bilhar de Poncelet e criptografia

Israel Vainsencher

UFMG

http://www.mat.ufmg.br/∼israel

laptop financiado pelo CNPq

BRASIL
UM PAÍS DE TODOS

transmissão segura

Ana quer enviar uma mensagem secreta ao Bruno, mas não confia no portador.

Ela remete numa caixa fechada

com um cadeado inviolável.

Bruno recebe a caixa,
mas é claro que não conseguirá
abrir o cadeado da Ana. . .

(DIC. AURÉLIO) inviolável: impossível de ser aberto, até mesmo pelo super

Bruno...

:-(

Esperto, ele põe outro cadeado

e devolve a caixa para Ana.

Ela retira o seu cadeado

Ela retira o seu cadeado

e re-envia a caixa ao Bruno, que agora pode abrir e ler o segredo!
(-:Simon Singh, *The Code Book*.:-)

Na “prática”, digamos que o segredo da caixa fosse “QUERO IR AO CINEMA COM VOCÊ”.

A mensagem vai por email.
Antes, é *digitalizada e criptografada.*

digitalizar?

Transformar letras em números.

Um esquema corrente

é ± o seguinte.

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	21	22	23	24

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
25	26	27	28	29	31	32	33	34	35	36	37	38	00

espaço entre palavras:

modo de usar

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	21	22	23	24

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
25	26	27	28	29	31	32	33	34	35	36	37	38	00

$$153127111326001525322915002711231134291131\ (??!)$$

15	31	27	11	13	26	00	15	25	32	29	15	00	27	11	23	11	34	29	11	31
E	S	P	A	C	O		E	N	T	R	E		P	A	L	A	V	R	A	S

A N A

11 25 11

ANA (em digital) = 112511.

1229332526 = ??

exercício

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	21	22	23	24

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
25	26	27	28	29	31	32	33	34	35	36	37	38	00

$$29191311291426001326291113112600141500231511 26$$

$$(??!)$$

——os 300 primeiros que acertarem, ganham u

(clique para ver a resposta)

bobo, use spacebar!!!!!

resposta

RICARDO CORACAO DE LEAO

RICARDO CORACAO DE LEAO

RICARDO CORACAO DE LEAO

RICARDO CORACAO DE LEAO

RICARDO CORACAO DE LEAO

RICARDO CORACAO DE LEAO

RICARDO CORACAO DE LEAO

Apenas digitalizar, não torna
a transmissão segura.
O “cadeado” da Ana é
operacionalizado embaralhando
a mensagem digitalizada.

cripto. . .

A arte na criptografia é inventar regras de embaralhamento.

Uma regra em uso, de maneira muuuuuuuuito simplificada, consiste no seguinte. Ana escolhe um número (só dela),

digamos 111 ($= \mathrm{chave_A}$),
e *multiplica* a mensagem:

28 33 15 29 26 00 19 29 00 11 26 00 13 19 25 15 24 11 00 13 26 24 00 34 26 13 15

$\times 111 =$

$$3144799747862141191249861464369191762114721264380300596 5$$

Nem tente decifrar, pois o número acima não provém de qualquer frase. (POR QUE?)

Mas é isso

$$3144799747862141191249861464369191762114721264380300596 5$$

que o pobre do Bruno recebe. . .
Digamos que o “cadeado” dele seja multiplicação por 113:

$$3144799747862141191249861464369191762114721264380300596 5 \times 113 =$$

$$355362371508421954611234345473718669118963502874973967404 5;$$

é o que Ana tem de volta.

A retirada do cadeado da Ana significa fazer a operação inversa:

$$35536237150842195461123434547371866911896350287497396740 45 \div 111 =$$
$$32014628063821797712723814907542222443149865123871528595$$

Por fim, Bruno recebe a cifra acima, e divide por sua “chave secreta”:

$$32014628063821797712723814907542222443149865123871528595 \div 113 =$$

$$28331529260019290011260013192515241100132624034261315$$

Q U E R O I R A O C I N E M A C O M V O C E

que agora faz perfeito sentido!

