La Ecuación de Pell y sus aplicaciones criptográficas

Soledad Villar

Universidad de la República, Facultad de Ciencias

4 de diciembre de 2009

Motivación

- La ecuación de Pell es interesante en sí misma, y este es un enfoque distinto al aritmético.
- Permite encontrar la relación entre un grupo que proviene de la geometría y el grupo multiplicativo de $\mathbb{F}_p$.
- Es el caso base para estudiar sistemas criptográficos en curvas de género más grande.

Motivación

- La ecuación de Pell es interesante en sí misma, y este es un enfoque distinto al aritmético.
- Permite encontrar la relación entre un grupo que proviene de la geometría y el grupo multiplicativo de $\mathbb{F}_p$.
- Es el caso base para estudiar sistemas criptográficos en curvas de género más grande.

Motivación

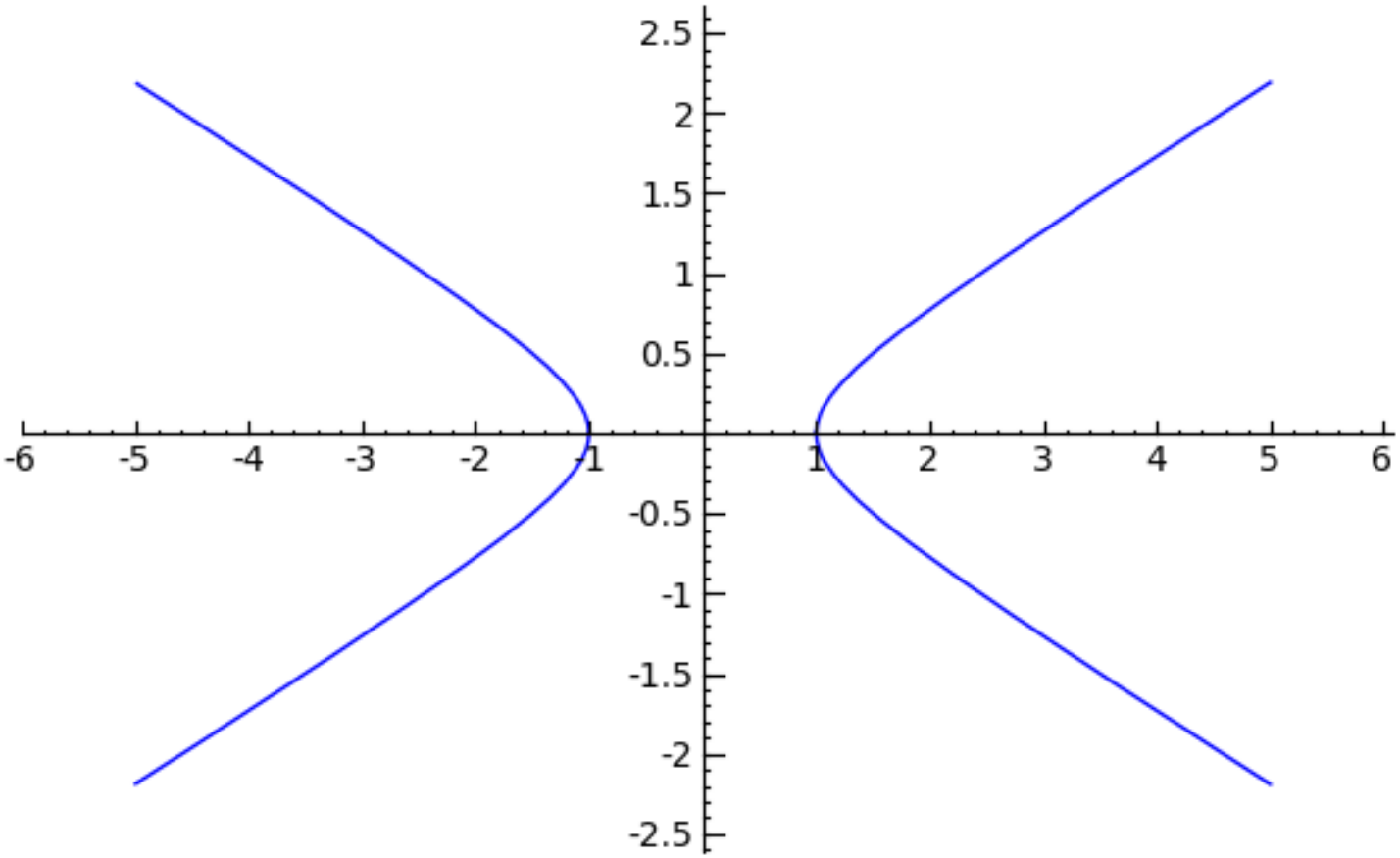
- La ecuación de Pell es interesante en sí misma, y este es un enfoque distinto al aritmético.
- Permite encontrar la relación entre un grupo que proviene de la geometría y el grupo multiplicativo de $\mathbb{F}_p$.
- Es el caso base para estudiar sistemas criptográficos en curvas de género más grande.

