Aplicações de Combinatória e Geometria na Teoria dos Números

Nesse artigo vamos discutir algumas abordagens diferentes na Teoria dos Números, no sentido de envolverem também outras grandes áreas, como a Combinatória e a Geometria e, por que não, uma mistura dos dois.

1. Mas o que é Teoria dos Números?

A Teoria dos Números, falando de modo bastante simplificado, trata dos números inteiros e racionais. Por que há tanto trabalho com números inteiros? Vamos ver o que acontece com as operações com inteiros. Ao somarmos dois inteiros, obtemos um inteiro. Ao subtrairmos, também. Ao multiplicarmos também.

Até aí, nenhum problema. Mas e se quisermos *dividir* dois números inteiros? É inteiro ou não é? A resposta não é sim, nem não: é *depende*. Por exemplo, 4 dividido por 2 dá inteiro, mas 5 dividido por 3 não. Assim, uma das missões da Teoria dos Números é dizer quando uma expressão representa um número inteiro ou não.

E quando envolvemos operações um pouco mais complicadas como a radiciação, o problema fica cada vez mais complicado. Por exemplo, o problema de saber para que inteiros x, y, n positivos o número $\sqrt[n]{x^n + y^n}$ (o *Teorema de Fermat*) é inteiro demorou mais de 300 anos para ser resolvido e utiliza matemática extremamente avançada!

A base dos inteiros são os *números primos*, de modo que, para a Teoria dos Números, quanto mais soubermos dele, melhor. Os primos são os números que admitem exatamente *dois* divisores positivos: 1 e ele mesmo. Note que, com essa definição, 1 **não é primo**, pois admite somente um divisor.

2. Um toque de Combinatória

A *Combinatória*, por outro lado, quer saber da *existência* de coisas e, se possível, quer saber *quantas* delas existem. Na Combinatória, utilizamos, por exemplo, idéias da Teoria dos Conjuntos e fazemos contagens.

A primeira idéia combinatória que vamos explorar é a idéia de que os únicos conjuntos em que sempre podemos colocar um elemento a mais são os infinitos.

2.1. Uma das primeiras demonstrações da Matemática

Você já deve saber que existem infinitos primos. Mas você sabe por quê? A primeira demonstração conhecida desse fato vem da Antiguidade, e foi feita por Euclides.

Teorema 2.1. *Existem infinitos primos.*

Demonstração

Suponha o contrário, ou seja, que a quantidade de primos é finita. Seja $P = \{p_1, p_2, \ldots, p_n\}$ o conjunto de todos os primos. Agora, considere o sucessor do produto desses primos, ou seja,

$$N = p_1 p_2 \ldots p_n + 1$$

Todo inteiro é produto de primos, e N não é exceção. Mas nenhum dos primos p_i pode dividir N, porque N excede um múltiplo de p_i em 1. Assim N tem um divisor primo que não está em P, o que não é possível, porque P é o conjunto de *todos* os primos.

Isso é uma contradição, e portanto a quantidade de primos não pode ser finita, isto é, é infinita. ∎

2.2. Mais alguns conceitos da Teoria dos Números e uma idéia da Combinatória

Antes de continuar, vamos definir alguns conceitos importantíssimos da Teoria dos Números.

Definição 2.1. *Dois números são primos entre si quando não têm fator primo em comum.*

Definição 2.2. *Seja m um inteiro positivo maior do que 1. Dois números a e b são congruentes módulo m quando deixam o mesmo resto na divisão euclidiana (aquela que, bem, deixa restos) por m. Simbolizamos isso por*

$$a \equiv b \pmod{m}$$

Agora, uma idéia bastante simples, mas extremamente útil.

Princípio da Casa dos Pombos. *Se há $n+1$ pombos para serem colocados em n casas, haverá uma casa com pelo menos dois pombos.*

De forma ainda um pouco mais intuitiva:

Princípio da Casa dos Pombos (intuitivo). *Se há muitos pombos para poucas casas, alguma casa vai ter muitos pombos. E se há poucos pombos para muitas casas, haverá uma (ou até muitas!) casa(s) vazia(s).*

Utilizaremos essa idéia simples.

Exemplo 2.1.

Existe um inteiro positivo d tal que

$$3^d \equiv 1 \quad (\text{mód. } 2006)$$

Em palavras: alguma potência de 3 ($3^0 = 1$ não vale!) deixa resto 1 na divisão por 2006.