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	21	22	23	24

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
25	26	27	28	29	31	32	33	34	35	36	37	38	00

Em resumo,
Ana codifica sua mensagem
(digitalizada) M
fazendo a operação

$$\boxed{\mathrm{M} \rightsquigarrow \mathrm{M}' = \mathrm{chave}_{\mathrm{A}} \times \mathrm{M}.}$$

Bruno devolve

$$\begin{aligned} \mathrm{M}'' &= \mathrm{chave_B} \times \mathrm{M}' \\ &= \mathrm{chave_B} \times (\mathrm{chave_A} \times \mathrm{M}). \end{aligned}$$

Ana retorna

$$\begin{aligned} \mathrm{M}''' &= \mathrm{chave_A}^{-1}(\mathrm{chave_B} \times (\mathrm{chave_A} \times \mathrm{M})) \\ &= \mathrm{chave_B} \times \mathrm{M} \end{aligned}$$

e por fim, Bruno faz

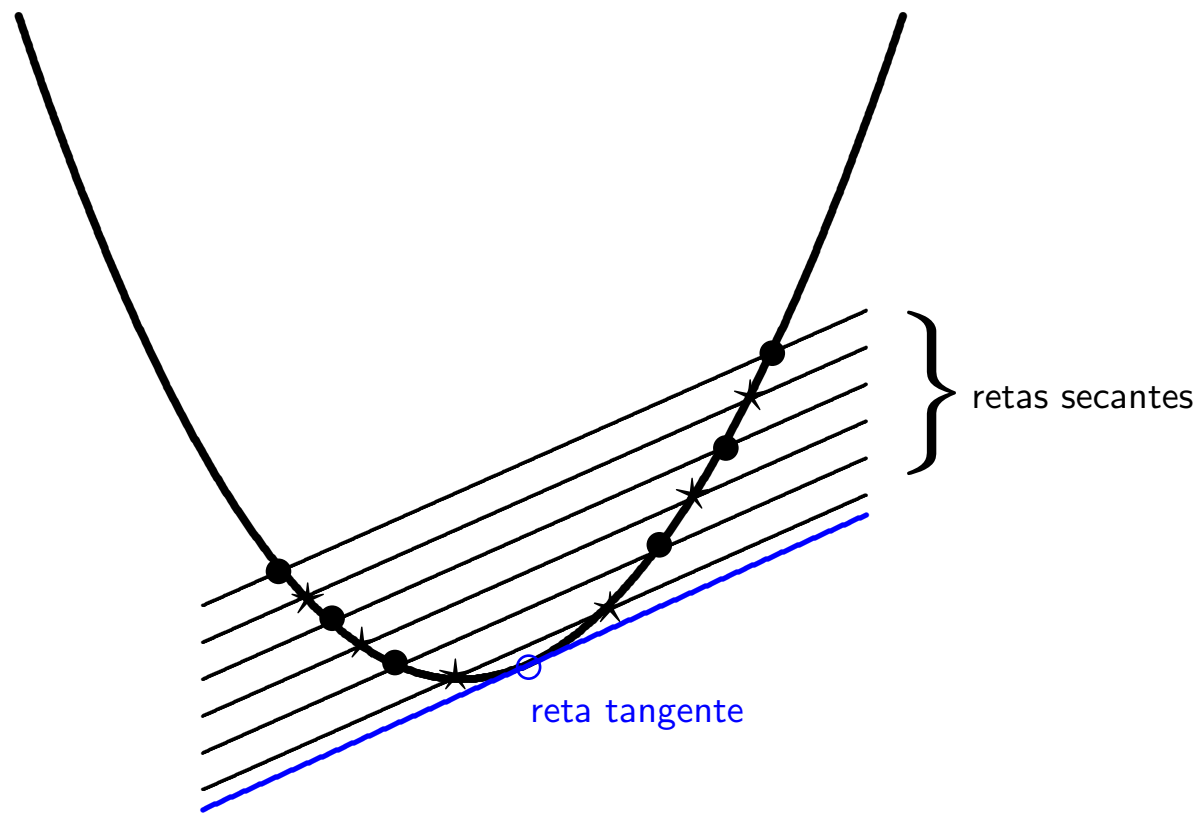
$$\mathrm{chave_B}^{-1}\mathrm{M}''' = \mathrm{M}.$$

Na realidade, embora a digitalização seja de fato quase do jeito que descrevemos, as operações de embaralhamento são bem mais sofisticadas. Veremos adiante um exemplo mais próximo da realidade.

