ITI
Instituto Nacional de Tecnologia da Informação

PSC e uma reflexão sobre a ICP-Brasil

Certforum 2018

BRASIL GOVERNO FEDERAL

Pergunta?

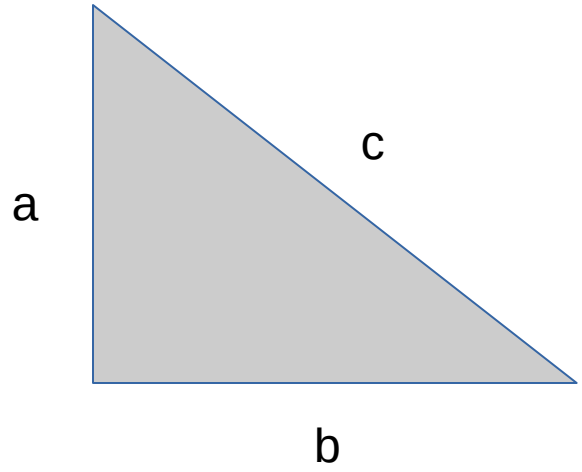
Imagem Fonte: dadsteachthebible.blogspot.com

Pergunta?

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

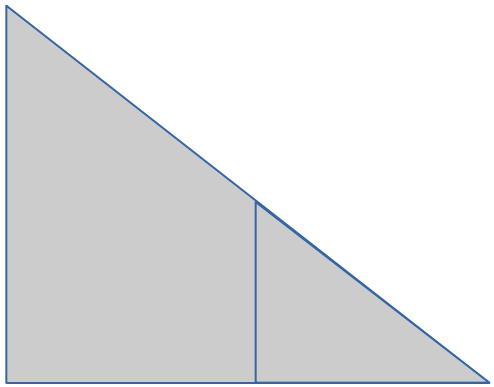
Teorema de Pitágoras

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



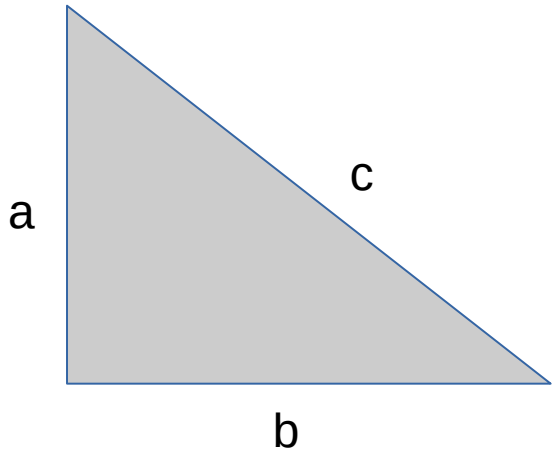
$$3^2 + 4^2 = 5^2$$

$$(3/5)^2 + (4/5)^2 = 1$$



Teorema de Pitágoras

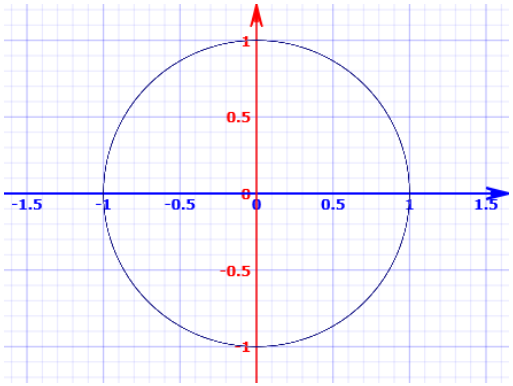
$$1^2 + 1^2 = ????^2$$

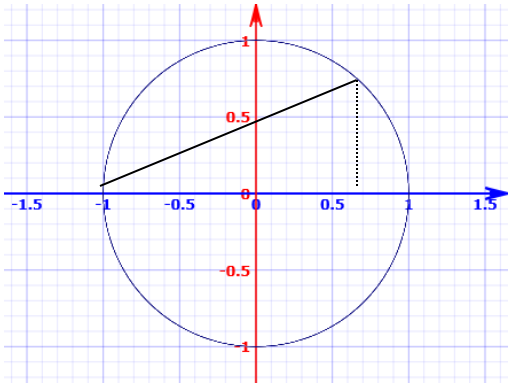


$$???? = 1{,}414\ldots$$

Análise Geométrica e Problema dos Números Congruentes

$(a/c)^2 + (b/c)^2 = 1$
$x^2 + y^2 = 1$

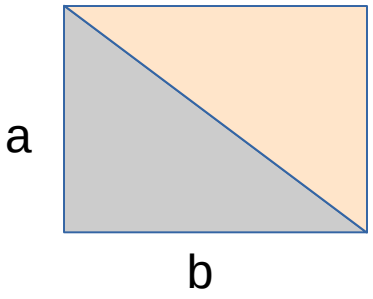




$y = t(x+1)$
$x^2 + y^2 = 1$

$x = 1-t^2/t^2+1$
$y= 2t/t^2+1$

Quais são as possíveis áreas inteiras de um triângulo reto com lados racionais?