Resolução

Considere os restos das divisões por 2006 de

$$3, 3^2, 3^3, 3^4, \ldots$$

Há 2006 possíveis restos $(0, 1, 2, \ldots, 2005)$ e infinitas potências de 3. Então duas potências de 3, digamos, 3^k e 3^ℓ, $k > \ell$, deixam o mesmo resto da divisão por 2006. Isto quer dizer que $3^k - 3^\ell = 3^\ell(3^{k-\ell} - 1)$ é múltiplo de 2006. Como 2006 não tem fator 3, na verdade $3^{k-\ell} - 1$ é múltiplo de 2006 e, portanto, $3^{k-\ell}$ deixa resto 1 na divisão por 2006, de modo que podemos tomar $d = k - \ell$. ∎

Isso fica um pouco mais curto se utilizarmos a notação de congruência:

Resolução (o retorno)

Considere os números

$$3, 3^2, 3^3, \ldots \quad (\text{mód. } 2006)$$

Como há 2006 possíveis restos na divisão por 2006, existem duas potências de 3, digamos 3^k e 3^ℓ,$k > \ell$, que deixam o mesmo resto na divisão por 2006. Então

$$3^k \equiv 3^\ell \pmod{2006} \overset{(*)}{\iff} 3^{k-\ell} \equiv 1 \pmod{2006}$$

e podemos tomar $d = k - \ell$ ∎

Observação importante: A passagem $(*)$ que acabamos de fazer só pode ser feita quando o que cortamos (no caso, 3^ℓ) e o número no módulo (2006) são **primos entre si**.

O último exemplo pode ser generalizado:

Lema 2.1. *Se a e m são primos entre si, existe um inteiro positivo d tal que*

$$a^d \equiv 1 \pmod{m}$$

Em palavras: alguma potência de a ($a^0 = 1$ não vale!) deixa resto 1 na divisão por m.

A demonstração desse lema fica a cargo do leitor.

Isso prova também que

Lema 2.2. *Se a e m são primos entre si, existe um inteiro b, chamado inverso de a mód m tal que*

$$ab \equiv 1 \pmod{m}$$

Demonstração

Seja d tal que $a^d \equiv 1 \pmod{m}$. Então $b = a^{d-1}$. ∎

O próximo problema é de um teste de seleção para a equipe da Romênia da IMO e explora as idéias acima como um todo.

Exemplo 2.2.

(Teste de Seleção para a Equipe Romena da IMO 1997) Seja $a > 1$ um inteiro. Prove que o conjunto

$$\{a^2 + a - 1; a^3 + a^2 - 1; \ldots; a^{n+1} + a^n - 1; \ldots\}$$

admite um subconjunto infinito tal que quaisquer dois de seus elementos são primos entre si.

Resolução

A idéia é tomar um subconjunto B com a propriedade desejada e colocar mais um elemento. Se provarmos que conseguimos *sempre* colocar mais um elemento em B provamos a existência de um subconjunto infinito: basta seguir colocando elementos!

Comece com $B = \{a^2 + a - 1\}$. A cada etapa, seja P o produto de todos os elementos de B. Então vamos procurar n tal que $a^{n+1} + a^n - 1$ e P são primos entre si. Para isso, primeiro note que a e P são primos entre si, pois P é o produto de sucessores de múltiplos de a. Cada um desses sucessores não tem fator primo em comum com a e não vai ser multiplicando eles que vai aparecer algum fator comum.

Assim, como a e P são primos entre si, existe d tal que $a^d \equiv 1 \pmod{P}$. Logo

$$a^{d+1} + a^d - 1 \equiv a \cdot 1 + 1 - 1 \equiv a \pmod{P}$$

(você sabia que podemos substituir assim? É por isso que o símbolo de congruência é tão parecido com o igual!)

Assim, se $a^{d+1} + a^d - 1$ e P têm algum fator primo em comum, então esse fator deve estar em a. Mas sabemos que a e P não têm fator comum, logo $a^{d+1} + a^d - 1$ e P são primos entre si e, portanto, $a^{d+1} + a^d - 1$ e *qualquer elemento de B* são primos entre si. Ou seja, podemos colocar $a^{d+1} + a^d - 1$ em B, e acabou. ∎

2.3. Contar para provar!

Lembra que provamos que, dados inteiros a e m primos entre si, existe um inteiro positivo d tal que $a^d \equiv 1 \pmod{m}$? Na verdade, é possível encontrar uma fórmula para d. Faremos isso para m primo.