Motivación

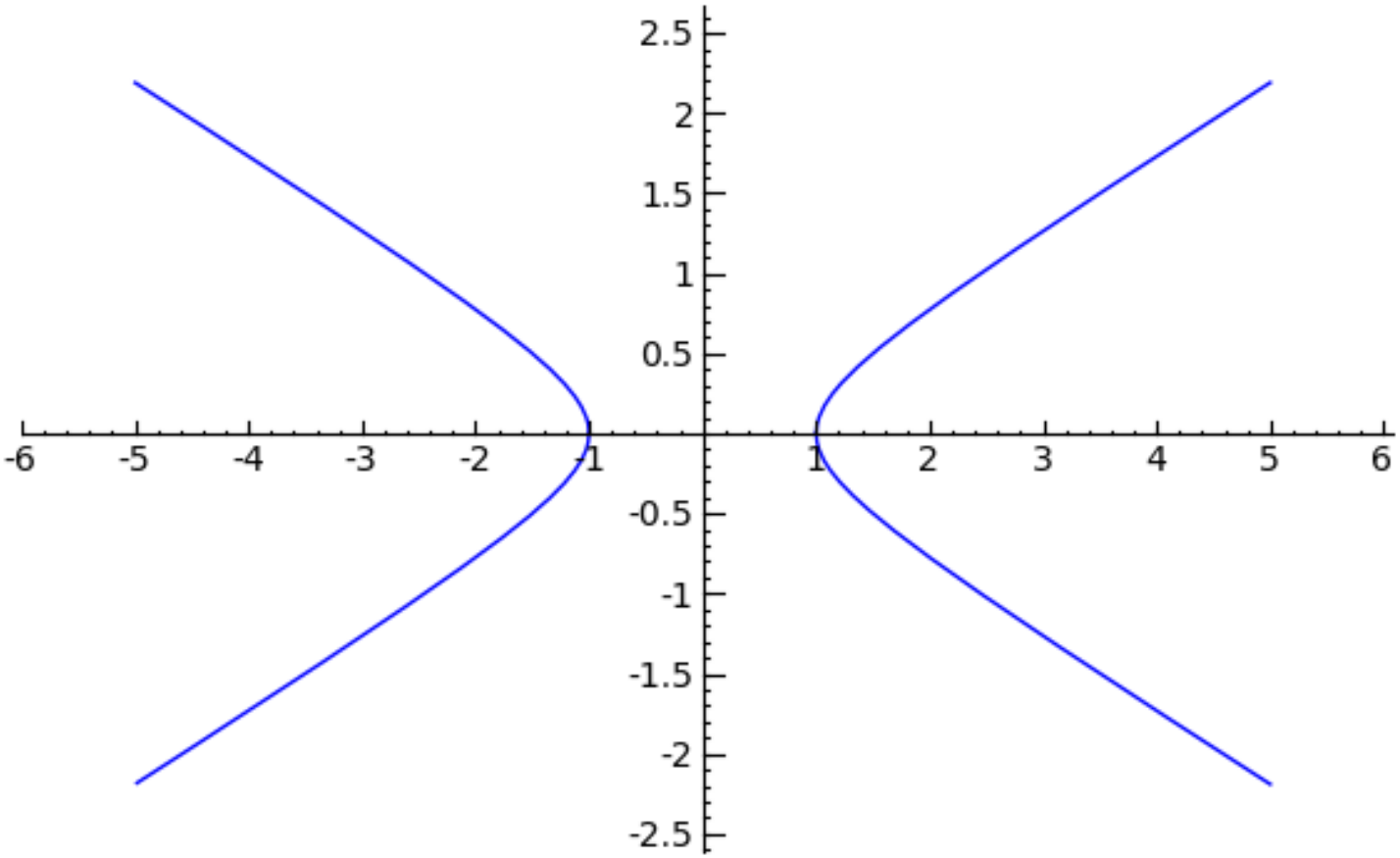
- La ecuación de Pell es interesante en sí misma, y este es un enfoque distinto al aritmético.
- Permite encontrar la relación entre un grupo que proviene de la geometría y el grupo multiplicativo de $\mathbb{F}_p$.
- Es el caso base para estudiar sistemas criptográficos en curvas de género más grande.

La ecuación de Pell

$x^2 - Dy^2 = 1$ *donde* $D > 0$ *no es un cuadrado*



Se define geométricamente una operación de suma en el conjunto de puntos $\mathcal{P}(\mathbb{R})$:



Descripción algebraica de la operación

Proposición

La operación definida anteriormente es equivalente a esta otra definición:
Si $P = (r, s)$ *y* $Q = (t, u)$ *ambos puntos en* $\mathcal{P}(\mathbb{F}_p)$*, entonces definimos* $P + Q = (rt + Dsu, ru + st)$

Demostración.