tangentes a uma parábola

$y = x^2$

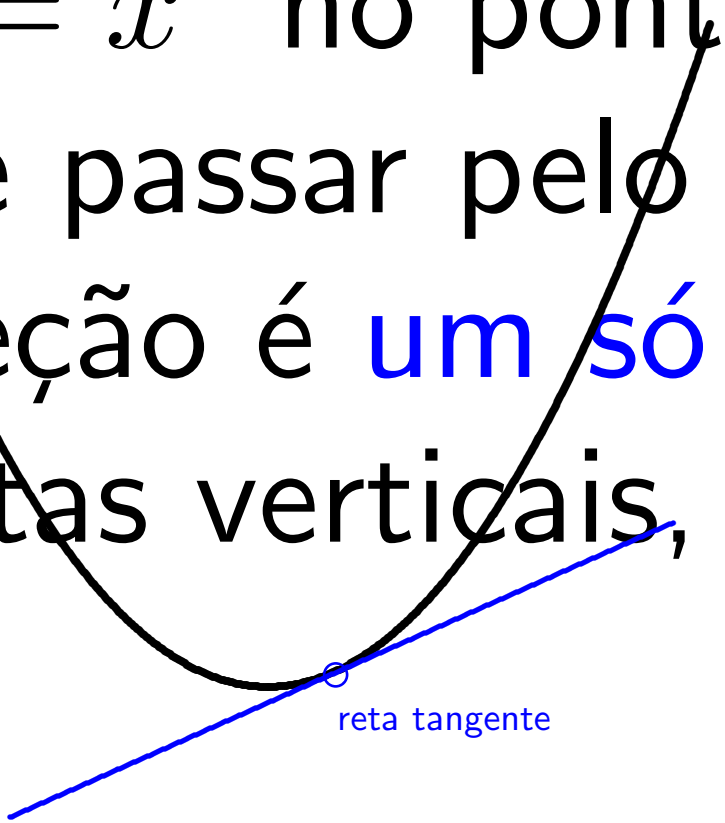
Lembram?



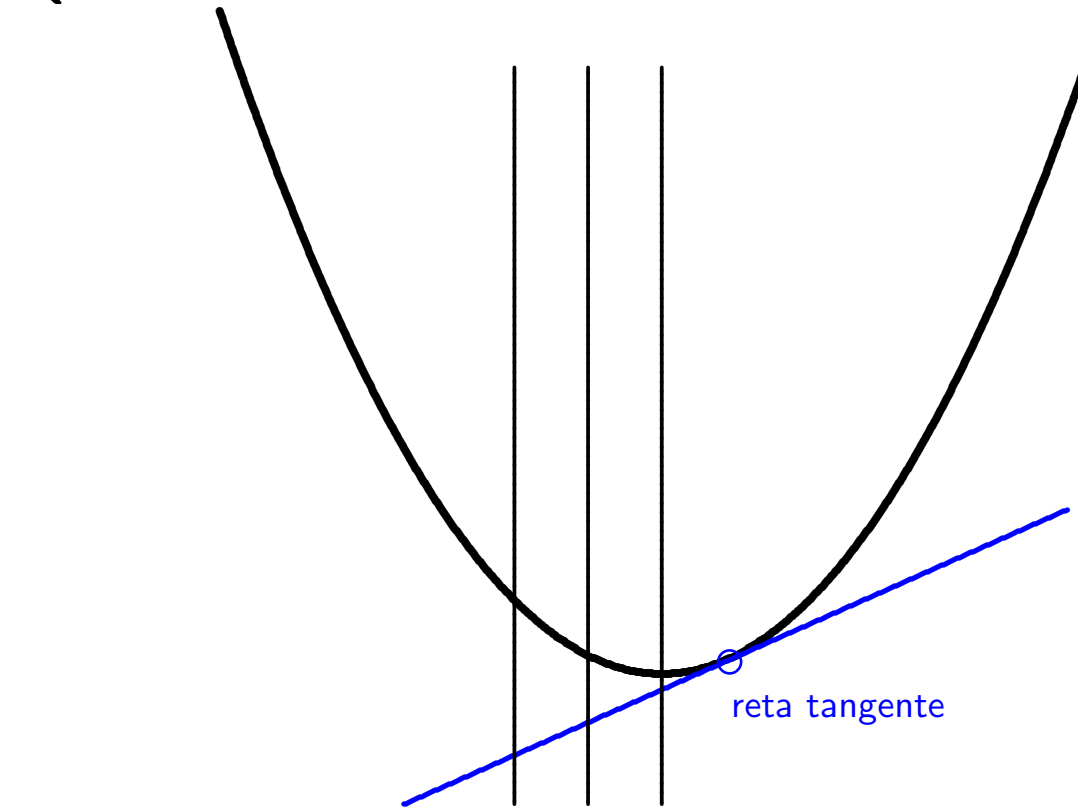
Quando é que uma reta $y = ax + b$ é tangente à parábola $y = x^2$ no ponto (t, t^2)?

- tem que passar pelo ponto;
- a interseção é um só ponto.

(¿ e as retas verticais, hein?)



(¿ e as retas verticais, hein?)



