Foco em criptografia

Def: Sejam a e b inteiros dizemos que a é divisível por b, se existe um inteiro c tal que $b \cdot c = a$
Representação: $b \mid a$

Def: (PAR) Um inteiro é chamado "par" se ele é divisível por 2

Def: (IMPAR) Um inteiro a é chamado "impar" desde que haja um inteiro n tal que $a = 2n+1$

Def: (PRIMO) Um inteiro P é "primo" se $P > 1$ e se os únicos divisores de P são 1 e P

Def: (COMPOSTO) Um número a é chamado de composto se existe um número inteiro b tal que $1 < b < a$ e $b \mid a$

Teorema (Teo): é uma afirmação para a qual existe uma prova.

Conjectura: afirmação cuja veracidade não podemos garantir.

- Afirmação falsa - erros
- Afirmação absurda

Verdade Matemática

Se a e b são os comprimentos dos catetos de um triângulo retângulo e c é o comprimento da hipotenusa, então $a^2+b^2=c^2$

q p

Se p então q, $\boxed{p \Rightarrow q}$

Hipótese (Hip): a, b, c → lados do triângulo retângulo

Tese: $a^2+b^2=c^2$

Se p então q ⟶ $p \Rightarrow q$

Ex. "A soma de dois números inteiros é par"
"Se x e y são inteiros pares então x+y é par"

Se e somente se ⟶ $p \Leftrightarrow q$ ⟶ $p \Rightarrow q$, $q \Rightarrow p$

"Se um inteiro x é par, então x+1 é ímpar"

"Se $x+1$ é ímpar então x é um inteiro par"
"Um inteiro x é par se e somente se $x+1$ é ímpar"

Conjectura: todo inteiro par maior do que 2 é a soma de dois primos"

Proposição: → A soma de dois números par é par
→ Se x e y são pares então $x+y$ é um inteiro par

$\square$
$2|x$ — $x=2a$
$2|y$ — $y=2b$
$x+y = 2a+2b = 2.(a+b) = 2c$ $x+y=2c$
$2|(x+y) \to x+y$ é par $\blacksquare$

Afirmações

$\vdash x+x = 2x$
$\square$ $x+x = 1x+1x = (1+1)x = 2x$ $\blacksquare$

$\vdash (x-y)(x+y) = x^2-y^2$
$\square$ $(x-y)(x+y) = x.x + xy - xy - y.y = x^2-y^2$ $\blacksquare$