Observar que $P + Q \in \mathcal{P}(\mathbb{F}_p)$ (verifica la ecuación de Pell) y que si $N = (1, 0)$, la pendiente de $\overline{PQ}$ coincide con la pendiente de $\overline{N(P + Q)}$. □

Teorema

Sea p un primo impar. Consideramos la cónica de Pell $\mathcal{P} : x^2 - Dy^2 = 1$, donde $p \nmid D$.
Entonces $\mathcal{P}(\mathbb{F}_p)$ es un grupo cíclico de cardinal

$$\#\mathcal{P}(\mathbb{F}_p) = \begin{cases} p+1, & si \left(\frac{D}{p}\right) = -1 \\ p-1, & si \left(\frac{D}{p}\right) = 1 \end{cases}$$

Consideramos todas las rectas por $N = (1, 0)$ con pendiente $m \in \mathbb{F}_p$.

Para cada recta la intersección con la cónica de Pell es:

$$P = (1, 0) \text{ y } P_m = \left(\frac{Dm^2+1}{Dm^2-1}, \frac{2m}{Dm^2-1}\right).$$

Si $Dm^2 - 1 = 0$ no tiene solución módulo p, entonces $\#\{P_m\} = p$ y si tiene solución $\#\{P_m\} = p - 2$

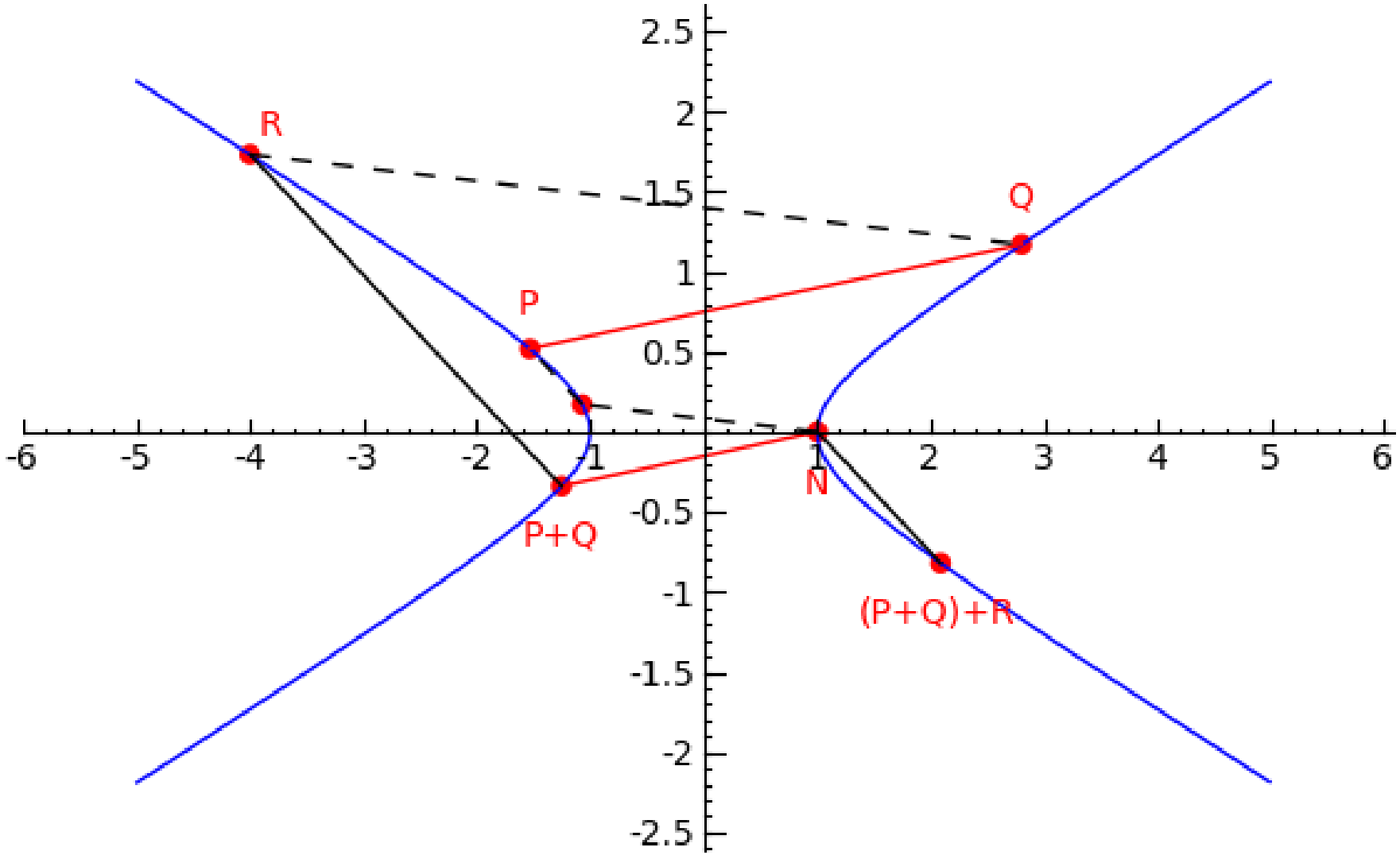
Asociatividad de la operación

Teorema (Pascal)

