Equação de Pell Generalizada

Guilherme Zeus; Lecturer: Rafael Filipe

§1 Equação de Pell

Uma equação de Pell é uma equação do tipo

$$x^2 - D \cdot y^2 = 1,$$

com D não quadrado perfeito, para variáveis x e y inteiros positivos.

Teorema 1.1 Existe solução para toda equaçãoo de Pell.

Teorema 1.2 Existe uma solução minimal (x_0, y_0), que vamos representar como $x_0 + y_0\sqrt{D}$. Todas as soluções são da forma

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$$

§1.1 Como achar soluções para a equação de Pell

- Usar frações contínuas.

§1.2 Olhar as soluções da Equação de Pell como uma recorrência

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$$
$$x_n - y_n\sqrt{D} = (x_1 - y_1\sqrt{D})^n$$

Logo:

$$x_n = \frac{(x_1 + y_1\sqrt{D})^n + (x_1 + y_1\sqrt{D})^n}{2}$$
$$y_n = \frac{(x_1 + y_1\sqrt{D})^n - (x_1 + y_1\sqrt{D})^n}{2\sqrt{D}}$$

Portanto, ambas as seqências (x_n) e (y_n) seguem a recorrência:

$$u_{n+2} - 2x_1 u_{n+1} + u_n = 0$$

§2 Equação de Pell Generalizada

Agora, vamos resolver equações do tipo

$$x^2 - Dy^2 = C.$$

Nesse caso, nem sempre tem solução (e.g., $x^2 - 3y^2 = 7$ não possui solução[1]). Além disso, mesmo quando existe uma solução, não existe necessariamente uma única solução minimal, mas na verdade várias soluções minimais e uma família de soluções para cada uma delas.

[1] Basta ver módulo 4.

Teorema 2.1 Seja (x_0, y_0) a solução da equação de Pell $x^2 - Dy^2 = 1$.
Se (x, y) é solução de $x^2 - Dy^2 = C$, então

$$x + y\sqrt{D} = (u + v\sqrt{D})(x_1 + y_1\sqrt{D})^k,$$

com k inteiro e $u^2 - Dv^2 = C$,

$$u + v\sqrt{D} < (x_1 + y_1\sqrt{D})\sqrt{|C|}$$

Usando o teorema acima, podemos achar todas as soluções dessa generalização da equação de Pell.

§3 Um Truque Especial

Teorema 3.1 Em uma recorrência de segunda ordem $a_{n+2} + ba_{n+1} + ca_n = 0$, seja p um primo e T_p o período dessa sequência módulo p. Podemos achar T_p usando que:

- Se $\left(\frac{b^2-4c}{p}\right) = 1$, então $T_p | p - 1$.
- Se $\left(\frac{b^2-4c}{p}\right) = 1$, então $T_p | p^2 - 1$.
- Se $b^2 - 4c \equiv 0 \pmod{p}$, então $p | T_p$ e $T_p | p(p - 1)$.