E faremos isso com uma contagem!

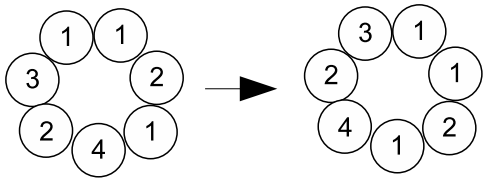
Faremos um exemplo numérico para facilitar.

Exemplo 2.3.

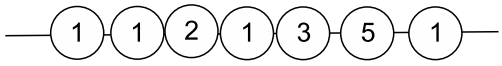
Vamos mostrar que $5^7 \equiv 5 \pmod 7$. Podemos passar o 1 para o outro lado e fatorar, mas vamos pensar combinatorialmente.

Resolução

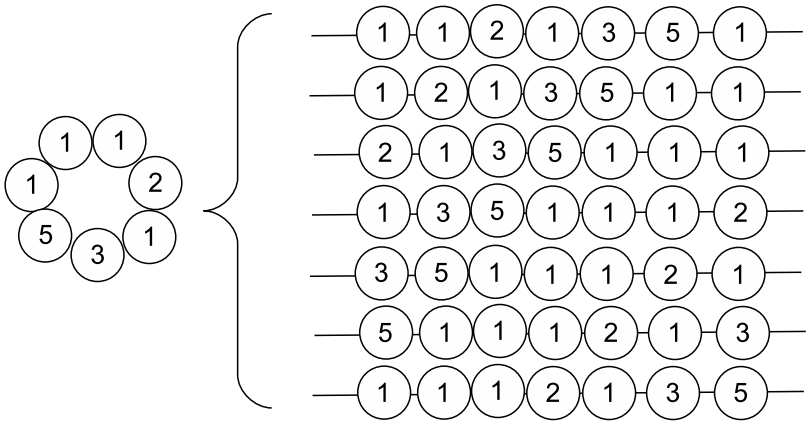
Suponha que temos linha e pedras de 5 tipos diferentes (que simplesmente numeraremos 1 a 5) para colocar na linha, formando um colar. No fio cabem exatamente 7 pedras. Quantos colares podemos formar? Note que o colar não muda se o girarmos.



Primeiro, imagine a linha do colar antes de amarrá-lo. Há 5 escolhas para cada uma das 7 pedras a serem colocadas, de modo que há 5^7 maneiras de escolhermos as pedras para serem colocadas na linha.



Agora, ao fecharmos o colar, podemos girá-lo de 7 maneiras. Note, então, que outras escolhas de pedras podem formar o mesmo colar:



Assim, devemos dividir 5^7 por... 7? Mas aí não vai dar inteiro! O que acontece é que os 5 colares com todas as pedras do mesmo tipo são formados pela mesma escolha de pedras.

Logo, na verdade devemos separar essas 5 escolhas primeiro e depois somar o que sobrou dividido por 7, de modo que o total de colares é $5 + \frac{5^7-5}{7}$. Para isso ser inteiro, $5^7 - 5$ tem que ser múltiplo de 7, ou seja, $5^7 \equiv 5 \pmod 7$. ∎

Você pode provar de modo completamente análogo o *pequeno teorema de Fermat*:

Teorema 2.2. *Seja p primo e a inteiro. Então $a^p \equiv a \pmod p$ ou, equivalementemente, $a^p - a$ é múltiplo de p.*

2.4. Mais casa dos pombos e primos como somas de dois quadrados

Muitos dos fatos mais interessantes da Teoria dos Números podem ser obtidos utilizando o princípio da casa dos pombos.

Lema 2.3. *Sejam m e n inteiros positivos primos entre si e sejam a e b inteiros positivos tais que $ab > n$. Então existe $x \in \{1, 2, \ldots, a-1\}$ e $y \in \{1, 2, \ldots, b-1\}$ tais que*

$$mx \equiv \pm y \pmod{n}$$

Demonstração

Considere as ab expressões da forma $mx + y$

$$\begin{array}{ccccc} m\cdot 1+1 & m\cdot 1+2 & m\cdot 1+3 & \cdots & m\cdot 1+b \\ m\cdot 2+1 & m\cdot 2+2 & m\cdot 2+3 & \cdots & m\cdot 2+b \\ m\cdot 3+1 & m\cdot 3+2 & m\cdot 3+3 & \cdots & m\cdot 3+b \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m\cdot a+1 & m\cdot a+2 & m\cdot a+3 & \cdots & m\cdot a+b \end{array}$$

