polícia deve repetir os passos i) e ii) Note que a diferença entre os números das linhas do polícia e do ladrão sempre diminui e o ladrão sempre fica na região à direita da diagonal inferior direita do polícia.

Assim, após repetirmos i) e ii) um número finito de vezes, chegamos na situação (na vez do ladrão)

Polícia		
		Ladrão

(note que não pode ocorrer outra situação na qual a diferença entre linhas é 1, pois, na vez do ladrão, os dois devem estar em casas do mesmo tipo).
Seguindo o que é feito em ii), o ladrão, em algum momento, se move para a casa à direita do polícia. Assim, na próxima jogada, o polícia prende o ladrão.

A FÓRMULA DE CARDANO ALÉM DAS CÚBICAS

José Cloves Verde Saraiva, São Luis – MA

♦ Nível Avançado.

INTRODUÇÃO:

Motivado pela leitura do trabalho Equação do Terceiro Grau do Professor Alberto de Azevedo [1], ocorreu-me a curiosidade de saber as fórmulas das raízes calculadas por radicais de uma equação polinomial do 5° grau, solúvel, que não fosse a trivial $x^5 + a = 0$, que todos conhecem. Daí então, seguindo os mesmos passos da dedução da fórmula de Cardano para as equações polinomiais cúbicas foi possível provar que a $x^5 - px^3 + \frac{1}{5}p^2x - r = 0$, já estudada por DE MOIVRE, tem raízes dadas por uma fórmula análoga a de Cardano. Além desta, outras fórmulas semelhantes são possíveis deduzir para graus maiores que o quinto.

Deixamos para o leitor essa generalização!.

A FÓRMULA DE CARDANO:

É fascinante toda a história da resolução das equações polinomiais do 3° grau. Em resumo a referência [2] apresenta o seguinte:

"O descobridor do método foi Scipione del Ferro (1465 - ≈ 1562), matemático italiano, que antes de morrer o revelou aos discípulos Antônio Maria Fior e Annibale Della Nave".

"Houve uma disputa matemática entre Fior contra Niccolo Fontana (1500 – 1557), conhecido pelo apelido de Tartaglia (gago, em italiano). A vitória deste último, muito divulgada, foi do conhecimento do médico e professor Girolano Cardano (1501 – 1576) que conseguiu lhe atrair para ensinar a regra de resolução sob o juramento de jamais publicá-la. Cardano procurou a demonstração da regra - e achou - e ainda motivou seu discípulo Ludovico Ferrari (1522 – 1565) a descobrir solução para as equações do quarto grau."

"Cardano, numa visita a Della Nave, soube do manuscrito de Del Ferro contendo a regra de Tartaglia que já existia há 30 anos. Motivo que o levou quebrar o juramento. Publicou os métodos no seu famoso livro *Ars Magna*, em 1545, onde não deixou de fazer referência aos descobridores, embora a contragosto de Tartaglia que se considerou traído."

Podemos representar a equação geral do 3° grau na forma $x^3 + a_1x^2 + a_2x + a_3 = 0$ e por uma mudança de variável $x = y - \frac{a_1}{3}$ a equação fica mais simples na forma

$y^3 - py - q = 0$. Calculando o cubo de um binômio $(u+v)^3 = u^3 + 3u^2v + 3uv^2 + v^3$, e pondo em evidência $3uv$, temos:

$$(*)\ (u+v)^3 = 3uv(u+v) + (u^3 + v^3)$$

ou melhor,

$$(u+v)^3 - 3uv(u+v) - (u^3+v^3) = 0$$

isto é, $y = u + v$ é uma raiz para valores de $p = 3uv$ e $q = u^3 + v^3$, onde podemos elevar ao cubo a primeira e ter $\dfrac{p^3}{27} = u^3v^3$ e $q = u^3 + v^3$ e cair num problema onde u^3 e v^3 são as raízes de uma equação do 2° grau conhecendo a soma e o produto das raízes, cuja solução é conhecida:

$$u^3 = \frac{q}{2} + \sqrt{\frac{q^2}{4} - \frac{p^3}{27}} \text{ e } v^3 = \frac{q}{2} - \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}$$

donde obtemos a famosa fórmula de Cardano:

$$y = u + v = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}}$$

A FÓRMULA DE CARDANO ALÉM DAS CÚBICAS:

O resultado principal destas notas foi motivado por uma analogia da dedução na fórmula de Cardano. Vamos provar que: a equação $x^5 - px^3 + \dfrac{1}{5}p^2x - r = 0$ tem uma de suas raízes dada pela fórmula:

$$x = u + v = \sqrt[5]{\frac{r}{2} + \sqrt{\frac{r^2}{4} + \frac{p^5}{3125}}} + \sqrt[5]{\frac{r}{2} - \sqrt{\frac{r^2}{4} + \frac{p^5}{3125}}}$$

DEMONSTRAÇÃO:

Considere $x^5 - px^3 - qx - r = 0$. Calculemos polinômios do binômio:

$$(u+v)^5 = u^5 + 5u^4v + 10u^3v^2 + 10u^2v^3 + 5uv^4 + v^5$$

pondo em evidência obtemos:

$$(u+v)^5 = 5uv(u^3+v^3) + 10u^2v^2(u+v) + (u^5+v^5)$$

da igualdade (*) obtemos que:

$$(u^3+v^3) = (u+v)^3 - 3uv(u+v)$$

para substituir no desenvolvimento donde obtemos que:

$$(u+v)^5 = 5uv(u+v)^3 - 15u^2v^2(u+v) + 10u^2v^2(u+v) + (u^5+v^5),$$

isto é,

$$(u+v)^5 = 5uv(u+v)^3 - 5u^2v^2(u+v) + (u^5+v^5)$$

o que permite obter as igualdades: $p = 5uv$; $q = -5u^2v^2$ e $r = u^5 + v^5$.

Estabelecemos $p^2 = 25u^2v^2$, logo temos que $q = -\dfrac{p^2}{5}$ faz com que a equação seja da forma $x^5 - px^3 + \dfrac{1}{5}p^2x - r = 0$, se $x = u + v$ for uma raiz.

Verificar as relações $\begin{cases} r = u^5 + v^5 \\ p = 5uv \end{cases}$ nos leva ao já estudado na dedução da fórmula de Cardano $r = u^5 + v^5$ e $\left(\dfrac{p}{5}\right)^5 = u^5v^5$, da mesma forma as raízes são:

$$u^5 = \frac{r}{2} + \sqrt{\frac{r^2}{4} - \frac{p^5}{5^5}} \text{ e } v^5 = \frac{r}{2} - \sqrt{\frac{r^2}{4} - \frac{p^5}{5^5}}$$

de onde concluímos que a raiz $x = u + v$ é dada pela fórmula:

$$x = \sqrt[5]{\frac{r}{2} + \sqrt{\frac{r^2}{4} - \frac{p^5}{3125}}} + \sqrt[5]{\frac{r}{2} - \sqrt{\frac{r^2}{4} - \frac{p^5}{3125}}}\ .$$

OBSERVAÇÕES FINAIS:

Esta fórmula torna mais fácil a determinação das raízes do que a indicada por De Moivre estudada na referência [3], onde uma análise completa das raízes e o estudo dos Grupos de Galois nos diversos casos é feito.

Como exercício estude a sétima $x^7 + px^5 - qx^3 + rx + s = 0$ e generalize.

Finalizando, seria interessante o leitor paciente calcular todas as raízes da equação abaixo estudada por Adriaan van Roomen (1561 – 1615) por polinômios trigonométricos.

$$\begin{aligned} &x^{45} - 45x^{43} + 945x^{41} - 12300x^{39} + 111150x^{37} - 740259x^{35} + 3764565x^{33} - \\ &- 14945040x^{31} + 46955700x^{29} - 117679100x^{27} + 236030652x^{25} - 378658800x^{23} + \\ &+ 483841800x^{21} - 488494125x^{19} + 384942375x^{17} - 232676280x^{15} + 105306075x^{13} - \\ &- 34512075x^{11} + 7811375x^9 - 1138500x^7 + 95634x^5 - 3795x^3 + 45x = \sqrt{2+\sqrt{2}} \end{aligned}$$

(Ver referência [4], pp 154).

REFERÊNCIAS:

[1] Alberto de Azevedo, *Equação do 3º grau*, Depto. Matemática, UNB, 2002.
[2] César Polcino Milies, *A Resolução das equações de terceiro e quarto graus*, Notas de aula, IME-USP, 2000.
[3] R.L. Borger, *On De Moivre' s Quintic*, *American Math. Monthly*, pp. 171 - 174, vol. 15, 1908.
[4] Paulo A. Martin, *Introdução à Teoria dos Grupos e a Teoria de Galois*, IME-USP, 1996.

RECIPROCIDADE QUADRÁTICA

Carlos Gustavo T. de A. Moreira & Nicolau C. Saldanha, Rio de Janeiro - RJ

♦ Nível Avançado.

A lei de Gauss de reciprocidade quadrática afirma que se p e q são primos há uma relação direta entre p ser quadrado módulo q e q ser quadrado módulo p. Este teorema fornece um rápido algoritmo para determinar se a é quadrado módulo p onde a é um inteiro e p um número primo. Lembramos que a é quadrado módulo n se existe $x \in \mathbb{Z}$ com $x^2 \equiv a(\text{mod } n)$. Este artigo foi adaptado de [3].

Definição: Seja p um primo e a um inteiro. Definimos o símbolo de Lagrange $\left(\dfrac{a}{p}\right)$ por

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ se } p \text{ divide } a \\ -1 \text{ se } a \text{ não é quadrado módulo } p \\ 1 \text{ se } p \text{ não divide } a \text{ e } a \text{ é quadrado módulo } p. \end{cases}$$

Proposição: Seja p um primo ímpar e $a \in \mathbb{Z}$ tal que p não divide a.

Então $\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\text{mod } p)$.

Demonstração: Sabemos que se p não divide a então $a^{p-1} \equiv 1(\text{mod } p)$, ou seja, $x^{p-1} - 1$ tem como raízes $1, 2, \ldots, p - 1$ em $\mathbb{Z}/p\mathbb{Z}$. Por outro lado, $x^{p-1} - 1 = \left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right)$. Se existe $b \in \mathbb{Z}$ tal que $a \equiv b^2 (\text{mod } p)$ então $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1(\text{mod } p)$; ou seja, $\left(\dfrac{a}{p}\right) = 1 \equiv a^{\frac{p-1}{2}} (\text{mod } p)$.

Como $x^2 \equiv y^2 (\text{mod } p) \Leftrightarrow x \equiv \pm y(\text{mod } p)$, há pelo menos $\dfrac{p-1}{2}$ quadrados em $(\mathbb{Z}/p\mathbb{Z})^*$, logo os quadrados são exatamente as raízes de $x^{\frac{p-1}{2}} - 1$ em $\mathbb{Z}/p\mathbb{Z}$, donde os não quadrados são exatamente as raízes de $x^{\frac{p-1}{2}} + 1$, ou seja, se $\left(\dfrac{b}{p}\right) = -1$ então $b^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$.