A explicação está no infinito, mas isso fica para outra vez:-)

A reta $y = ax + b$ passa pelo ponto $(t, t^2) \Leftrightarrow t^2 = at + b$.

Isto permite calcular b,

uma vez conhecido a.

A condição de tangência significa que a reta só corta a parábola no ponto (t, t^2). A interseção se acha resolvendo a equação $ax + b = x^2$. A raiz é única quando o discriminante do trinômio $x^2 - ax - b$ valer 0.

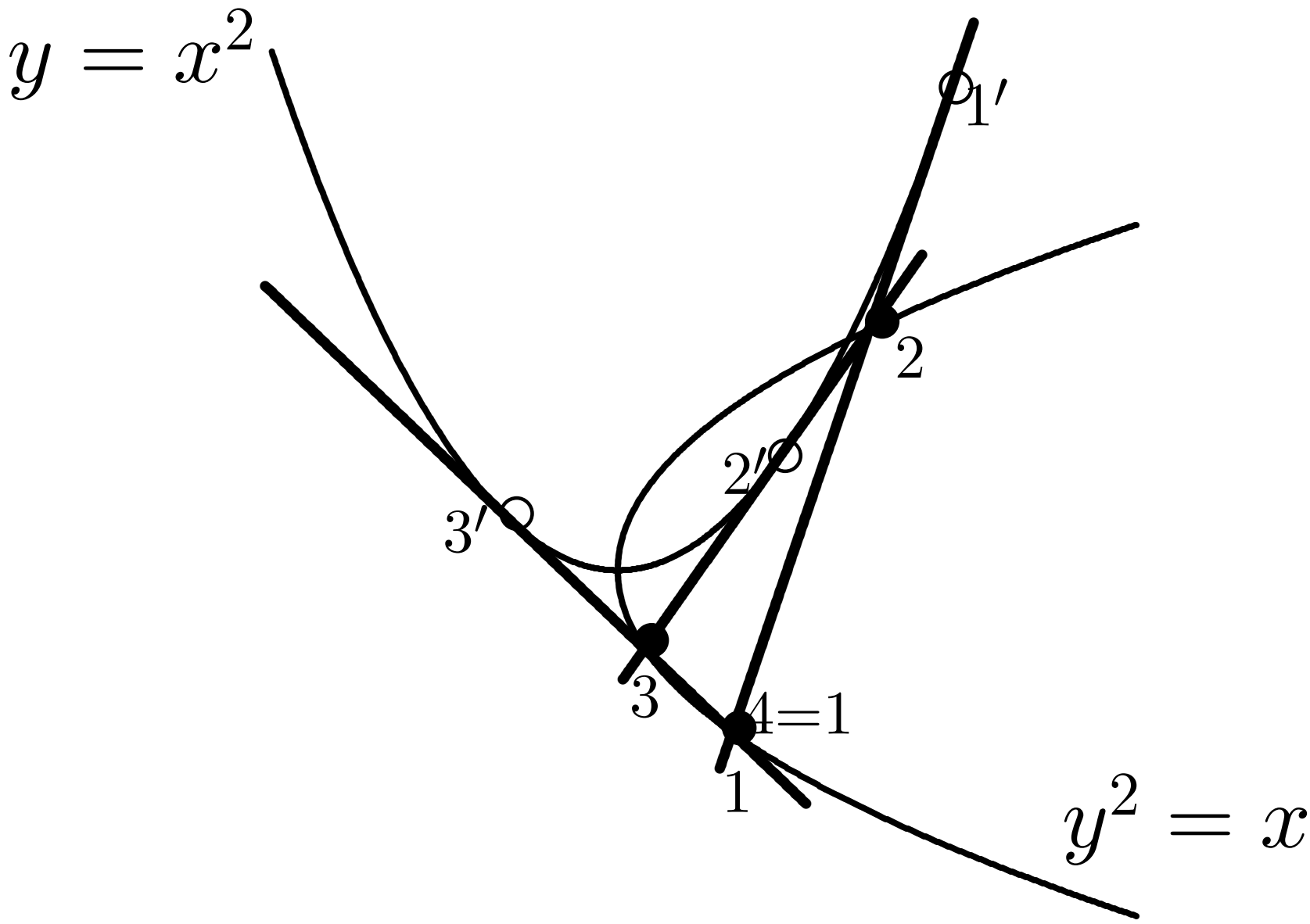
Ou seja, $a^2 + 4b = 0$.
Substituindo $b = t^2 - at$,
resulta $a^2 + 4(t^2 - at) =$
$a^2 - 4at + 4t^2 = (a - 2t)^2$.
Daí vem $a = 2t$.

recapitulando

Aprendemos que a reta tangente à parábola $y = x^2$ no ponto (t, t^2) é dada por $y = 2tx - t^2$.