Como $ab > n$, existem duas expressões que deixam o mesmo resto na divisão por n, digamos $mx_1 + y_1$ e $mx_2 + y_2$, com $x_1 > x_2$. Assim,

$$mx_1 + y_1 \equiv mx_2 + y_2 \pmod{n} \iff m(x_1 - x_2) \equiv y_2 - y_1 \pmod{n}$$

Note que $y_1 \neq y_2$ pois senão $x_1 = x_2$. Assim, sendo $x = x_1 - x_2$ e $y = |y_1 - y_2|$, temos $0 < x \leq a-1$ e $0 < y \leq b-1$ e

$$mx \equiv \pm y \pmod{n}$$

∎

Vamos mostrar mais uma aplicação de Combinatória, agora com contagem.

Lema 2.4. *Se $p = 4k+1$ é primo, existe x tal que $x^2 \equiv -1 \pmod{p}$.*

Demonstração

Vamos repartir o conjunto $\{1, 2, \ldots, p-1\}$ em conjuntos da forma $C_a = \{a, p-a, \overline{a}, p-\overline{a}\}$, em que $\overline{a}$ é o inverso de a mód p. Note que $C_1 = \{1, p-1\}$, pois o inverso de 1 mód p é 1. Além desse conjunto, como $p-1 = 4k$ é múltiplo de 4, deve haver mais um conjunto C_m com 2 elementos. Isso ocorre quando $m \equiv p - \overline{m}$ (mód. p) $\iff m^2 \equiv -m\overline{m} \equiv -1 \pmod{p}$. Note que não pode ocorrer $m \equiv p - m \pmod{p}$ nem $m \equiv \overline{m}$ (mód. p). ∎

Agora, vamos provar um dos teoremas mais belos da Teoria dos Números.

Teorema 2.3. *Todo primo da forma $p = 4k+1$ pode ser escrito como soma de dois quadrados.*

Demonstração

Sejam m tal que $m^2 \equiv -1 \pmod{p}$ (ele existe pelo lema anterior) e g o menor inteiro maior que $\sqrt{p}$. Assim $p < g^2$, e pelo primeiro lema desta seção, existem inteiros $x \in \{1, 2, \ldots, g-1\}$ e $y \in \{1, 2, \ldots, g-1\}$ tais que

$$mx \equiv \pm y \pmod{p} \implies m^2x^2 \equiv y^2 \pmod{p} \iff x^2 + y^2 \equiv 0 \pmod{p}$$

Assim, $x^2 + y^2$ é múltiplo de p e, como $0 < x, y < g$, $0 < x^2 < p$ e $0 < y^2 < p$, $0 < x^2 + y^2 < 2p$. Mas o único múltiplo de p entre 0 e $2p$ é p, ou seja, $p = x^2 + y^2$ pode ser escrito como soma de dois quadrados. ∎

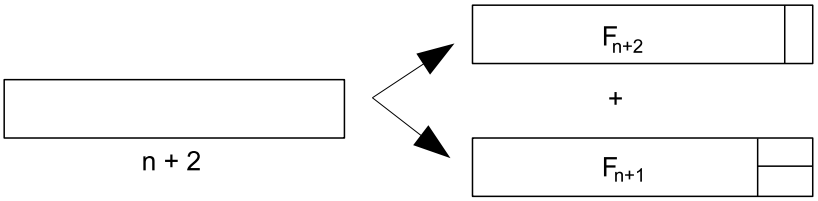
2.5. A seqüência de Fibonacci e um pouco de Combinatória

Uma das seqüências de números inteiros mais interessantes da Matemática é a de *Fibonacci*:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \ldots$$

Descobriu o padrão? Sim, é isso mesmo! Cada termo é a soma dos dois anteriores. Ou mais formalmente, $F_0 = 0$, $F_1 = 1$ e, para $n \geq 0$, $F_{n+2} = F_{n+1} + F_n$.

A verdade é que o $(n+1)$-ésimo termo da seqüência de Fibonacci é igual ao número de maneiras de preenchermos uma caixa $2 \times n$ com dominós. Com efeito, há $F_2 = 1$ maneira de preenchermos a caixa 2×1 e $F_3 = 2$ maneiras de preenchermos a caixa 2×2. Além disso, o número de maneiras de preenchermos a caixa $2 \times (n+2)$ é igual ao número de maneiras de preenchermos a caixa $2 \times (n+1)$ (se o seu último dominó está de pé) mais o número de maneiras de preenchermos a caixa $2 \times n$ (se o seus dois últimos dominós estão deitados).