Corolário: Se p é primo ímpar então $\left(\dfrac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

Vamos agora reinterpretar a proposição. Seja $a\in(\mathbb{Z}/p\mathbb{Z})^*$. Para cada $j=1,2,\ldots,\dfrac{p-1}{2}$ escrevemos $a\cdot j$ como $\varepsilon_j m_j$ com $\varepsilon_j\in\{-1,1\}$ e $m_j\in\left\{1,2,\ldots,\dfrac{p-1}{2}\right\}$. Se $m_i=m_j$ temos $a\cdot i=a\cdot j$ ou $a\cdot i=-a\cdot j$; a primeira possibilidade implica $i=j$ e a segunda é impossível. Assim, se $i\neq j$ temos $m_i\neq m_j$ donde $\left\{m_1;m_2;\ldots;m_{\frac{p-1}{2}}\right\}=\left\{1,2,\ldots,\dfrac{p-1}{2}\right\}$. Assim,

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}=\frac{(a\cdot 1)(a\cdot 2)\ldots\left(a\cdot\dfrac{p-1}{2}\right)}{1\cdot 2\cdot\ldots\cdot\dfrac{p-1}{2}}\equiv$$

$$\equiv\frac{\varepsilon_1\varepsilon_2\ldots\varepsilon_{\frac{p-1}{2}}m_1\cdot m_2\cdot\ldots\cdot m_{\frac{p-1}{2}}}{1\cdot 2\cdot\ldots\cdot\dfrac{p-1}{2}}=\varepsilon_1\varepsilon_2\ldots\varepsilon_{\frac{p-1}{2}}\ (\mathrm{mod}\ p)$$

donde $\left(\dfrac{a}{p}\right)=\varepsilon_1\varepsilon_2\ldots\varepsilon_{\frac{p-1}{2}}$, pois ambos pertencem a $\{-1,1\}$. Assim, $\left(\dfrac{a}{p}\right)=(-1)^m$, onde m é o número de elementos j de $\left\{1,2,\ldots,\dfrac{p-1}{2}\right\}$ tais que $\varepsilon_j=-1$. Como primeira conseqüência deste fato temos o seguinte resultado.

Proposição: Se p é um primo ímpar então

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, & \text{se } p\equiv\pm1\ (\mathrm{mod}\ 8),\\ -1, & \text{se } p\equiv\pm3\ (\mathrm{mod}\ 8).\end{cases}$$

Demonstração: Se $p\equiv1(\mathrm{mod}\ 4)$, digamos $p=4k+1$, temos $\dfrac{p-1}{2}=2k$. Como $1\le 2j\le\dfrac{p-1}{2}$ para $j\le k$ e $\dfrac{p-1}{2}<2j\le p-1$ para $k+1\le j\le 2k$, temos

$$\left(\frac{a}{p}\right)=(-1)^k=\begin{cases}1, & \text{se } p\equiv1\ (\mathrm{mod}\ 8),\\ -1, & \text{se } p\equiv5\ (\mathrm{mod}\ 8).\end{cases}$$

Se $p \equiv 3 (\text{mod } 4)$, digamos $p = 4k + 3$, temos $\dfrac{p-1}{2} = 2k + 1$. Para $1 \le j \le k$ temos $1 \le 2j \le \dfrac{p-1}{2}$ e para $k + 1 \le j \le 2k + 1$ temos $\dfrac{p-1}{2} < 2j \le p - 1$, donde

$$\left(\frac{a}{p}\right) = (-1)^{k+1} = \begin{cases} -1, & \text{se } p \equiv 3 \pmod 8, \\ 1, & \text{se } p \equiv 7 \pmod 8. \end{cases}$$

Teorema: (Lei de reciprocidade quadrática) Sejam p e q primos ímpares.
Então $\left(\dfrac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \left(\dfrac{q}{p}\right)$.

Demonstração: Na notação acima, com $a = q$, para cada $j \in P$, onde

$$P = \{1, 2, \ldots, (p-1)/2\},$$

temos que $\varepsilon_j = -1$ se e só se existe $y \in \mathbb{Z}$ tal que $-(p-1)/2 \le qj - py < 0$. Tal y deve pertencer a Q, onde $Q = \{1, 2, \ldots, (q-1)/2\}$.

Assim, temos que $\left(\dfrac{q}{p}\right) = (-1)^m$ onde $m = |X|$ e

$$X = \{(x, y) \in P \times Q \mid -(p-1)/2 \le qx - py < 0\};$$

note que $qx - py$ nunca assume o valor 0. Analogamente, $\left(\dfrac{p}{q}\right) = (-1)^n$, onde $n = |Y|$

$$\text{e } Y = \{(x, y) \in P \times Q \mid 0 < qx - py \le (q-1)/2\}.$$

Daí segue que $\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right) = (-1)^k$ onde $k = m + n = |Z|$ onde

$$Z = \{(x, y) \in P \times Q \mid -(p-1)/2 \le qx - py \le (q-1)/2\}$$

pois $qx - py$ nunca assume o valor 0. Temos $k = |C| - |A| - |B|$ onde $C = P \times Q$,

$$A = \{(x, y) \in C \mid qx - py < -(p-1)/2\},$$

$$B = \{(x, y) \in C \mid qx - py > (q-1)/2\}.$$

Como $|C| = (p-1)(q-1)/4$, basta mostrar que $|A| = |B|$. Mas $f: C \to C$ definida por $f(x, y) = (((p+1)/2) - x, ((q+1)/2) - y)$ define uma bijeção entre A e B $\square$

Exemplo: Se $n \geq 1$ e $p = 2^{2^n} + 1$ é primo, então 3 não é quadrado módulo *p* (e logo 3 é raiz primitiva módulo *p*; ver [1]).

De fato, como $p \equiv 1 (\text{mod } 4), \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$, mas $2^{2^n} \equiv 1 (\text{mod } 3)$, como pode ser facilmente mostrado por indução, donde $p = 2^{2^n} + 1 \equiv 2 (\text{mod } 3)$, e $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1.$

REFERÊNCIAS:

[1] Carlos Gustavo T. de A. Moreira, *Divisibilidade, Congruências e Aritmética módulo n,* Eureka! N^{o}. 2, pp. 41-52, 1998.

[2] Guilherme Camarinha Fujiwara, *Inteiros de Gauss e Inteiros de Eisenstein, Eureka! N^{o}*. 14, pp. 23-31, 2002.

[3] Carlos Gustavo T. de A. Moreira e Nicolau C. Saldanha, *Primos de Mersenne (e outros primos muito grandes),* 22^{o}. Colóquio Brasileiro de Matemática, IMPA, 1999.

APLICAÇÕES DE PLANOS PROJETIVOS EM TEORIA DOS NÚMEROS E COMBINATÓRIA

Carlos Yuzo Shine, São Paulo - SP

♦ Nível Avançado.

1. Definição de plano projetivo

A definição dada aqui é a mais geral. Dizemos que um conjunto S é um *plano projetivo* se existem subconjuntos $\ell_1, \ell_2, \ldots$ de S que satisfazem as seguintes propriedades:

(i) Se P e Q pertencem a S, um e somente um dos subconjuntos ℓ_i contém P e Q.

(ii) A interseção de ℓ_i e ℓ_j consiste sempre de um único elemento, para todo $i \neq j$.

(iii) Existem pelo menos quatro elementos de S tais que, entre eles não haja três contidos em um dos conjuntos ℓ_i.

Os elementos de S são normalmente chamados pontos e os subconjuntos ℓ_i, retas. Note que a propriedade (i) pode ser entendida como "por dois pontos passa uma única reta" e a propriedade (iii) nos diz que "existem quatro pontos, três a três não colineares".

Exercícios

01. Um torneio de tênis é disputado entre duas equipes. Cada membro de uma equipe joga com um ou mais membros da outra equipe, de modo que

(i) Dois membros de uma mesma equipe têm exatamente um oponente em comum;

(ii) Não existem dois membros de uma equipe que enfrentam, juntos, todos os membros da outra equipe.

Prove que cada jogador deve jogar um mesmo número de partidas.

02. Mostre que as seguintes proposições são equivalentes em planos projetivos:

(1) Existe uma reta que passa por exatamente $n + 1$ pontos;
(2) Existe um ponto que está contido em exatamente $n + 1$ retas;
(3) Todas as retas passam por exatamente $n + 1$ pontos;
(4) Todos os pontos estão contidos em exatamente $n + 1$ retas;
(5) Há exatamente $n^2 + n + 1$ retas;
(6) O plano projetivo tem exatamente $n^2 + n + 1$ pontos (diz-se nesse caso que o plano projetivo tem ordem n).

03. (Cone Sul 1998) O prefeito de uma cidade deseja estabelecer um sistema de transportes com pelo menos uma linha de ônibus, no qual:

(i) cada linha passe exatamente por três paradas;

(ii) cada duas linhas distintas tenham exatamente uma parada em comum;

(iii) para cada duas paradas de ônibus distintas exista exatamente uma linha que passe por ambas.

Determine o número de paradas de ônibus da cidade.

Dica: com o que parecem as condições (ii) e (iii)? Para encontrar os possíveis valores, faça uma contagem dupla.

2. Construção de planos projetivos baseados em corpos

Seja K um corpo (ou seja, um conjunto onde estão definidas duas operações, + e ·, tal que todo elemento admite oposto e todo elemento não nulo admite inverso). Então o conjunto $P_2(K)$ de ternas $(x, y, z) \neq (0, 0, 0)$, $x, y, z \in K$, onde ternas da forma (x, y, z) e (kx, ky, kz) devem ser consideradas iguais, é um plano projetivo na qual a reta correspondente ao ponto (a, b, c), reta dual de (abc), é o conjunto de pontos (x, y, z) que satisfazem

$$ax + by + cz = 0$$

Demonstração

Basta mostrar que o conjunto dado tem as propriedades (i), (ii) e (iii).

(i) Sejam (x_1, y_1, z_1) e (x_2, y_2, z_2) pontos distintos, ou seja, tais que não existe $\lambda \in K$ tal que $(x_1, y_1, z_1) = \lambda(x_2, y_2, z_2)$. Temos que mostrar que existe somente uma reta que contém ambos os pontos, ou seja, que existe uma única terna (a, b, c) (que são os coeficientes da reta) tal que

$$\left|\begin{array}{l} ax_1 + by_1 + cz_1 = 0 \\ ax_2 + by_2 + cz_2 = 0 \end{array}\right. \qquad (*)$$

Vejamos (*) como um sistema em a, b e c.

Como $(x_1, y_1, z_1) \neq \lambda(x_2, y_2, z_2)$ para todo $\lambda \in K$, a matriz completa $C = \begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{pmatrix}$ do sistema (*) tem posto 2. Suponhamos, sem perda de generalidade, que $\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} \neq 0.$ Logo, resolvendo (*) em a e b, obtemos (verifique!) $a = mc$ e $b = nc$, onde m e n são constantes de K. Logo, as soluções de (*) são da forma $(mc, nc, c) = c(m, n, 1)$. Note que $c \neq 0$ pois $c = 0$ implicaria $a = b = c = 0$. Assim, no plano projetivo $P_2(K)$, todas as soluções são equivalentes, ou seja, é única. Logo existe somente uma reta que passa por esses dois pontos.

(ii) Análogo ao item (i). Tente você fazer!

(iii) Observe que (1, 1, 1), (1, 0, 0), (0, 1, 0) e (0, 0, 1) satisfazem essas condições. Aqui, 0 e 1 são os elementos neutros da soma e produto em K, respectivamente.

3. Dualidade

Observe que se r e s são retas duais dos pontos $R = (a, b, c)$ e $S = (d, e, f)$ de $P_2(K)$, respectivamente, então

$$R \in s \Leftrightarrow da + eb + fc = 0 \Leftrightarrow ad + be + cf = 0 \Leftrightarrow S \in r$$

A propriedade $R \in s \Leftrightarrow S \in r$ é a chave do *princípio da dualidade*. Por isso, pontos e retas no plano projetivo se comportam de maneira semelhante quando se fala de incidência.

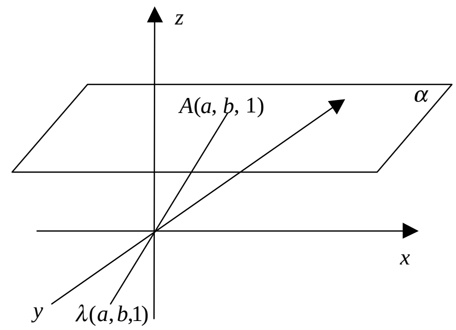
4. O caso $K = \mathbb{R}$

Quando $K = \mathbb{R}$, temos o plano projetivo $P_2(\mathbb{R})$ visto na referência [2]. Vamos entender a semelhança entre o plano definido aqui e o plano estudado em [2] (se você não leu essa referência, você pode pular essa seção; mas leia o artigo, ele realmente vale muito a pena!!).

