Equações do tipo $x^2 + Dy^2 = A$

Diego Eloi

13 de janeiro de 2015

Equações do tipo $x^2+Dy^2 = A$ aparecem em alguns problemas de olimpíada. Para resolvê-las, é importante ter uma noção de como resolver equações diofantinas quadráticas. Aprenderemos um pouco mais sobre como resolver este tipo de equação. Antes de tudo, uma breve revisão de reciprocidade quadrática. Seja a um inteiro e m um natural tais que $mdc(a, m) = 1$. Dizemos que a é um *resíduo quadrático* módulo m quando existe um inteiro x tal que $x^2 \equiv a(mod\, m)$.
Por exemplo, 4 é resíduo quadrático módulo 5, pois $2^2 \equiv 4(mod\, 5)$, mas 5 não é resíduo quadrático módulo 8, pois um quadrado módulo 8 só pode ser congruente a 0, 1 ou 4.
Exemplo: Encontre todas as soluções inteiras da equação $x^2-8y^2+12 = 2015$.
Solução: Olhando a equação módulo 8, veja que chegamos a:

$$x^2 \equiv 3(mod\, 8)$$

Então essa equação não possui solução nos inteiros, pois, como já sabemos, nenhum quadrado é 3 módulo 8.
Para tais problemas, podemos utilizar propriedades aprendidas quando estudamos reciprocidade quadrática. Como em muitos problemas relacionado aos inteiros, basta olharmos para os números primos. Seja p um primo ímpar, o *símbolo de Legendre* é dado por:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{se a é resíduo quadrático módulo p,} \\ -1, \text{se a não é resíduo quadrático módulo p,} \\ 0, \text{se } p|a. \end{cases}$$

Para p e q números primos ímpares, valem algumas propriedades do símbolo de Legendre:
1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}(mod\, p)$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. $\left(\frac{a^2}{p}\right) = 1$, se $a \not\equiv 0(mod\, p)$
4. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
5. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

6. (**Lei da Reciprocidade Quadrática**) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

Exercício: Mostre que a equação $x^2 - 17y^2 = 12$ não possui soluções inteiras.

Exercício: Sejam p e q primos congruentes a 3 módulo 4. Mostre que a equação

$$x^2 - py^2 = q$$

não possui soluções inteiras.

Lema de Thue: Seja p um primo e a um inteiro tal que $mdc(a, p) = 1$. Então, existem inteiros x e y tais que $ax \equiv y(mod\ p)$ com $0 < |x|, |y| < \sqrt{p}$.

Lema Importante: Seja $D \in N$ e seja p um número primo tal que $mdc(D, p) = 1$. Se existem x e y inteiros tais que $x^2 + Dy^2 = p$, então $-D$ é um quadrado módulo p

Teorema: Seja $D \in N$ e p um primo ímpar tal que $\left(\frac{-D}{p}\right) = 1$. Então, existem k, x, $y \in Z$ com $0 \leq k < D$ e $0 < |x|, |y| < \sqrt{p}$ tais que:

$$x^2 + Dy^2 = kp$$

Exercício: Prove que são equivalentes:
(i) $\exists x, y \in Z$ tais que $x^2 + 2y^2 = p$
(ii) $\left(\frac{-2}{p}\right) = 1$
(iii) $p \equiv 1, 3(mod\ 8)$

Problema 1 (India 2014) Seja p um número primo tal que $p|2a^2 - 1$para algum inteiro a. Mostre que existem inteiros b e c tais que $p = 2b^2 - c^2$.

Problema 2 Seja n um inteiro ímpar maior que 1. Prove que a equação

$$x^n + 2^{n-1} = y^2$$

não possui soluções inteiras.

Problema 3 Mostre que a equação $x^2 - 3y^2 = p$ não possui soluções inteiras para $p = 2$ ou $p = 3$.

Problema 4 Mostre que a equação $x^3 - x^2 + 8 = y^2$ não possui soluções inteiras.

Problema 5 Sejam a e b inteiros primos entre si e p um primo ímpar tal que $p|a^2 + b^2$, mostre que $p \equiv 1(mod\ 4)$

Problema 6 (Balcânica) Resolva a equação abaixo nos inteiros

$$x^5 - y^2 = 4$$