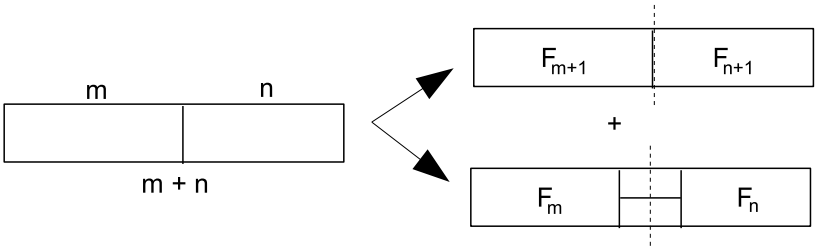
Uma identidade interessante que prova, entre outros fatos legais, que $\text{mdc}(F_m, F_n) = F_{\text{mdc}(m,n)}$, é

$$F_{m+n+1} = F_{m+1} \cdot F_{n+1} + F_m \cdot F_n \qquad (*)$$

Uma demonstração bem rápida utiliza uma das técnicas mais poderosas da Combinatória: a *contagem dupla*.

Vamos contar duas vezes o número de maneiras de preenchermos uma caixa $2 \times (m+n)$ com dominós.

A primeira a gente acabou de fazer: é F_{m+n}. A segunda é mais interessante: trace uma reta dividindo a caixa em duas caixas, uma $2 \times m$ e outra $2 \times n$. Tal reta pode atravessar um par de dominós deitados ou não. Vamos contar nos dois casos.



Logo $(*)$ está provado. ∎

3. Geometria

Como você pode ver, aplicações de Combinatória à Teoria dos Números são bastante freqüentes e, depois de ver alguns exemplo, até naturais.

Mas e a Geometria. O que o estudo das figuras tem a ver com números inteiros?

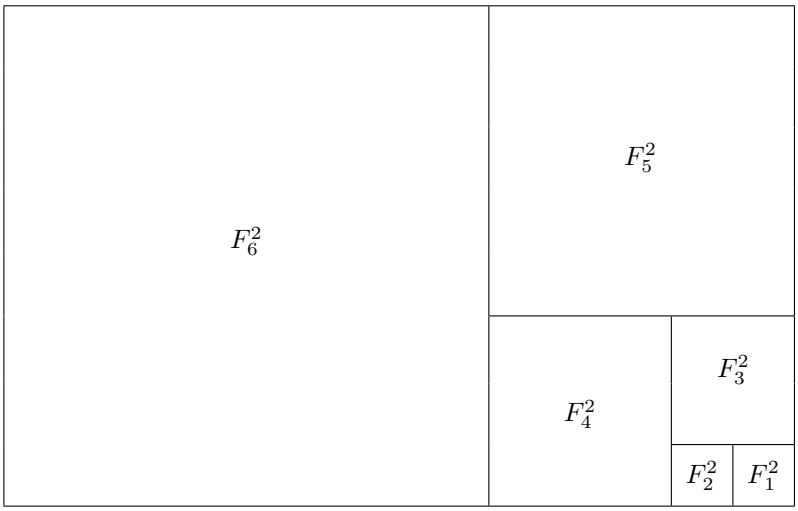
Uma das figuras mais simples da Geometria é o quadrado. Sabemos que a área de um quadrado de lado ℓ é ℓ^2. Será que é daí que vem o nome "quadrado perfeito"?

3.1. Mais uma identidade com Fibonacci: recortando quadrados de um retângulo

Outra identidade interessante com números de Fibonacci é

$$F_{n+1}F_n = F_n^2 + F_{n-1}^2 + \cdots + F_2^2 + F_1^2$$

Você consegue enxergá-la na figura a seguir, em que fizemos $n = 6$??



Essa idéia pode ser generalizada para resolver os seguintes problemas, que caíram no Torneio das Cidades:

Exercícios

01. (Torneio das Cidades) Na lousa estão escritos os números inteiros positivos x e y, $x < y$. Maria escreve em seu caderno o quadrado x^2 do menor deles, apaga a lousa e escreve os números x e $y - x$. Ela repete o procedimento acima (escreve quadrado do menor, apaga a lousa, escreve o menor e a diferença na lousa) até que um dos números seja zero. Qual é a soma dos números escritos no caderno de Maria?