Primeiro, vamos explicar a primeira "estranheza" do plano projetivo $P_2(\mathbb{R})$. Por que ele tem três coordenadas, e não duas? A coordenada adicional é que faz aparecerem pontos e retas no infinito. Podemos fazer a seguinte correspondência: o ponto (x, y) do plano $\mathbb{R}^2$ corresponde ao ponto $(x, y, 1)$ de $P_2(\mathbb{R})$. Sobraram os pontos do tipo $(x, y, 0)$ de $P_2(\mathbb{R})$, que são os pontos do infinito.

A reta $ax + by + c = 0$ de $\mathbb{R}^2$ pode ser transformada na reta $ax + by + cz = 0$ de $P_2(\mathbb{R})$ substituindo-se x e y na reta de $\mathbb{R}^2$ por x/z e y/z. Aqui, nós *homogeneizamos* a equação $ax + by + c = 0$.

Você pode visualizar a correspondência que fizemos da seguinte forma: se imaginarmos as ternas (x, y, z) como pontos no espaço, percebemos que os pontos de $P_2(\mathbb{R})$ correspondem a retas que passam pela origem. Se tomarmos o plano $\alpha : z = 1$ de $\mathbb{R}^3$, por exemplo, fazemos corresponder um ponto de $P_2(\mathbb{R})$ com o traço da reta correspondente nesse plano.



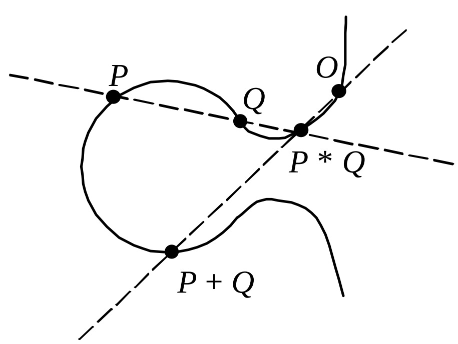
A reta dual de (a, b, c) corresponderia ao traço do plano $ax + by + cz = 0$ em π.
Com alguns cálculos verifica-se que se $R = (a, b, c)$ e r: $ax + by + cz = 0$, então, sendo $O = (0, 0, 1)$, R' e r'os respectivos correspondentes ao ponto R e à reta r em α, então $OR' \perp r'$.

4.1. O plano projetivo e curvas elípticas

Considere a curva cúbica de R^2

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0, \qquad (**)$$

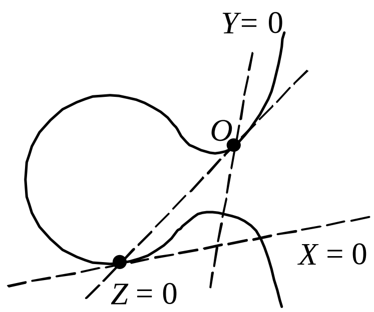
onde todas as letras de a a j são números racionais.
Gigantesco, não? Estamos interessados em saber sobre os seus pontos racionais (isto é, pontos cujas coordenadas são ambas racionais). Para isso, é feita a seguinte operação: tomamos um ponto racional da curva, denominado O. Dados dois pontos P e Q racionais da curva, encontre o terceiro ponto $P * Q$ de interseção de PQ com a curva. Defina $P + Q$ (isso mesmo, estamos somando pontos!) como o terceiro ponto de interseção da reta que passa por O e $P * Q$ com a curva (isto é, $P + Q = O * (P * Q)$). Pode-se provar que $P + Q$ também é um ponto racional.



Só que a gigantesca equação (**) pode ser simplificada para a forma

$$y^2 = x^3 + ax^2 + bx + c, \quad (\star)$$

que é bem mais simples. Esta é a forma de *Weierstrass*. Para isso, usamos a geometria projetiva.
Vamos fazer um caso particular. Considere a curva $u^3 + 2v^3 = 2uv + 1$. Um de seus pontos racionais é (1; 1).
Primeiro devemos homogeneizar a curva. Fazendo $u = U/W$, obtemos $U^3 + 2V^3 = 2UVW + W^3$. Note que agora vamos trabalhar no plano projetivo $P_2(\mathbb{R})$.
Depois, escolhemos um ponto racional O na curva. Uma escolha é $O = (1; 1; 1)$.
Agora, nós vamos mudar as coordenadas. A tangente à curva pelo ponto O é o nosso eixo de equação $Z = 0$. Se a tangente encontra a curva novamente em P (isso sempre ocorre se O não for ponto de inflexão), o eixo de equação $X = 0$ é a tangente à curva que passa por P. O eixo de equação $Y = 0$ pode ser qualquer reta que passe por O. Se O for ponto de inflexão, podemos escolher qualquer reta que não passa por O como o eixo $X = 0$. Observe que como $P_2(\mathbb{R})$ tem três coordenadas, precisamos de três eixos.



Fazendo algumas contas (use um pouquinho de cálculo; para trabalhar só com duas variáveis, "desomogenize" - essa palavra existe? - a equação), obtemos que a tangente a $O = (1; 1; 1)$ é a reta $U + 4V - 5W = 0$. Esta reta corta novamente a curva em (–3; 2; 1). A tangente por esse ponto (use cálculo novamente) é $23U + 30V + 9W = 0$. Por fim, tomamos a reta $U - V = 0$ como o eixo $Y = 0$. Assim, queremos que

$$\begin{vmatrix} U + 4V - 5W & = Z \\ 62U - 62V & = Y \\ 23U + 30V + 9W & = X \end{vmatrix} \Leftrightarrow \begin{vmatrix} U = \dfrac{5X + 3Y + 9Z}{310} \\ V = \dfrac{5X - 2Y + 9Z}{310} \\ W = \dfrac{5X - Y - 53Z}{310} \end{vmatrix}$$

(usamos $Y = 62U - 62V$ para simplificar um pouco as contas).
Substituindo U, V e W (veja que o 310 dos denominadores vai cancelar), temos

$$(5X+3Y+9Z)^3+2(5X-2Y+9Z)^3=2(5X+3Y+9Z)\cdot(5X-2Y+9Z)\cdot$$
$$(5X-Y-53Z)+(5X-Y-53Z)^3$$

A equação parece mais gigantesca que antes, mas após "desomogeneizar" (basta substituir Z = 1) e abrir tudo (eu colocaria as contas, mas a margem neste artigo é muito pequena para isso) obtemos

$$xy^2-(4x-30)y=-25x^2+96x-515$$

Em geral, quando fazemos essa mudança de eixos (a transformação que fizemos ao resolver o sistema é uma *transformação projetiva*) a equação se reduz à forma

$$xy^2+(ax+b)y=cx^2+dx+e$$

Multiplicando por x nos dois membros, temos $(xy)^2+(ax+b)xy=cx^3+dx^2+ex$

Agora substitua $z = xy$: $z^2+(ax+b)z=cx^3+dx^2+ex$

Completando quadrado no primeiro membro e substituindo $z+\frac{1}{2}(ax+b)$ por t chegamos finalmente em t^2 = cúbica em x

Para a cúbica ser mônica (ou seja, ter coeficiente dominante unitário e não ser dentuça), como o coeficiente dominante é c, basta multiplicar ambos os membros por c^2 e fazer as substituições (são as últimas!) $t = m/c$ e $x = n/c$. Vamos fazer isso no nosso exemplo.

Multiplicando por x, fazendo $z = xy$ e completando quadrado:

$$z^2-(4x-30)z+(2x-15)^2=-25x^3+96x^2-515x+(2x-15)^2$$
$$\Leftrightarrow (z-2x+15)^2=-25x^3+100x^2-575x+225$$

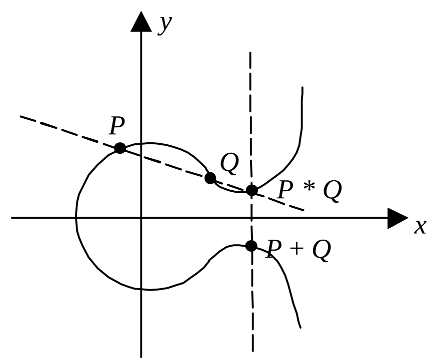
Agora, $t = z - 2x + 15$: $t^2=-25x^3+100x^2-575x+225$

Por fim, $t=-\dfrac{m}{25}$ e $x=-\dfrac{n}{25}$ e chegamos à forma de Weierstrass:

$$m^2=n^3+100n^2+14375n+140625$$

Se você escrever m e n em função de u e v (e vice-versa), vai obter funções racionais (isto é, o quociente de dois polinômios) com todos os coeficientes racionais. Logo pontos racionais são transformados em pontos racionais, de modo que achar os pontos racionais da curva original é a mesma coisa que achar os pontos racionais da curva na forma de Weierstrass (fora, é claro, os pontos que anulam os denominadores das funções racionais, que não são muitos e são fáceis de achar).

Qual a vantagem da forma de Weierstrass? A vantagem é que podemos normalizar a curva para a forma (✯), além da soma de pontos. O ponto O pode ser um ponto infinito, por exemplo. Homogeneizando (✯), obtemos $Y^2Z=X^3+aX^2Z+bXZ^2+cZ^3$, e não é difícil ver que o ponto do infinito (0; 1; 0) pertence à curva (e além disso, é o único!). Então podemos fazer $O = (0;\ 1;\ 0)$. Isso facilita um pouco as contas para adição de pontos. Se $P * Q = (a;\ b)((a;\ b;\ 1)$ no plano projetivo), a reta que passa por O e $P * Q$ é $Y = bZ$, ou $y = b$. Conseqüentemente, como a curva é simétrica em relação ao eixo Ox, temos $P + Q = (a;\ –b)$.



Exercícios

04. Prove que se P e Q são pontos racionais numa cúbica então $P + Q$ também é racional.

05. Transforme a cúbica $u^3 + v^3 = \alpha$ na forma de Weierstrass (um ponto racional da curva homogeneizada é (1; –1; 0) e a conta não é tão terrível assim).

06. (OBM 2002, nível U) Considere a curva $C = \{(x; y) \in R^2 \mid y^2 = x^3 - 43x + 166\}$.

(a) Seja $Q = (a;\ b)$ um ponto de C. Suponha que a reta tangente a C no ponto Q intersecte C num único outro ponto, Q'. Determine as coordenadas de Q'.

(b) Seja $P_0 = (3;\ 8)$. Para cada inteiro não negativo n, definimos $P_{n+1} = P'_n$, o ponto de interseção de C com a reta tangente a C em P_n. Determine P_{2002}.

07. A adição de pontos é definida somente quando a cúbica no segundo membro de (✯) tem três raízes distintas (não necessariamente todas reais). Os outros casos são mais fáceis!

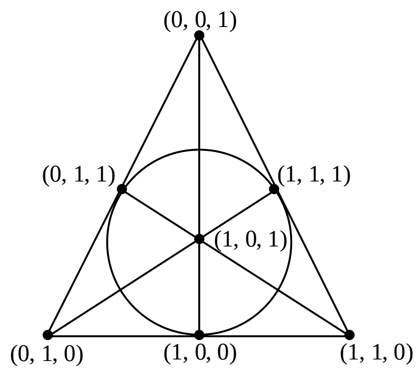
(a) Encontre todos os pontos racionais da curva $y^2 = x^2\,(x - 1)$.

(b) Encontre todos os pontos racionais da curva $y^2 = x^3$.

5. O caso $K = \mathbb{Z}/p\mathbb{Z}$

Sendo K qualquer corpo, podemos tomar $K = \mathbb{Z}/p\mathbb{Z}$ (os inteiros vistos mod p), em que p é um primo. Nesse caso, sendo $\mathbb{Z}/p\mathbb{Z}$ um corpo finito (com p elementos) o plano projetivo $P_2(\mathbb{Z}/p\mathbb{Z})$ é finito.

Por exemplo, fazendo $p = 2$, obtemos o plano de Fano (rimou!), como pode ser visto na figura.



Vamos fazer algumas continhas.

6. Algumas contagens

6.1. Número de elementos de $P_2(\mathbb{Z}/p\mathbb{Z})$

Temos $p^3 - 1$ ternas $(a, b, c) \neq (0, 0, 0)$. Como (a, b, c) é equivalente a $\lambda(a,b,c)$ e λ pode assumir $p - 1$ valores (1 a $p - 1$), cada ponto está sendo contado $p - 1$ vezes. Logo $P_2(\mathbb{Z}/p\mathbb{Z})$ tem $\dfrac{p^3-1}{p-1} = p^2 + p + 1$ pontos.