Sean A, B, C, D, E, F seis puntos sobre una cónica. Si $\overline{AB} \parallel \overline{DE}$ y $\overline{BC} \parallel \overline{EF}$, entonces $\overline{CD} \parallel \overline{FA}$.

Teorema (Asociatividad de +)

Sean $P, Q, R \in \mathcal{P}(\mathbb{F}_p)$, entonces $(P + Q) + R = P + (Q + R)$


R
Q
P
P+Q
N
(P+Q)+R
2.5
2
1.5
1
0.5
-0.5
-1
-1.5
-2
-2.5
-6
-5
-4
-3
-2
-1
1
2
3
4
5
6

Demostración.

Considerar los puntos $P, Q, R, P+Q, N, Q+R$ sobre la curva $\mathcal{P}(\mathbb{F}_p)$. Para ver que estamos en las hipótesis del teorema de Pascal basta observar:

- $\overline{PQ} \parallel \overline{(P+Q)N}$
- $\overline{QR} \parallel \overline{N(Q+R)}$

$\Rightarrow$ El teorema de Pascal afirma que $\overline{P(Q+R)} \parallel \overline{(P+Q)R}$, lo que implica que las paralelas por N a ambas rectas coinciden, y por lo tanto

$$(P+Q)+R = P+(Q+R)$$

Estructura del grupo

Si $D = a^2 \bmod p$

$$\begin{aligned} \psi : (\mathcal{C}_p, +) &\rightarrow (\mathbb{F}_p^{\times}, \times) \\ (1,0) &\mapsto 1 \\ (x,y) &\mapsto x - ay \bmod p \end{aligned}$$

ψ es de hecho un isomorfismo, donde:

$$\begin{aligned} \psi^{-1} : (\mathbb{F}_p^{\times}, \times) &\rightarrow (\mathcal{C}_p, +) \\ u &\mapsto \left(\frac{u + u^{-1}}{2}, \frac{u - u^{-1}}{2a} \right) \end{aligned}$$

Entonces $(\mathcal{C}_p, +) \simeq (\mathbb{F}_p^{\times}, \times)$ y por lo tanto el grupo de puntos de la cónica de Pell con $D = a^2 \bmod p$ es un grupo cíclico de orden $p - 1$.

Si $D \neq \square \bmod p$, consideramos $\mathbb{F}_{p^2} = \mathbb{F}_p[\sqrt{D}]$ y el siguiente homomorfismo:

$$\begin{aligned} \psi : (\mathcal{C}_p, +) &\rightarrow (\mathbb{F}_{p^2}^{\times}, \times) \\ (x, y) &\mapsto x + y\sqrt{D} \bmod p \end{aligned}$$

En este caso, ψ no es sobreyectivo.
De hecho, la imagen de ψ es $\{x + y\sqrt{D} : x^2 - Dy^2 = 1\}$, es decir los elementos de norma 1.

En particular es un grupo cíclico.

Aplicaciones criptográficas - RSA

A	E	B
elige dos primos grandes p y q; calcula $N = pq$; elige e coprimo con $\Phi(N)$ (el orden del grupo): $\Phi(N) := (p - (\frac{D}{p}))(q - (\frac{D}{q}))$ Si d, e tal que $de \equiv 1 \bmod \Phi(N)$ clave pública: (N, e, D); clave privada: d	$\xrightarrow{(N, e, D)}$	codifica su mensaje a un punto de la curva: $m \mapsto P$; encripta el mensaje como $C = eP$;
conociendo que $de \equiv 1 \bmod \Phi(N)$ computa $P = dC$ y decodifica $P \mapsto m$	$\xleftarrow{C}$	

Aplicaciones criptográficas - ElGamal

A	E	B
elige $a \in \mathbb{F}_p^\times$; si G es un generador del grupo de puntos $A = aG$ es la clave pública;		
	$\xrightarrow{A}$	
		codifica su mensaje a un punto de la curva: $m \mapsto P$; elige $b \in \mathbb{F}_p^\times$ al azar $B = bG$ encripta el mensaje como $C = P + bA$;
	$\xleftarrow{B, C}$	
$P = C + (p - a)B \bmod p$ $P \mapsto m$		