02. (Torneio das Cidades) Na lousa estão escritos os números inteiros positivos x, y e z. João escolhe dois dos números, escreve o produto deles em seu caderno e apaga o número que sobrou, substituindo-o pelo antecessor. Ele repete o procedimento acima até que um dos números seja zero. Qual é a soma dos números escritos no caderno de João?

3.2. O Problema 6 da IMO 2001: como obter uma fatoração inacreditável com Geometria

Problema 6, IMO 2001. *Sejam a, b, c, d inteiros com $a > b > c > d > 0$. Considere que*

$$ac + bd = (b + d + a - c)(b + d - a + c).$$

Prove que $ab + cd$ não é um número primo.

Resolução

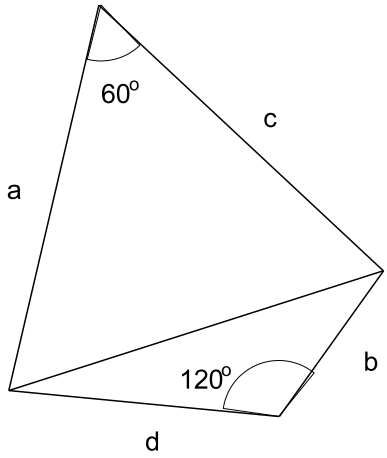
Primeiro, vamos abrir a equação dada. Obtemos $a^2 - ac + c^2 = b^2 + bd + d^2$.

E é aí que entra a Geometria.

3.3. Geometria? Onde? Alguns fatos da Geometria

É que triângulos com lados a, c e $\sqrt{a^2 - ac + c^2}$ têm um ângulo de $60°$. E o mais interessante, triângulos com lados b, d e $\sqrt{b^2 + bd + d^2}$ têm um ângulo de $120°$. Não vamos provar isso aqui, mas adiantamos que isso vem da lei dos co-senos.

E, do fato que $a^2 - ac + c^2 = b^2 + bd + d^2$ podemos construir dois triângulos com um lado comum:



3.4. Quadriláteros inscritíveis

Quando a soma de dois ângulos opostos de um quadrilátero é 180°, ele é inscritível, ou seja, existe um círculo que passa pelos seus quatro vértices (e isso não acontece com qualquer quadrilátero!).

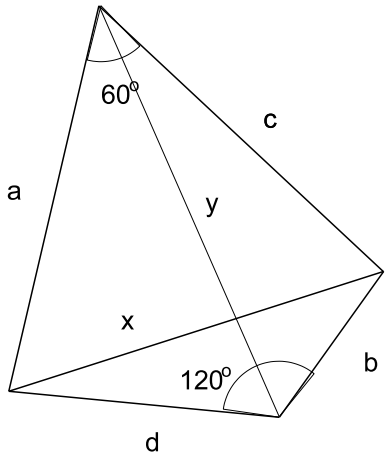
Em quadriláteros inscritíveis, vale o *teorema de Ptolomeu* (que também deixaremos sem demonstração):

Teorema 3.1. *Em todo quadrilátero inscritível $ABCD$,*

$$AC \cdot BD = AB \cdot CD + AD \cdot BC$$

Para você se situar: AC e BD são diagonais; AB e CD são um par de lados opostos; AD e BC são o outro par de lados opostos.

Vamos aplicar esse teorema! No nosso quadrilátero, $xy = ab + cd$. Opa! Apareceu $ab + cd$!



Com algumas contas envolvendo (novamente) a lei dos co-senos, obtemos

$$y^2 = \frac{(ab + cd)(ac + bd)}{ad + bc}$$

Assim, como $x^2y^2 = (ab+cd)^2$, e obtemos a nossa incrível fatoração!

$$\frac{(a^2-ac+c^2)(ab+cd)(ac+bd)}{ad+bc} = (ab+cd)^2 \iff (a^2-ac+c^2)(ac+bd) = (ab+cd)(ad+bc)$$

Agora, suponha que $ab+cd$ é primo. Então, como $(a-d)(b-c) < 0 \iff ac+bd < ab+cd$ (verifique!), $ac+bd$ não pode ter fator comum com $ab+cd$ (que seria o próprio). Então $ad+bc$ é múltiplo de $ac+bd$, o que implica $ad+bc \geq ac+bd$, o que é falso porque na verdade $ad+bc < ac+bd$ (verifique!). Logo $ab+cd$ não pode ser primo. ∎