Observe que, pelo princípio da dualidade, há também $p^2 + p + 1$ retas.

6.2. Número de pontos em cada reta

Fixados a, b, e c, não todos nulos, queremos contar o número de soluções não equivalentes $(x, y, z) \neq (0, 0, 0)$ da congruência

$$ax + by + cz \equiv 0 \pmod{p} \qquad (***)$$

Suponhamos, sem perda de generalidade, que $c \neq 0 \pmod{p}$. Temos então

$$(***) \qquad \Leftrightarrow z \equiv -ac^{-1}x - bc^{-1}y \pmod{p}$$

Podemos escolher x e y de p^2 maneiras. Porém, não podemos escolher $x = y = 0$, pois isso implicaria $z = 0$. Logo, considerando que cada elemento de $P_2(\mathbb{Z}/p\mathbb{Z})$ tem $p - 1$ equivalentes, temos que cada reta tem $\frac{p^2-1}{p-1} = p+1$ pontos.

6.3. Número de retas que passam por um ponto

Pelo princípio da dualidade, há $p + 1$ retas que passam por um ponto dado.

7. Um problema

A seguir, o problema 3 da Olimpíada Iberoamericana de 1996, realizada na Costa Rica.

Temos um tabuleiro quadriculado de $k^2 - k + 1$ *linhas e* $k^2 - k + 1$ *colunas, onde* $k = p + 1$ e *p é um número primo. Para cada primo p, dê um método para distribuir números* 0 *e* 1, *um número em cada casa do tabuleiro, de modo que em cada linha haja exatamente k números 0, em cada coluna haja exatamente k números 0 e, além disso, não haja nenhum retângulo, de lados paralelos aos lados do tabuleiro, com números 0 em seus quatro vértices.*

Resolução

Para $k = p+1, k^2 - k + 1 = (p+1)^2 - (p+1) + 1 = p^2 + p + 1$ (coincidência? destino? ou puramente sorte?). Assim, devemos preencher um tabuleiro $(p^2 + p + 1) \times (p^2 + p + 1)$ com 0 e 1 de modo que haja $p + 1$ (que coisa…) 0 em cada linha e coluna, e sem retângulos com 0 vértices.

Considere o plano projetivo $P_2(\mathbb{Z}/p\mathbb{Z})$ (por que será?) e a cada linha associe um ponto e a cada coluna associe uma reta. Coloque 0 na casa (i, j) se, e somente se, o ponto i pertence à reta j. Nas demais casas, coloque 1.

Há claramente $p + 1$ zeros em cada coluna. Pelo princípio da dualidade, também há $p + 1$ zeros em cada linha.

Agora, suponha que exista um retângulo de vértices (a, c), (a, d), (b, c) e (b, d), $a \neq b$ e $c \neq d$, todos com 0. Logo, pela nossa construção, os pontos a e b pertencem a ambas as retas c e d. Absurdo, pois a interseção de duas retas é exatamente um ponto.

É claro que na prova você teria que demonstrar todas as propriedades que demonstramos antes.

8. Outros fatos sobre planos projetivos finitos

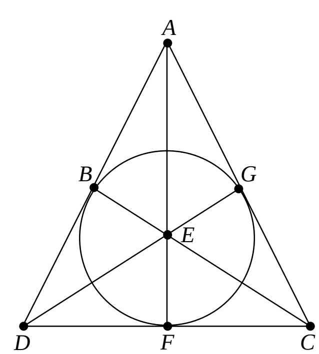
A construção baseada em corpos vale para qualquer corpo. Mas infelizmente, o número de elementos de um corpo finito deve ser potência de primo (um corpo com

p^n elementos, p primo, n inteiro positivo, é o conjunto dos polinômios com coeficientes em $\mathbb{Z}/p\mathbb{Z}$, vistos módulo um polinômio $P(x)$ de grau n e irredutível em $\mathbb{Z}/p\mathbb{Z}[x]$). Assim, tal construção só nos permite construir planos projetivos de ordem potência de primo. Será que existem planos projetivos com outra ordem? Conjectura-se que não, porém esse problema continua em aberto. O teorema de Bruck-Ryser-Chowla ajuda um pouquinho, dizendo que se $n \equiv 1 \pmod 4$ ou $n \equiv 2$ (mod 4) e n é ordem de um plano projetivo então n deve ser soma de dois quadrados. Pensando nos casos pequenos, esse teorema elimina o caso $n = 6$. A demonstração de que não existe plano projetivo de ordem $n = 10$ foi obtida em 1989 por C. W. H. Lam (com o auxílio de um computador!) e a história da prova está disponível em [7]. O caso $n = 12$ está em aberto.

Planos projetivos também servem para construir alguns *block designs*. Um *block design* consiste num sistema de incidência (v, k, λ, r, b) na qual um conjunto X de v pontos é particionado numa família A de b subconjuntos (chamados *blocks*) de modo que dois pontos quaisquer determinam λ blocks com k pontos em cada block, e cada ponto está contido em r blocks. Na verdade, os cinco parâmetros não são independentes. Fica como exercício para você mostrar que $vr = bk$ e $\lambda(v - 1) = r(k - 1)$ (são duas contagens duplas). Assim, pode-se representar o block design simplesmente como (v, k, λ). Se $b = v$ (e, conseqüentemente, $r = k$) o block design é dito *simétrico*. Note que um plano projetivo de ordem n é block design ($n^2 + n + 1$, n, 1). Outros exemplos e mais informações podem ser encontrados no site: `http://mathworld.wolfram.com/BlockDesign.html`.

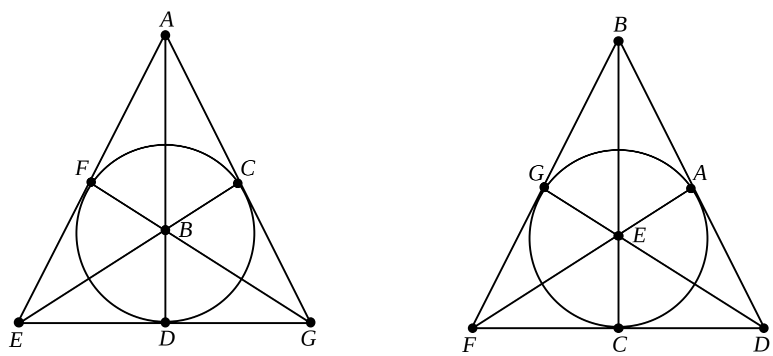
Exercícios

08. (OPM 2001) No condado Heptaprojetivo havia 7 castelos, batizados segundo grandes personagens: Arnold (A), Borcherds(B), Conway (C), Dilbert (D), Erdös (E), Faltings (F), Gowers (G). Havia também 7 ruas, cada uma com 3 castelos, como mostra o mapa a seguir (uma rua é circular):



Um belo dia, o conde Steiner decidiu retirar as placas que identificavam os castelos para fazer uma limpeza. Na hora de recolocá-las, ninguém se lembrava do lugar correto de cada uma, nem mesmo os moradores dos castelos! Os arquivos do condado só indicavam os castelos que ficavam numa mesma rua, mas não a ordem em que eles estavam. Assim, o conde sabia que havia uma rua com os castelos $\{A, B, D\}$, outra com $\{B, C, E\}$, outra com $\{B, F, G\}$, etc.

Frente aos fatos, Steiner resolveu determinar todas as maneiras de recolocar as placas respeitando os arquivos do condado, isto é, todas as maneiras nas quais placas que estavam juntas em uma mesma rua continuassem juntas em uma rua, possivelmente em outra ordem. Duas destas maneiras estão representadas a seguir:



Chamaremos essas maneiras de *válidas*.

(a) Prove que o total de maneiras válidas é 7 vezes o número de maneiras válidas nas quais a placa A é colocada no castelo A.

(b) Prove que o total de maneiras válidas nas quais a placa A é colocada no castelo A é 6 vezes o número de maneiras válidas nas quais a placa A é colocada no castelo A e a placa B é colocada no castelo B.

(c) Determine o número de maneiras válidas.

09. No reino da Alândia há n cidades, assim como no reino da Belândia. Foram construídas m estradas, sendo que cada estrada passa por exatamente duas cidades, uma de cada reino. Mostre que se não existem quatro cidades ligadas por um ciclo de estradas, então $m \le \frac{n}{2}(1+\sqrt{4n-3})$

Mostre que a igualdade pode ocorrer para infinitos valores de n.

Dicas: *a igualdade pode ser demonstrada com uma injeção e contagem dupla - veja o artigo Grafos e Contagem Dupla, na Eureka! 12; para mostrar que a igualdade pode ocorrer para infinitos valores de n, encontre primeiro os valores de n para os quais* $4n - 3$ é *um quadrado perfeito - você vai se surpreender!*

10. (Extensão do exemplo do artigo *Grafos e Contagem Dupla*) Na Terra de Oz há n castelos e várias estradas, sendo que cada uma liga dois castelos. Diz a lenda que se houver quatro castelos ligados em ciclo (ou seja, se existirem quatro castelos A, B, C, e D tais que A e B, B e C, C e D e D e A estão ligados), um dragão aparecerá do centro dos castelos e destruirá a Terra de Oz. Mostre que para esta desgraça não acontecer o número de estradas deve ser menor ou igual a $\left(1+\sqrt{4n-3}\right)\dfrac{n}{4}$ é mostre que para infinitos n é possível construir $\left(1+\sqrt{4n-3}\right)\dfrac{n-1}{4}$ estradas. (para mostrar isto você vai precisar saber um pouco de Álgebra Linear).

REFERÊNCIAS:

[1] *D. Pedoe, Geometry: A Comprehensive Course.* Este livro tem um bom texto não somente introdutório sobre geometria projetiva e contém mais aplicações geométricas. O problema 1 e os axiomas de planos projetivos foram retirados deste livro, assim como a construção de planos projetivos com coordenadas.

[2] *L. Castro, Introdução à Geometria Projetiva, Revista Eureka! 8.* A melhor referência que conheço para começar a estudar geometria projetiva aplicada a problemas de geometria.

[3] O problema 9 foi adaptado de um exemplo retirado do livro *Graph Theory: An Introductory Course,* de B. Bollobás. Ele é um caso particular do problema de *Zaranckiewsky:* qual é o número máximo de arestas de um grafo bipartido com m vértices em uma classe V_1 e n vértices na outra classe V_2, de modo que não haja nenhum subgrafo bipartido completo com r vértices de V_1 e s vértices de V_2? Tal número é normalmente representado por $z(m; n; r; s)$.

[4] O problema 10 é uma extensão de um exemplo de meu artigo *Grafos e Contagem Dupla*, que está na *Revista Eureka!* 12.

[5] A construção do exemplo do problema 10 pode ser encontrada no livro *Proofs From The Book*, de Martin Aigner e Günter M. Ziegler. Mas tente você mesmo fazê-la antes!

[6] Curvas elípticas e a redução para a forma de Weierstrass podem ser encontradas em *Rational Points on Elliptic Curves*, de Joseph H. Silverman e Jonh Tate.

[7] A história da demonstração de que não existe plano projetivo de ordem 10 está em
`http://www.cecm.sfu.ca/organics/papers/lam/paper/html/paper.html`

[8] Um glosário de termos da Matemática e principais fatos relacionados está em
`http://mathworld.wolfram.com/`

[9] Uma discussão muito interessante sobre o assunto está em
`http://www.mathematik.uni-bielefeld.de/~sillke/PUZZLES/projective_plane`
(o grande matemático John Conway inclusive participa desta discussão).

OLIMPÍADAS AO REDOR DO MUNDO

Chegamos ao último número de 2002. Apresentamos, como sempre, questões que não são encontradas facilmente na Internet. Feliz 2003, divirtam-se e enviem as suas soluções.

Continuamos à disposição na OBM para aqueles que estiverem interessados na solução de algum problema particular. Para tanto, basta contactar a OBM, através de carta ou e-mail.

