

Problema

Dados $a, b \in \mathbb{N}$ tais que $ab + 1$ divide $a^2 + b^2$, prove que o quociente $Q = \frac{a^2+b^2}{ab+1}$ é um quadrado perfeito.

Sugestão:

Usar um método iterativo do tipo Algoritmo de Euclides.

Solução:

Podemos supor logo que $b > a > 0$, pois o caso $a = 0$ é trivial com $Q = b^2$. Dividindo b por a temos $b = ak + r$ com $0 \leq r < a$.

O caso $r = 0$: Neste caso temos que $a^2k + 1$ divide $a^2k^2 + a^2$ e facilmente se verifica que o quociente Q não pode ser nem menor que k , nem maior que k , ou seja, $Q = k$. Segue resolvendo a equação

$$(a^2k + 1)k = a^2k^2 + a^2,$$

que $b = a^3$ e $Q = a^2$.

O caso geral ($r \geq 1$): Vamos mostrar que o par $a, a - r$ satisfaz exactamente a mesma condição, isto é $a(a - r) + 1$ divide $a^2 + (a - r)^2$ com o mesmo quociente $Q = \frac{a^2+(a-r)^2}{a(a-r)+1}$. Isto mostra que podemos aplicar repetidas vezes este procedimento até encontrarmos um par de números $b' > a' > 0$ em que o resto da divisão de b' por a' seja zero. Então, pelo caso acima, o quociente será um quadrado perfeito. Mas como o quociente se mantém constante ao longo de todo o procedimento resulta que o quociente original Q é um quadrado perfeito.

Resta justificar a afirmação feita. Temos

$$(0.1) \quad (a^2k + ar + 1)Q = a^2k^2 + 2ark + r^2 + a^2.$$

Facilmente se verifica que Q não pode ser menor que k , nem maior que $k + 1$. Restam assim dois sub-casos a considerar: $Q = k$ e $Q = k + 1$. Vejamos que o primeiro caso, $Q = k$, é impossível. Simplificando (0.1) obtemos

$$(1 - ar)k = r^2 + a^2,$$

e esta equação só é possível quando $r = 0$, o que contaria a hipótese $r \geq 1$. Logo $Q = k + 1$, e a equação (0.1) é sucessivamente equivalente a

$$\begin{aligned} (a^2k + ar + 1)(k + 1) &= a^2k^2 + 2ark + r^2 + a^2 \\ \Leftrightarrow (a^2 - ar + 1)k &= a^2 + r^2 - ar - 1 \\ \Leftrightarrow (a(a - r) + 1)k &= (a - r)^2 + ar - 1 \\ \Leftrightarrow (a(a - r) + 1)(k + 1) &= (a - r)^2 + a^2 \\ \Leftrightarrow (a(a - r) + 1)Q &= (a - r)^2 + a^2. \end{aligned}$$