$N = ½ ab$

Número 1 é congruente?

Álgebra

Coordenadas racionais com N = 1?

$$a = cx \qquad b = cy$$

$$\tfrac{1}{2}\, ab = \tfrac{1}{2}\, (cx)\,(cy)$$

$$\tfrac{1}{2}\, c^2\, xy = \tfrac{1}{2}\, c^2\, (1-t^2/t^2+1)(2t/t^2+1)$$

$$1 = c^2/(t^2+1)\,(1-t^2)t$$

$$(t^2+1)^2/c^2 = (1-t^2)t$$

$$(t^2+1/c)^2 = t-t^3$$

$$Y = t^2+1/c$$

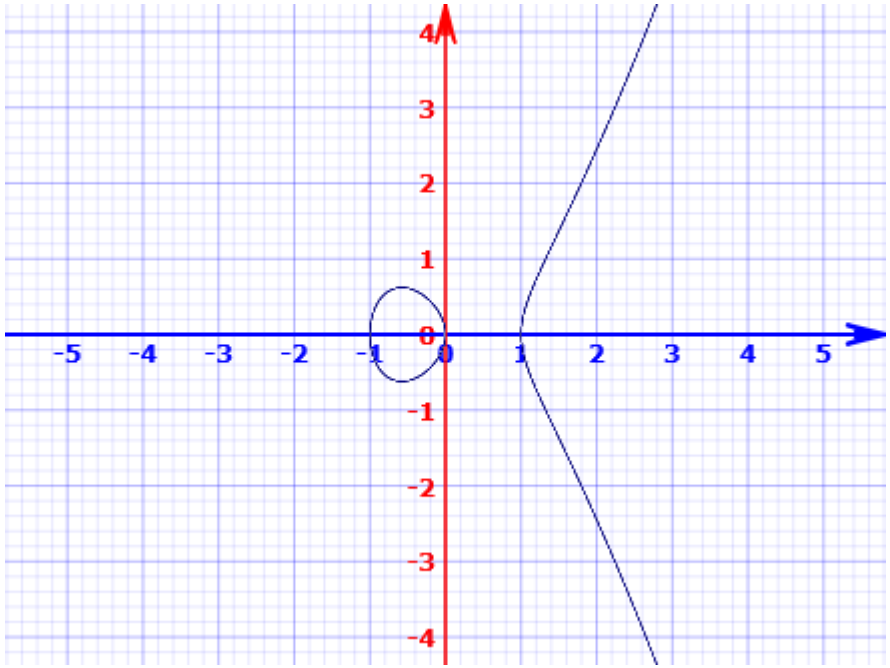
$$X = -t$$

$$Y^2 = X^3 - X$$

Fermat: As únicas soluções m em números racionais são com Y = 0, ou seja, 1 não é um número congruente