Antonio Luiz Santos

Primeiramente vamos aos problemas propostos deste número

181.(Rússia-2002) Um número de *quatro* algarismos é escrito em um quadro negro. É permitido adicionar 1 a quaisquer dois algarismos adjacentes se nenhum deles for igual a 9 ou subtrair 1 de quaisquer dois algarismos adjacentes se nenhum deles for igual a 0. Partindo de 1234 é possível obtermos 2002 após efetuarmos estas operações diversas vezes ?

182.(Rússia-2002) Seja ABC um triângulo cujas medidas dos lados são distintas duas a duas. Exteriormente ao triângulo, são construídos sobre os seus lados os triângulos eqüiláteros ABC_1, BCA_1 e CAB_1. Mostre que o triângulo $A_1B_1C_1$ *não* é equilátero.

183.(Rússia-2002) Um polinômio quadrático de coeficientes inteiros e coeficiente do segundo grau igual a 1 assume valores primos em três valores inteiros e consecutivos. Mostre que ele assume um valor primo em pelo menos mais um valor inteiro.

184.(Rússia-2002) Seja O o circuncentro de um triângulo isósceles $ABC(AB = BC)$. Um ponto M pertence ao segmento BO e o ponto M' é o simétrico de M em relação ao ponto médio de AB. Sejam ainda K o ponto de interseção de $M'O$ com AB e L um ponto sobre o lado BC tal que $\angle CLO = \angle BLM$. Mostre que os pontos O, K, B, L pertencem a um mesmo círculo.

185.(Rússia-2002) Qual o maior número de termos possível de uma *progressão aritmética* de números inteiros positivos $(a_1, a_2, a_3,\ldots,a_n)$ de razão igual a 2 tal que o número $a_k^2 + 1$ seja primo para todo $k = 1, 2, 3,\ldots,n$?

186.(Rússia-2002) Sobre o eixo x são escolhidos pontos $x_1, x_2,.., x_n$ com $n \geq 3$ distintos dois a dois. Traçam-se então todas as parábolas de coeficientes do segundo grau igual a 1 e que cortam o eixo dos x somente nos pontos escolhidos. Sejam

$y = f_1, \ldots, y = f_m$ as equações destas parábolas. Mostre que a parábola $y = f_1 + \cdots + f_m$ corta o eixo x em exatamente dois pontos.

187.(Rússia -2002) Uma seqüência de números (a_n) é tal que $a_0 = 0$ e $a_{n+1} \geq a_n + 1$. Mostre a desigualdade : $\sum_{k=1}^{n} a_k^3 \geq \left(\sum_{k=1}^{n} a_k\right)^2$

188.(Rússia-2002) No intervalo $(2^{2n}, 3^{2n})$ são escolhidos $2^{2n-1}+1$ números ímpares. Mostre que podemos encontrar entre estes números dois números tais que o quadrado de cada um deles não é divisível pelo outro.

189.(Albânia-2002) Sendo $f : \mathbb{R}^* \to \mathbb{R}$ uma função definida por

$$f(x) = \frac{1}{3}\left(2^{\frac{1+x}{x}} - 2^x\right)$$

Determine o valor da soma :

$$f\left(\frac{1}{2002}\right) + f\left(\frac{2}{2002}\right) + \cdots + f\left(\frac{2002}{2002}\right) + 2f\left(\frac{2002}{2001}\right) + 2f\left(\frac{2002}{2000}\right) + \cdots + 2f\left(\frac{2002}{1}\right)$$

190.(Albânia-2002) Mostre como dividir um triângulo qualquer em :

(i) 2002 triângulos semelhantes a ele.

(ii) 2003 triângulos semelhantes a ele.

191.(Irlanda-2002) Em um triângulo ABC tem-se que $AB = 20$, $AC = 21$ e $BC = 29$. Se D e E são pontos do segmento BC tais que $BD = 8$ e $EC = 9$, determine a medida do ângulo $\angle DAE$.

192.(Irlanda-2002) Suponha que n seja o produto de quatro números primos distintos a, b, c, d tais que :

(i) $a + c = d$

(ii) $a(a + b + c + d) = c(d - b)$

(iii) $1 + bc + d = bd$

Determine n.

193.(Irlanda-2002) Seja (a_n) uma seqüência definida por $a_1 = 1$, $a_2 = 1$, $a_3 = 1$ e $a_{n+1}a_{n-2} - a_n a_{n-1} = 2$ para todo $n \geq 3$. Prove que a_n é um inteiro positivo para todo $n \geq 1$.

194.(Eslovênia-2002) 38 é o menor inteiro positivo tal que o seu quadrado termina com *três quatros* ($38^2 = 1444$). Qual o próximo inteiro positivo com esta propriedade ?

195.(Eslovênia-2002) Sejam M o ponto médio da base AB do trapézio $ABCD$; E um ponto interior ao segmento AC tal que BC e ME intersectam-se em F; G o ponto de interseção de FD e AB; H o ponto de interseção de DE e AB. Mostre que M é o ponto médio do segmento GH.

196.(Eslovênia-2002) Sejam k um círculo do plano euclidiano, k_1 e k_2 dois círculos disjuntos interiores a k e que o tangenciam nos pontos A e B respectivamente. Seja ainda (t) a tangente comum aos círculos k_1 e k_2 nos pontos C e D respectivamente tal que k_1 e k_2 estejam situados num mesmo semiplano determinado pela reta (t) enquanto que o centro do círculo k pertence ao outro semiplano. Se E é o ponto de interseção de AC e BD, mostre que o ponto E pertence ao círculo k.

197.(Eslovênia-2002) Determine o menor inteiro positivo que pode ser escrito como uma soma de 9, 10 e 11 inteiros positivos consecutivos.

198.(Estônia-2002) Em um triângulo ABC tem-se que $\angle B = 2 \cdot \angle C$ e a bissetriz do ângulo $\angle A$ intersecta o lado BC no ponto D tal que $AB = CD$. Determine a medida do ângulo $\angle A$.

199.(Estônia-2002) Um número natural de 10 *algarismos distintos* é dito *mágico* se ele for múltiplo de 99999. Quantos números *mágicos* não começados por zero existem ?

200. (Grécia-2002) Determine todos os inteiros positivos N tais que :
(i) N possui exatamente16 divisores $1 = d_1 < d_2 < \ldots < d_{16} = N$
(ii) $d_5 = (d_2 + d_4)d_6$.

201. (Inglaterra-2002) Um quadrilátero $ABCD$ está inscrito em um círculo. As diagonais AC e BD intersectam-se no ponto Q. Os prolongamentos dos lados DA e CB, a partir de A e B respectivamente, intersectam-se em P. Sabendo que $CD = CP = DQ$, mostre que $\angle CAD = 60^o$.

202.(Inglaterra-2002) *Doze* pessoas estão sentadas em torno de uma mesa circular. De quantos modos seis pares de pessoas podem trocar apertos de mão de modo que não haja cruzamentos de braços?
(Não é permitido que uma pessoa troque apertos de mão com mais de uma pessoa de cada vez)

203.(Inglaterra-2002) Seja *f* uma função de $\mathbb{N}$ em $\mathbb{N}$, onde $\mathbb{N}$ é o conjunto dos números inteiros não negativos, que possui as seguintes propriedades :
(i) $f(n+1) > f(n)$, para cada $n \in \mathbb{N}$.
(ii) $f(n + f(m)) = f(n) + m + 1$, para todos $m, n \in \mathbb{N}$.
Determine todos os valores possíveis de $f(2001)$.

204.(Inglaterra-2002) A altura traçada de um dos vértices de um triângulo *ABC* intersecta o lado oposto no ponto *D*. A partir do ponto *D* são traçadas perpendiculares aos outros dois lados intersectando-os nos pontos *E* e *F*. Mostre que a medida do segmento *EF* independe do vértice do qual a altura é traçada.

205.(Áustria-2002) Determine o menor inteiro positivo x para o qual todas as frações :
$$\frac{3x+9}{8}, \frac{3x+10}{9}, \frac{3x+11}{10}, \ldots, \frac{3x+49}{48}$$
são irredutíveis.

206.(Áustria-2002) Determine o maior número real C tal que
$$\frac{((x+y)^2-6)((x-y)^2+8)}{(x-y)^2} \geq C$$
é verdadeira para todos os números reais x e y $(x \neq y)$ com $xy = 2$. Para quais pares ordenados (x, y) a igualdade é verdadeira ?

207.(Áustria-2002) Seja $f(x) = \dfrac{9^x}{9^x+3}$

Determine a soma de todas as expressões da forma $f\left(\dfrac{k}{2002}\right)$ onde *k* é um número inteiro entre 0 e 2002 tal que a fração $\dfrac{k}{2002}$ seja irredutível.

208. (Bielorússia-2002) Determine o maior número possível de grupos que podem ser extraídos do conjunto {1, 2, 3,…,19, 20}, de modo que o produto dos números de cada um dos grupos seja um *quadrado perfeito* .
(O grupo pode conter apenas um número e, neste caso, o produto é igual a este número; além disso, cada número deve fazer parte de apenas um grupo)

209. (Bielorússia-2002) A altura CH de um triângulo retângulo ABC, com $\angle C = 90º$ intersecta as bissetrizes AM e BN nos pontos P e Q respectivamente. Prove que a reta que passa pelos pontos médios de QN e PM é paralela à hipotenusa de ABC.

210. (Bielorússia-2002) Um conjunto de números naturais de três algarismos formados com 1, 2, 3, 4, 5, 6 é chamado *agradável* se ele satisfaz à seguinte condição: para quaisquer dois algarismos distintos de 1, 2, 3, 4, 5, 6, existe um número deste conjunto que contém ambos. Se, para qualquer conjunto *agradável* calcularmos a soma de seus elementos, determine o menor valor possível destas somas.

Agora vamos aos comentários e soluções dos leitores para alguns dos problemas apresentados em números anteriores de EUREKA!. *Como sempre, o critério por nós adotado para este número foi apresentar as soluções dos problemas que foram, até o presente momento, resolvidos pelo maior número de leitores.*

32. (Moldávia-1998) A seqüência (a_n), $n \in \mathbb{N}^*$ verifica as relações $a_1 = \dfrac{1}{2}$ e $a_n = \dfrac{a_{n-1}}{2na_{n-1}+1}$ para todo número natural $n > 1$. Calcule $a_1 + a_2 + \cdots + a_{1998}$.

Resumo das soluções de diversos leitores:
Escrevamos a lei de recorrência de uma forma ligeiramente diferente:

$$\frac{1}{a_n} = 2n + \frac{1}{a_{n-1}} \Leftrightarrow \frac{1}{a_n} - \frac{1}{a_{n-1}} = 2n$$

Logo,

$$\sum_{k=2}^{n}\left(\frac{1}{a_k} - \frac{1}{a_{k-1}}\right) = \sum_{k=2}^{n}(2k)$$

O primeiro membro desta última igualdade é uma *soma telescópica* e igual a $\dfrac{1}{a_n} - \dfrac{1}{a_1}$ enquanto que o segundo membro é igual a $4+6+8+\cdots+2n = \dfrac{(4+2n)(n-1)}{2}$. Daí,

$$\frac{1}{a_n} - 2 = (n+2)(n-1) \Leftrightarrow \frac{1}{a_n} = n(n+1) \Leftrightarrow a_n = \frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$$

Finalmente,

$$\sum_{i=1}^{1998} a_i = \sum_{n=1}^{1998}\left(\frac{1}{n} - \frac{1}{n+1}\right) = 1 - \frac{1}{1999} = \frac{1998}{1999}$$

36.(China-1999) Seja *PQRS* um quadrilátero inscrito num círculo e cuja medida do ângulo $\angle PSR$ seja igual a 90^o. Se H e *K* são os pés das perpendiculares baixadas de *Q* sobre *PR* e *PS* respectivamente (convenientemente prolongados se necessário). Mostre que *HK* divide *QS* ao meio.

Resumo das soluções de diversos leitores:

Seja *G* o ponto de interseção de *KH* e *SR*. Como *P, Q, R* e *S* são *cíclicos* (pertencem a um mesmo círculo), assim como *K, Q, H* e *P* tem-se que $\angle QKG = \angle QKH = \angle QPR = \angle QSG$. Daí *K, Q, G* e *S* são cíclicos com $\angle KSG = \pi/2 = \angle SKQ$. Desta forma, *KQGS* é um retângulo e *KH* divide *QS* ao meio.

39. (Irlanda-1999) Determine todos os inteiros positivos *m* tais que a quarta potência do número de seus divisores positivos é igual a *m*.

Resumo das soluções de diversos leitores:

Observemos em primeiro lugar que *m* = 1 possui a referida propriedade. Suponhamos agora que *m* ≥ 2. Como *m* é uma quarta potência ele pode ser escrito univocamente como

$$m = p_1^{4\beta_1} \times p_2^{4\beta_2} \times \cdots \times p_n^{4\beta_n}$$

onde $p_1 < p_2 < \cdots < p_n$ são números primos e $\beta_i > 0,\ \ i = 1, 2, \dots, n$. O número de divisores de *m* é dado por

$$(4\beta_1 + 1)(4\beta_2 + 1)\cdots(4\beta_n + 1)$$

A requerida propriedade é

$$(4\beta_1 + 1)(4\beta_2 + 1)\cdots(4\beta_n + 1) = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_n^{\beta_n}$$

Como o lado esquerdo é ímpar então $p_1 \ge 3$. Observe que $3^\beta > 4\beta + 1$ se $\beta \ge 3$; também, $5^\beta > 4\beta + 1$ se $\beta \ge 2$; finalmente $p^\beta > 4\beta + 1$ se $\beta \ge 1$ e $p \ge 7$. Além disso, $5^\beta \ge 4\beta + 1$ se $\beta \ge 1$, assim, se $p^\beta < 4\beta + 1$ para algum primo ímpar p e algum $\beta \ge 1$ então $p = 3$. Deste modo, devemos ter $p_1 = 3$ ou $p_1 = 5$.

1º Caso : $p_1 = 5$

Neste caso, $\beta_1 = 1$ e assim

$$5(4\beta_2+1)\cdots(4\beta_n+1) = 5\times p_2^{\beta_2}\times\cdots\times p_n^{\beta_n}$$

Pela terceira desigualdade acima não podem existir outros fatores primos em *m* distintos de *5* e portanto a única solução é $m = 5^4$.

2º Caso : $p_1 = 3$. Claramente $\beta_1 = 1$ ou $\beta_1 = 2$ uma vez que $3^3 > 4(3)+1$.

Se $\beta_1 = 1$, então $5(4\beta_2+1)\cdots(4\beta_n+1) = 3\times p_2^{\beta_2}\times\cdots\times p_n^{\beta_n}$. Assim $p_2 = 5$. Se $\beta_2 > 2$ então $5^{\beta_2} > \frac{5}{3}(4\beta_2+1)$ o que nos leva a uma contradição. Deste modo, $\beta_2 = 1$ ou $\beta_2 = 2$.

Se $\beta_2 = 1$ então $25(4\beta_3+1)\cdots(4\beta_n+1) = 15\times p_3^{\beta_3}\times\cdots\times p_n^{\beta_n}$ o que é uma contradição já que 25 não divide o lado direito.

Se $\beta_2 = 2$, então $45(4\beta_3+1)\cdots(4\beta_n+1) = 75\times p_3^{\beta_3}\times\cdots\times p_n^{\beta_n}$ o que é uma contradição já que *9* não divide o lado direito.

Se $\beta_1 = 2$ então $9(4\beta_2+1)\cdots(4\beta_n+1) = 9\times p_2^{\beta_2}\times\cdots\times p_n^{\beta_n}$.

Não podemos ter $p_2 \ge 7$ logo, $n = 1$ ou ($n = 2$ e $p_2 = 5$ e $\beta_2 = 1$). O primeiro caso nos dá $m = 3^8$; o último caso nos dá $m = 3^8\times 5^4$. Concluindo existem *quatro* soluções a saber,

$$1, 5^4, 3^8 \text{ e } 3^8\times 5^4$$

40. (Irlanda-1999) Mostre que existe um número inteiro positivo na seqüência de Fibonacci que é divisível por 1000.

Resumo das soluções de diversos leitores:

Considere o conjunto de $10^6 + 1$ pares

$$\{(F_i, F_{i+1}) \mid i = 1,2,\dots,10^6\}$$

tomados $\bmod(10^3)$. Como o conjunto $\{(a,b) \mid 0 \le a,b \le 999\}$ com a e b inteiros possui apenas 10^6 elementos, o *Princípio da Casa dos Pombos* nos diz que existem inteiros $i > j$ tais que $F_{i+1} - F_{j+1}$ e $F_i - F_j$ são ambos divisíveis por 1000. Mas

$$F_{i-1} - F_{j-1} = (F_{i+1} - F_{j+1}) + (F_j - F_i)$$

Logo, $F_{i-1} - F_{j-1}$ é também divisível por 1000. Argumentando desta maneira de frente para trás vemos que $F_{i-j+1} - F_1$ e $F_{i-j} - F_0$ são divisíveis por 1000. Mas, $F_0 = 0$ daí, F_{i-j} é divisível por 1000.

60. (St.Petersburg-1999) Três mágicos apresentam um truque entregando a uma pessoa da platéia um maço de cartas numeradas com 1, 2,...,2 n + 1 (n > 6). O espectador fica com uma das cartas e aleatoriamente distribui as restantes entre o primeiro e o segundo mágicos (cada um deles fica com n cartas) . Estes olham suas cartas (sem se comunicar um ao outro) e cada um escolhe duas cartas formando um maço (ordenado) com estas cartas e as entrega ao terceiro mágico. O terceiro mágico olha estas quatro cartas e anuncia a carta que ficou com o espectador. Explique como este truque pode funcionar.

SOLUÇÃO DE JEAN-CHRISTOPHE YOCCOZ (PARIS - FRANÇA):

A ideia é que cada mágico transmita de algum jeito a soma de suas n cartas módulo $2n$ + 1 (e então o outro mágico descobre a carta que foi retirada, que é o simétrico da soma dos dois resultados módulo $2n$ + 1).

Assim, basta definir uma função $f : \mathbb{Z}/(2n+1)\mathbb{Z} \times \mathbb{Z}/(2n+1)\mathbb{Z} \to \mathbb{Z}/(2n+1)\mathbb{Z}$ tal que, dado c em $\mathbb{Z}/(2n+1)\mathbb{Z}$ e um subconjunto arbitrário A de $\mathbb{Z}/(2n+1)\mathbb{Z}$ com n elementos eles satisfazem a propriedade $P(A, c)$: existem elementos distintos x e y de A com $f(x, y) = c$.

A idéia é mostrar a existência de uma função $f(x, y)$ como acima que seja equivariante, isto é, que satisfaça $f(x + c, y + c) = f(x, y) + c$, para quaisquer x, y e c. É fácil ver que para uma tal função f vale $P(A, c)$ se e somente se vale $P(A - c, 0)$, onde $A - c = \{x - c \mid x \in A\}$. Assim, basta ver que todo A com n elementos satisfaz P(A, 0). Agora, em vez de construir f, vamos construir a pré-imagem de 0 pela f (ou um subconjunto conveniente dela).

Pela equivariância, se (x, y) e (u, v) são pares distintos com $f(x, y) = f(u, v) = 0$ então $y - x$ tem que ser diferente de $v - u$, senão, para $c = u - x$, temos $(u, v) = (x+ c, y + c)$, donde $f(u, v) = c$. Por outro lado, dado um conjunto de pares$\{(x_1, y_1),...,(x_k, y_k)\}$ com $y_j - x_j$ distinto de $y_i - x_i$ para todo i distinto de j, existe uma função equivariante f com $f(x_i, y_i) = 0$ para todo i. Nosso problema agora se reduz a encontrar um conjunto de pares $\{(x_1, y_1),...,(x_k, y_k)\}$ com os $y_i - x_i$ todos distintos (e distintos de 0) tal que para todo A com n elementos exista i tal que x_i e y_i estejam em A. Fazemos com que esse conjunto de pares contenha os pares (0, 1), (2, 1), (0, 2), (3, 6), (9, 6), (3, 9), (4, 8), (12, 8) e (4, 12). Note que as diferenças $y_i - x_i$ são 1, –1, 2, 3, – 3, 6, 4, – 4 e 8, e que um A ruim só pode conter um elemento de cada uma das triplas {0, 1, 2}, {3, 6, 9} e

{4, 8, 12}. Vamos completar nosso conjunto de pares com n – 4 pares que formarão uma partição de $\mathbb{Z}/(2n+1)\mathbb{Z}$ \{0, 1, 2, 3, 6, 9, 4, 8, 12}. Um conjunto ruim só pode ter um elemento de cada par, tendo pois no máximo $n - 4 + 3 = n - 1$ elementos, como queríamos. Para isso considere alguns casos:

I) n par, $n \geq 12$: Escrevemos $n = 2k$. Os pares serão $(-k + 6, k + 6)$, $(-k + 7, k + 5)$,...,(–1, 13) (diferenças n, n – 2 ,...,14); $(k + 7, 3k + 6)$, $(k + 8, 3k + 5)$,...,$(2k + 4, 2k + 9)$ (diferenças n –1, n – 3,...,5); e $(2k + 5, 5)$, $(2k + 6, 7)$, $(2k + 7, 11)$ e $(2k + 8, 10)$ (diferenças $-n$, $1 - n$, $4 - n$ e $2 - n$).

II) n ímpar, $m \geq 13$: Escrevemos $n = 2k + 1$. Os pares serão (–1, 13),..., $(-k + 6, k + 6)$ (diferenças 14 ,..., n –1); $(k + 7, 3k + 8)$,...,$(2k + 5, 2k + 10)$ (diferenças n ,..., 5); e $(2k + 6, 5)$, $(2k + 7, 7)$, $(2k + 8, 11)$ e $(2k + 9, 10)$ (diferenças $-n$, $1-n$, $4 - n$ e $2 - n$).

Casos particulares anteriores:
$n = 7$: Pares (5, 10), (13, 11) e (7, 14) (diferenças 5, – 2 e 7).
$n = 8$: Pares (5, –1), (7, 14), (15, 10) e (13, 11) (diferenças – 6, 7, – 5 e – 2).
$n = 9$: Pares (5, 14), (16, 7), (10, 17), (18, 11) e (15, 13) (diferenças 9, –9, 7, –7 e –2).
$n = 10$: Pares (20, 10),(19, 11),(18, 13),(5, 14),(16, 7) e (17, 15) (diferenças –10, – 8, – 5, 9, – 9 e – 2).
$n = 11$: Pares (16, 5), (17, 7), (20, 11), (18, 10), (19, 13), (21, 14) e (15, 22) (diferenças – 11, – 10 , – 9, – 8, – 6, – 7 e 7).

Publicamos a seguir, a pedidos, uma solução do problema 12, *proposto na Eureka*! *N*º. 8.

12. (Irlanda-1999) Três números $a < b < c$ estão em progressão aritmética se $c - b = b - a$. Definamos a seqüência (u_n), $n = 0, 1, 2, 3,\ldots$ da seguinte maneira: $u_0 = 0$, $u_1 = 1$ e para cada $n \geq 1$, u_{n+1} é o menor inteiro positivo tal que $u_{n+1} > u_n$ e $\{u_0, u_1, \ldots, u_n, u_{n+1}\}$ não possui três elementos em progressão aritmética. Determine u_{100}.

Vamos mostrar por indução que se $n = (a_k a_{k-1}...a_0)_2$, i.e, $n = \sum_{j=0}^{k} a_j \cdot 2^j$, com $a_j \in \{0,1\}, \forall j$, então $u_n = (a_k a_{k-1}...a_0)_3 = \sum_{j=0}^{k} a_j \cdot 3^j$. Suponha que isso seja válido para $0 \le n \le 2^k - 1$ (isso é verdade para k = 1).