Curva de uma equação cúbica plana

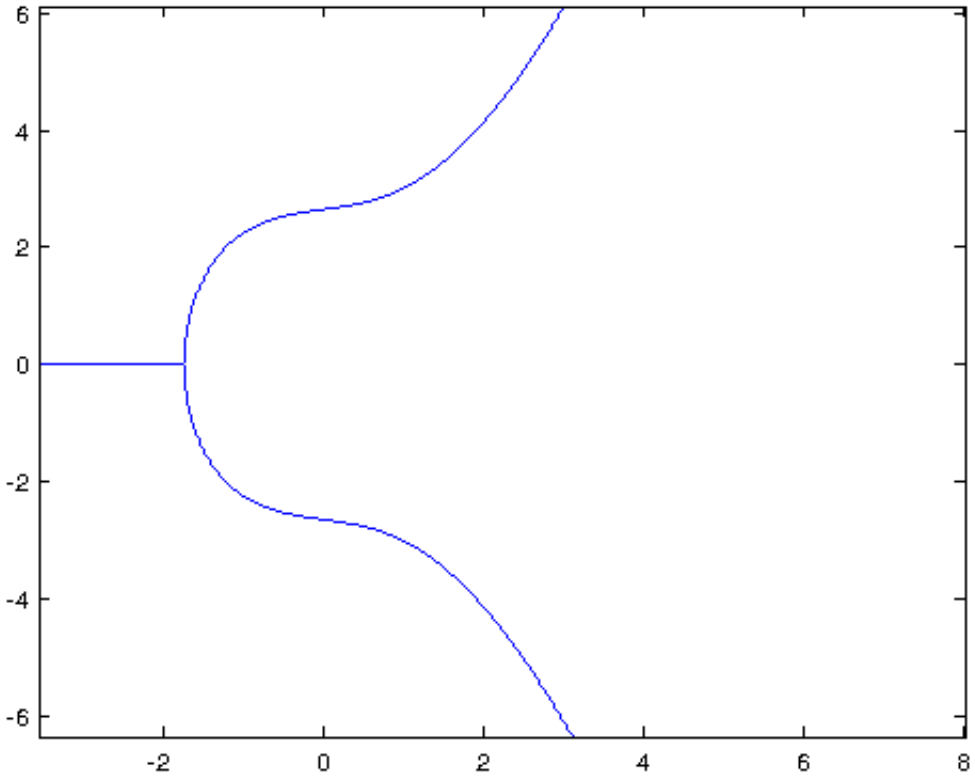
$$y^2 = x^3 - x$$



Curva Elíptica

Curva Elíptica – Bitcoin (secp256k1)

$$y^2 = x^3 + 7 \bmod 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$$



Reflexão

Imagem Fonte: keywordsuggest.org; carlosdamascenodesenhos.com.br

ITI
Instituto Nacional de Tecnologia da Informação

Futuro...

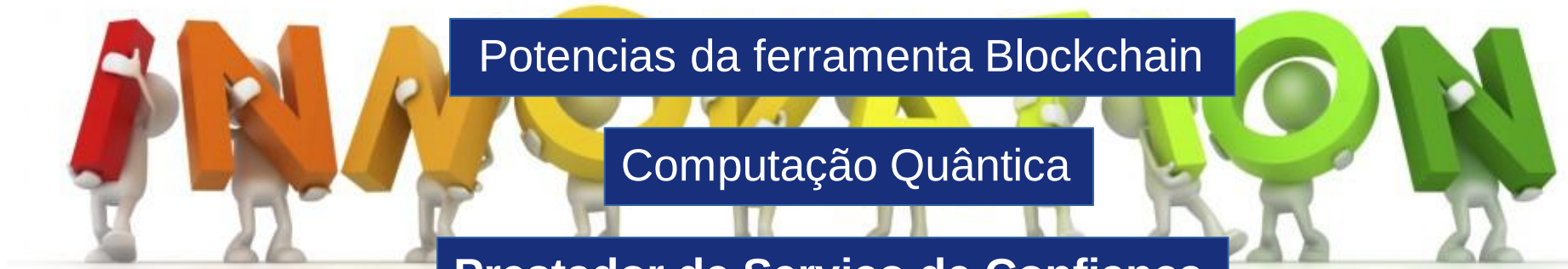
Nova legislação

Agenda Positiva

Novos procedimentos de identificação

Novos Algoritmos Criptográficos - ECC

Certificado para a Internet das Coisas - IoT



Potencias da ferramenta Blockchain

Computação Quântica

Prestador de Serviço de Confiança

Imagem Fonte: pmtic.net

Prestador de Serviço de Confiança

Armazenamento de Chaves Privadas em HSM

Portal de Serviço de Assinatura

Referências: DOC-ICP-17 e DOC-ICP-17.01

Imagem Fonte: quotesgram.com; freepik.es

Prestador de Serviço de Confiança

- Nível 4;
- Chave privada gerada no HSM (procedimentos de emissão permanecem o mesmo);
- HSM com certificação INMETRO;
- Controle e uso exclusivo do slot (chaves) no HSM por parte do usuário;
- Duplo fator de autenticação;
- SLA de 99,99%.

Imagem Fonte: darpa.mil

Prestador de Serviço de Confiança

- KMIP;

- Portabilidade;

- OAUTH 2.0;

Desafios...

- Comunicação direta dos web browsers ou app com o PSC (protocolo OAUTH 2.0);
- Aplicações full mobile (autenticação, assinatura e verificação);
- Ampliação da rede.

NOW MATTERS
(tema da RSA Conference 2018)

Imagem Fonte: leitorcabuloso.com.br

Eduardo Lacerda

ASSESSOR

(61) 3424-3875

eduardo.lacerda@iti.gov.br

www.iti.gov.br