Como $\{u_0, u_1, ..., u_{2^k-1}\}$ não possui três elementos em progressão aritmética e $u_{2^k-1} = \sum_{j=0}^{k-1} 1 \cdot 3^j = \frac{3^k - 1}{2}$, então $\{u_0, u_1, ..., u_{2^k-1}, 3^k + u_0, 3^k + u_1, ..., 3^k + u_{2^k-1}\}$ também não possui três elementos em progressão aritmética, pois se dois termos de uma progressão aritmética estão entre 0 e $\frac{3^k-1}{2}$, então o terceiro termo é menor ou igual a $3^k - 1 < 3^k$, e se dois termos de uma progressão aritmética estão entre 3^k e $3^k + \frac{3^k-1}{2}$ então o termo anterior é maior ou igual a $3^k - \frac{3^k-1}{2} = \frac{3^k+1}{2} > \frac{3^k-1}{2}$.

Vamos ver que, de fato, $u_{2^k} = 3^k$, donde $u_{2^k+j} \ge 3^k + u_j$ para $0 \le j \le 2^k - 1$, e logo, pelo fato acima, $u_{2^k+j} = 3^k + u_j$, para $0 \le j \le 2^k - 1$. Para isso, basta ver que se $\frac{3^k-1}{2} < u < 3^k$ então $\{u_0, u_1, ..., u_{2^k-1}, u\}$ contém uma progressão aritmética de três termos. Seja $u = \sum_{j=0}^{k-1} b_j \cdot 3^j$, com $b_j \in \{0,1,2\}, \forall j$. Então $u = 2v_2 - v_1$, onde $v_2 = \sum_{j=0}^{k-1} d_j \cdot 3^j, v_1 = \sum_{j=0}^{k-1} c_j \cdot 3^j$, e, se $b_j = 0$, então $(c_j, d_j) = (0,0)$; se $b_j = 1$ então $(c_j, d_j) = (1,1)$ e, se $b_j = 2$ então $(c_j, d_j) = (0,1)$.

Em particular, $\{c_j, d_j\} \subset \{0,1\}, \forall j$, donde v_1 e v_2 pertencem a $\{u_0, u_1, ..., u_{2^k-1}\}$, e $u - v_2 = v_2 - v_1$, logo $v_1 < v_2 < u$ estão em progressão aritmética.

Finalmente, $100 = 2^6 + 2^5 + 2^2$, donde $u_{100} = 3^6 + 3^5 + 3^2 = 981$.

Acusamos o recebimento de soluções de problemas anteriores dos seguintes leitores de **EUREKA!**:

Anderson Torres	São Paulo - SP	Prob. 24, 32, 35, 37, 40, 43, 45, 51, 54, 56, 63, 88, 103, 114, 124, 143, 151, 154, 158, 160, 164, 168, 169, 170, 171, 172.
Carlos A. Gomes	Natal - RN	Prob. 151, 162, 174.
Erasmo de Souza Dias	Goiânia - GO	Prob. 151.
Fernando Carvalho Ramos	Santa Maria - RS	Prob. 151, 160, 163, 174.
Francisco B. de Lima Holanda	Fortaleza - CE	Prob. 36, 45, 47, 69, 87, 88, 102, 104, 109, 169, 170.
Geraldo Perlino	Itapecerica da Serra - SP	Prob. 151, 160, 161, 164, 167.
Geraldo Perlino Júnior	Cotia - SP	Prob. 151, 152, 153, 154, 158, 159, 160, 161, 162, 163, 165, 166, 167, 168, 170, 171, 172, 173, 174, 178, 179,
Gibran Medeiros de Souza	Natal - RN	Prob. 163, 166.
Helder Oliveira de Castro	Mogi das Cruzes - SP	Prob. 43, 45, 46, 54, 66, 63, 67, 70, 74, 86, 90, 99, 101, 102, 105, 115, 128, 133, 143.
Luiz Sérgio Carvalho de Mello	Rio de Janeiro - RJ	Prob. 138, 151, 166.
Marcelo Ribeiro de Souza	Rio de Janeiro - RJ	Prob. 151, 153, 154, 160, 162.
Marcelo Rufino de Oliveira	Belém - PA	Prob. 151, 152, 153, 154, 158, 160, 162, 163, 164, 165, 166, 170, 171, 172, 173, 174, 179, 180.
Okakama Matsubaxi	São Paulo - Sp	Prob. 130.
Renato F. L. Mello	J. dos Guararapes - PE	Prob. 154, 160, 162, 166, 173, 179.
Tertuliano C. de Souza Neto	Salvador - BA	Prob. 61, 62, 68, 69, 70, 72, 74, 76, 82, 83, 87, 88, 90.

SOLUÇÕES DE PROBLEMAS PROPOSTOS

Publicamos aqui algumas das respostas enviadas por nossos leitores.

66) Prove que, dados um inteiro $n \geq 1$ e um conjunto $A \subset \mathbb{Z}/n^2\mathbb{Z}$ com n elementos existe $B \subset \mathbb{Z}/n^2\mathbb{Z}$ com n elementos tal que $A + B = \{x + y \mid x \in A, y \in B\} \subset \mathbb{Z}/n^2\mathbb{Z}$ tem mais de $n^2/2$ elementos.

SOLUÇÃO DE ZOROASTRO AZAMBUJA NETO (RIO DE JANEIRO - RJ):

Vamos mostrar que, dado um conjunto $X \subset \mathbb{Z}/n^2\mathbb{Z}$, existe $t \in \mathbb{Z}/n^2\mathbb{Z}$ tal que $(A + \{t\}) \cap X$ tem pelo menos $|X|/n$ elementos, onde $|X|$ é o número de elementos de X. De fato, $\sum\limits_{t \in \mathbb{Z}/n^2\mathbb{Z}} \left|(A + \{t\}) \cap X\right| = \sum\limits_{a \in A} \sum\limits_{x \in X} \left|\{t \in \mathbb{Z}/n^2\mathbb{Z} \mid a + t = x\}\right| = |A| \cdot |X| = n \cdot |X|$,

pois, para cada $a \in A$ e $x \in X$, existe um único $t \in \mathbb{Z}/n^2\mathbb{Z}$ tal que $a + t = x$. Assim, $\frac{1}{n^2} \sum\limits_{t \in \mathbb{Z}/n^2\mathbb{Z}} \left|(A + \{t\}) \cap X\right| = |X|/n$, donde o número médio de elementos de $(A + \{t\}) \cap X$ é $|X|/n$, o que claramente implica a nossa afirmação.

Agora, dado $k \geq 0$ existem $t_1, t_2, \ldots, t_k \in \mathbb{Z}/n^2\mathbb{Z}$ tais que $n^2 - \left|A + \{t_1, t_2, \ldots, t_k\}\right| \leq n^2 \cdot (1 - \frac{1}{n})^k$. De fato, por indução, dados tais $t_1, t_2, \ldots, t_k$, pela afirmação acima existe $t_{k+1} \in \mathbb{Z}/n^2\mathbb{Z}$ com $(A + \{t_{k+1}\}) \cap \left((\mathbb{Z}/n^2\mathbb{Z}) \setminus (A + \{t_1, t_2, \ldots, t_k\})\right) \geq \frac{1}{n} \cdot \left|(\mathbb{Z}/n^2\mathbb{Z}) \setminus (A + \{t_1, t_2, \ldots, t_k\})\right|$,

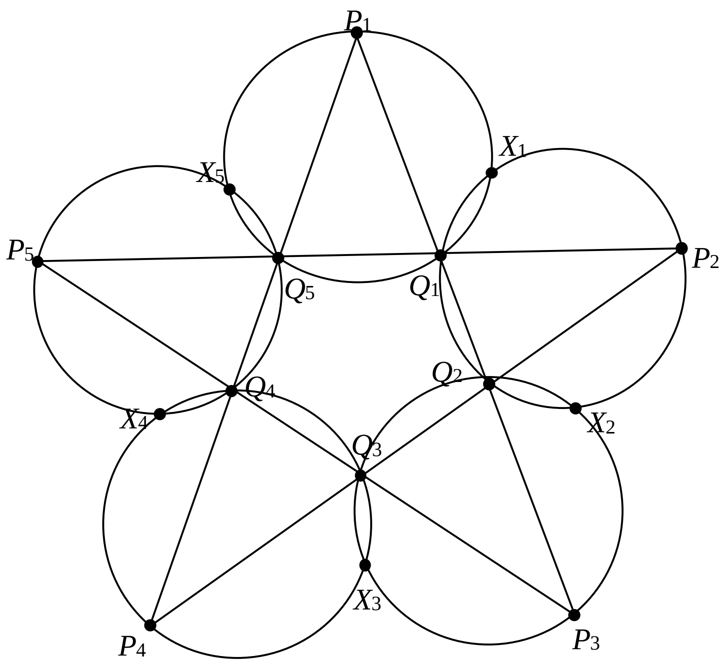
donde $\left|(A + \{t_1, t_2, \ldots, t_{k+1}\})^C\right| = \left|((A + \{t_1, t_2, \ldots, t_k\}) \cup (A + \{t_{k+1}\}))^C\right| \leq$

$\left(1 - \frac{1}{n}\right) \cdot \left|(A + \{t_1, t_2, \ldots, t_k\})^C\right| \leq \left(1 - \frac{1}{n}\right) \cdot n^2 \cdot \left(1 - \frac{1}{n}\right)^k = n^2 \left(1 - \frac{1}{n}\right)^{k+1}$ (aqui X^C denota $(\mathbb{Z}/n^2\mathbb{Z}) \setminus X$; temos $\left|X^C\right| = n^2 - |X|$).

Assim, existe $B = \{t_1, t_2, \ldots, t_n\}$ tal que $n^2 - |A + B| \leq n^2 \cdot \left(1 - \frac{1}{n}\right)^n < n^2/2$, donde $|A + B| > n^2/2$.

Obs. Para $n \geq 1, \left(\left(1-\frac{1}{n}\right)^{n}\right)^{-1} = \left(\frac{n}{n-1}\right)^{n} > \left(1+\frac{1}{n}\right)^{n} \geq 1+\binom{n}{1}\cdot\frac{1}{n} = 2,$ donde $\left(\frac{n}{n-1}\right)^{n} < \frac{1}{2}.$

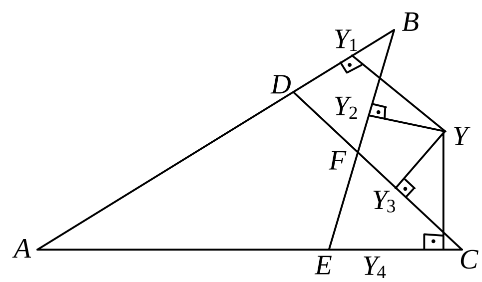
70)



Na figura acima, para $1 \leq j \leq 5$, X_j é o ponto de interseção dos círculos circunscritos aos triângulos $Q_{j-1}P_jQ_j$ e $Q_jP_{j+1}Q_{j+1}$ distintos de Q_j (os índices são tomados módulo 5). Prove que o pentágono $X_1X_2X_3X_4X_5$ é inscritível.

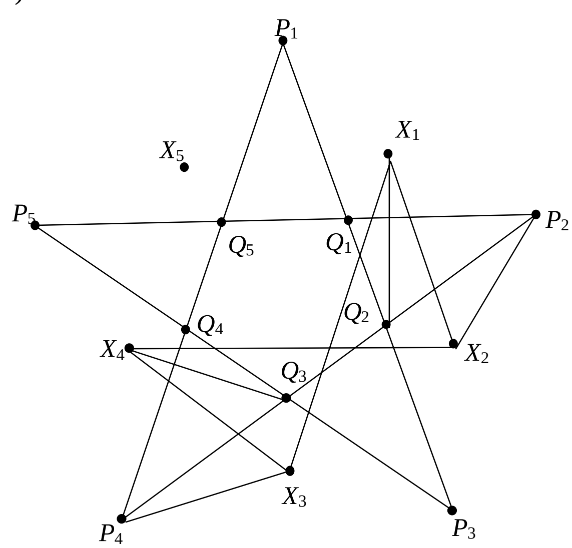
Obs: O pentágono $P_1P_2P_3P_4P_5$ não é necessariamente regular.

SOLUÇÃO DE ALEX CORRÊA ABREU (NITERÓI – RJ):



Lema: As circunferencias circunscritas a *BDF*, *CEF*, *CDA*, *BEA*, tem um ponto em comum.

Prova: Seja *X* a intersecção das circunferencias circunscritas a *BDF*, *CEF*.
Y_1, Y_2, Y_3, Y_4, o pé das perpendiculares por *Y* a $\overleftrightarrow{BD}, \overleftrightarrow{BE}, \overleftrightarrow{CD}, \overleftrightarrow{CE}$ respectivamente $\Rightarrow$ Y_1, Y_2, Y_3 são colineares pela reta de Simson já que *Y* pertence a circunferência circunscrita a *BDF* e analogamente Y_2, Y_3, Y_4 também são logo Y_1, Y_2, Y_3, Y_4 são colineares. Portanto pela recíproca da reta de Simson, *Y* pertence à circunferência circunscrita a *ABE*, (Y_1, Y_2, Y_4 colineares) e à circunferência circunscrita a *ADC* (Y_1, Y_3, Y_4 colineares).



Agora $X_2\hat{X}_1Q_2 = Q_2\hat{P}_2X_2$ pois $X_1X_2P_2Q_2$ é inscritível e $Q_2\hat{X}_1X_3 = Q_2\hat{P}_4X_3$ pois $X_1 \in$ circunferência circunscrita a $P_1Q_2P_4$ pelo lema e X_3 também.

Analogamente $Q_3\hat{X}_4X_3 = Q_3\hat{P}_4X_3$ e $Q_3\hat{X}_4X_2 = X_2\hat{P}_2Q_2 \Rightarrow X_2\hat{X}_1Q_2 = Q_3\hat{X}_4X_2$ e $Q_2\hat{X}_1X_3 = Q_3\hat{X}_4X_3 \Rightarrow X_2\hat{X}_1X_3 = X_2\hat{X}_4X_3 \Rightarrow X_1X_2X_3X_4$ é inscritível; analogamente $X_2X_3X_4X_5$ também é, logo $X_1X_2X_3X_4X_5$ é inscritível.

72) Ache todas as funções $f : \mathbb{R} \to \mathbb{R}$ tais que $f(x^4 + y) = x^3 f(x) + f(f(y))$, $\forall x, y \in \mathbb{R}$.

SOLUÇÃO DE RODRIGO VILLARD MILET (RIO DE JANEIRO – RJ):

$f(x^4 + y) = x^3 f(x) + f(f(y))$ (I)

Em (I) , $x = 0 \Rightarrow f(y) = f(f(y))$, logo $f(x^4 + y) = x^3 f(x) + f(y)$ (I'). Agora fazendo x = 1 e y = 0, segue que $f(0) = 0$. Portanto, fazendo y = 0, temos $f(x^4) = x^3 f(x)$ (II) (Em particular, f é ímpar). Em (I'), $f(x^4 + y) = f(x^4) + f(y)$, donde $f(x + y) = f(x) + f(y)$, para todo $x > 0$. Mas como f é ímpar, é fácil ver que vale $f(x + y) = f(x) + f(y)$, para todos x, y reais.

Lema: Todo x real pode ser escrito (de forma única) como $x = u + v$, onde $f(u) = u$ e $f(v) = 0$.

Prova: $x = f(x) + (x - f(x))$. Tome $u = f(x)$ e $v = x - f(x)$. Para a unicidade, suponha que $x = u + v = u' + v'$. Daí $u - u' = v' - v$ e aplicando f, segue que $u = u'$ e assim, $v = v'$.

Agora, em (II), escreva $x = u + v$, como no lema. Então:

$f((u+v)^4) = (u+v)^3 f(u+v) \Rightarrow 4f(u^3v) + 6f(u^2v^2) + 4f(uv^3) = 3u^2v(u+v)$ (III)

Podemos trocar v por $-v$, pois $f(-v) = 0$, logo:

$-4f(u^3v) + 6f(u^2v^2) - 4f(uv^3) = -3u^2v(u-v)$ (IV)

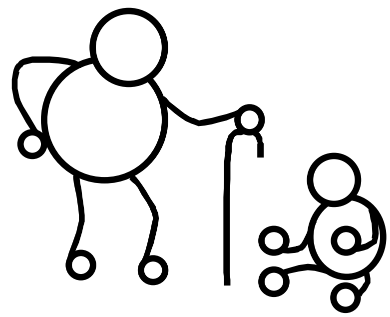
Fazendo (III) + (IV): $f(u^2v^2) = \dfrac{u^2v^2}{2}$. Pelo lema, $u^2v^2 = u' + v'$, com $f(u') = u'$ e $f(v') = 0$. Daí segue que $u' = f(u' + v') = \dfrac{u' + v'}{2} \Rightarrow u' = v'$. Aplicando f, segue que $u' = v' = 0$, ou seja $u \equiv 0$ ou $v \equiv 0$, o que nos dá respectivamente as soluções $f(x) \equiv 0$ e $f(x) \equiv x$, que claramente satisfazem a equação (I).

Agradecemos também o envio das soluções e a colaboração de:

Rildo Alves do Nascimento	**Santa Maria da Boa Vista – PE**
Leno Silva Rocha	**Goiânia – GO**
Minh Perez	**Rehoboth, EUA**
Carlos Alberto da Silva Victor	**Nilópolis – RJ**

Seguimos aguardando o envio de soluções dos problemas propostos Nº. 68, 69, 71 e 73 publicado na revista Eureka! Nº. 14

Você sabia… que para completar um álbum composto por n figurinhas supondo que você compre 1 figurinha por dia o tempo esperado (médio) é $n \cdot \ln n$ dias?
Considerando uma situação na qual você tem um álbum com 200 figurinhas e compre um pacote de 3 figurinhas por dia você deve demorar um ano para completar o álbum.



Você sabia… que foi descoberto por Manindra Agrawal, Nitin Saxena e Neeraj Kayal um algoritmo (determinístico) que checa a primalidade de números naturais n em tempo polinomial em log n?
Para mais informações veja: `http://www.cse.iitk.ac.in/news/primality.html` ou `http://www.utm.edu/research/primes/prove/prove4_3.html`

PROBLEMAS PROPOSTOS

✉ *Convidamos o leitor a enviar soluções dos problemas propostos e sugestões de novos problemas para os próximos números.*

74) Ache todas as funções $f:\mathbb{R}\to\mathbb{R}$ tais que: $f(x+y)+f(x-y)=2f(x)\cdot\cos y$, $\forall x, y\in\mathbb{R}$.

75) Seja T_n um triângulo retângulo cujos lados medem $(4\cdot n^2, 4\cdot n^4-1, 4\cdot n^4+1)$, onde n é um número inteiro positivo. Seja α_n a medida do ângulo oposto ao lado de medida $4\cdot n^2$. Mostre que, se n varia dentro dos inteiros positivos, $\alpha_1+\alpha_2+\alpha_3+\ldots=90^0$.

76) Mostre que um polígono qualquer pode ser recortado e os recortes reorganizados, sem superposição, de tal jeito que formem um quadrado.

77) Prove que as distâncias entre um ponto sobre uma circunferência e os quatro vértices de um quadrado nesta inscrita não podem ser todos números racionais.

78) Seja *ABCD* um quadrilátero convexo não trapézio, de diagonais *AC* e *BD* iguais. Tomamos sobre os lados *AB* e *CD*, respectivamente, pontos *P* e *Q* tais que:

$$\frac{\overline{AP}}{\overline{PB}}=\frac{\overline{DQ}}{\overline{QC}}=\frac{\overline{AD}}{\overline{BC}}$$

Mostre que os pontos *P* e *Q* são colinares com o ponto de interseção das mediatrizes dos lados *AD* e *BC*.

79) Temos uma fileira infinita de copos, cada um deles associado a um inteiro k, e um número finito de pedras distribuídas de alguma maneira por esses copos. Se há pelo menos duas pedras no copo k podemos pular uma pedra para o copo $k-1$ e outra para o copo $k+1$.
Prove que fazendo movimentos desse tipo um número suficientemente grande de vezes, chega-se necessariamente a uma situação onde não é possível fazer nenhum movimento desse tipo (i.e., onde há no máximo uma pedra em cada copo), e que a configuração final não depende da escolha dos movimentos durante o processo.

80) Sejam $\alpha = \frac{1+\sqrt{5}}{2}$, $A = \{\lfloor n\alpha \rfloor n \in \mathbb{N}^*\}$ e $B = \{\lfloor n\alpha^2 \rfloor n \in \mathbb{N}^*\}$. Prove que $A \cap B = \varnothing$ e $A \cup B = \mathbb{N}^*$.

Obs. $\lfloor x \rfloor$ é o inteiro tal que $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$.

Problema 74 proposto por Gibran M. de Souza (Natal - RN); Problema 75 proposto por Carlos A. Gomes (Natal - RN); Problema 76 proposto por Eduardo Casagrande Stabel (Porto Alegre - RS); Problemas 77 e 78 propostos por Evandro Makiyama de Melo (São Paulo - SP).

COORDENADORES REGIONAIS

Alberto Hassen Raad	(UFJF)	Juiz de Fora – MG
Amarísio da Silva Araújo	(UFV)	Viçosa – MG
Benedito Tadeu Vasconcelos Freire	(UFRN)	Natal – RN
Carlos Frederico Borges Palmeira	(PUC-Rio)	Rio de Janeiro – RJ
Claudio Arconcher	(Colégio Leonardo da Vinci)	Jundiaí – SP
Claus Haetinger	(UNIVATES)	Lajeado – RS
Cleonor Crescêncio das Neves	(UTAM)	Manaus – AM
Élio Mega	(Colégio Etapa)	São Paulo – SP
Florêncio Ferreira Guimarães Filho	(UFES)	Vitória – ES
Ronaldo Alves Garcia	(UFGO)	Goiânia – GO
Alexandra de Oliveira Abdala Cousin	(UEM)	Maringá – PR
Ivanilde Fernandes Saad	(UC. Dom Bosco)	Campo Grande– MS
Jacqueline Fabiola Rojas Arancibia	(UFPB)	João Pessoa – PB
João Benício de Melo Neto	(UFPI)	Teresina – PI
João Francisco Melo Libonati	(Grupo Educacional Ideal)	Belém – PA
José Carlos Pinto Leivas	(UFRG)	Rio Grande – RS
José Cloves Saraiva	(UFMA)	São Luis – MA
José Gaspar Ruas Filho	(ICMC-USP)	São Carlos – SP
José Luiz Rosas Pinho	(UFSC)	Florianópolis – SC
José Vieira Alves	(UFPB)	Campina Grande – PB
Licio Hernandes Bezerra	(UFSC)	Florianópolis – SC
Luzinalva Miranda de Amorim	(UFBA)	Salvador – BA
Marcelo Rufino de Oliveira	(Grupo Educacional Ideal)	Belém – PA
Marcondes Cavalcante França	(UFC)	Fortaleza – CE
Pablo Rodrigo Ganassim	(Liceu Terras do Engenho)	Piracicaba – SP
Ramón Mendoza	(UFPE)	Recife – PE
Reinaldo Gen Ichiro Arakaki	(INPE)	SJ dos Campos – SP
Ricardo Amorim	(Centro Educacional Logos)	Nova Iguaçu – RJ
Roberto Vizeu Barros	(Colégio Acae)	Volta Redonda – RJ
Rosângela Souza	(Colégio Singular)	Santo André – SP
Sérgio Cláudio Ramos	(IM-UFRGS)	Porto Alegre – RS
Tadeu Ferreira Gomes	(UEBA)	Juazeiro – BA
Tomás Menéndez Rodrigues	(U. Federal de Rondônia)	Porto Velho – RO
Valdenberg Araújo da Silva	(U. Federal de Sergipe)	São Cristovão – SE
Wagner Pereira Lopes	(CEFET – GO)	Jataí – GO