Agora vamos "jogar bilhar" com um par de parábolas.

bilhar



Algebricamente, escrevemos as parametrizações

$$t \mapsto \underbrace{(t, t^2)}_{y=x^2}, \; s \mapsto \underbrace{(s^2, s)}_{x=y^2}.$$

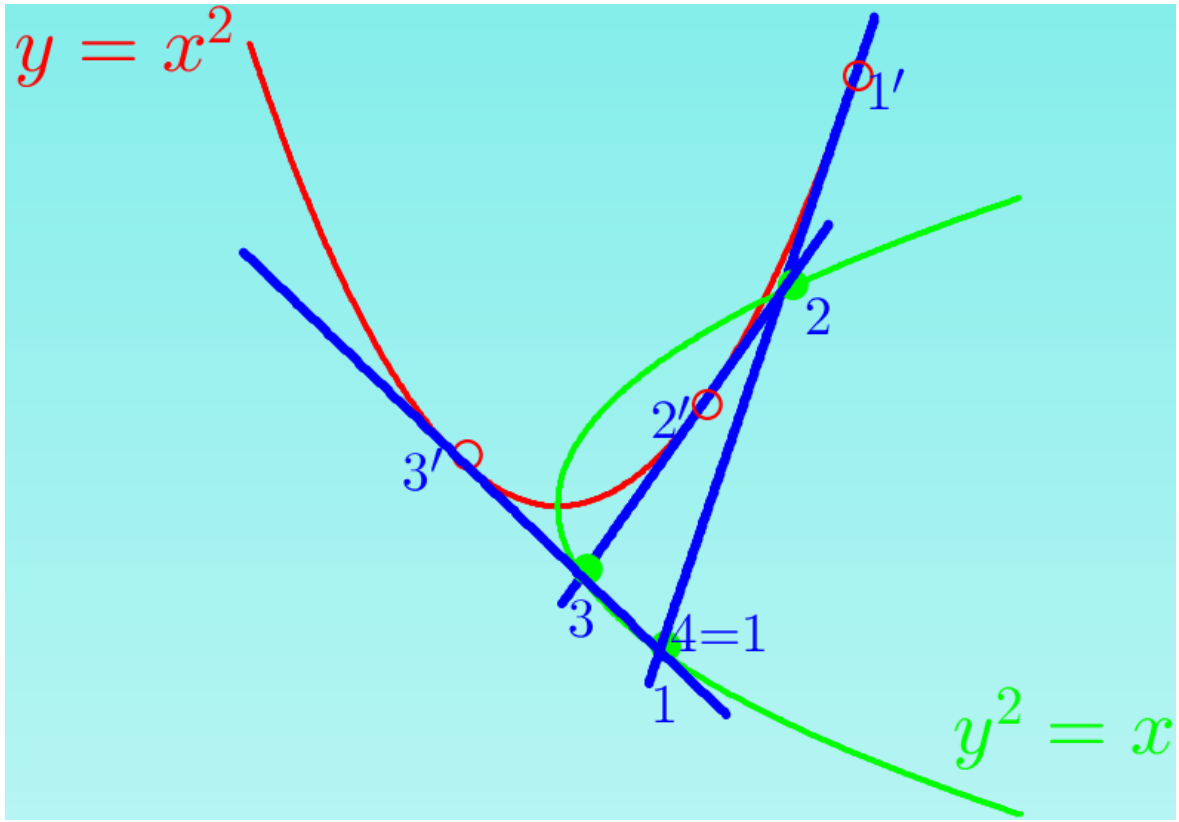
Exigimos que a reta tangente

$$y - t^2 = 2t(x - t)$$

passe pelo ponto (s^2, s), ou seja, vale a relação

$$t^2 - 2s^2 t + s = 0.$$

O movimento $1\vec{1}' \mapsto 2\vec{2}' \mapsto 3\vec{3}'$ feito na figura do bilhar



corresponde à transformação

$$\underbrace{(s,t)}_{\overrightarrow{11'}} \overset{\sigma}{\mapsto} \underbrace{(s',t)}_{\overrightarrow{21'}} \overset{\tau}{\mapsto} \underbrace{(s',t')}_{\overrightarrow{22'}}$$

$$\pi = \tau \circ \sigma$$

onde s' denota a 2ª raiz (idem t') na relação $t^2 - 2s^2t + s = 0$.

Lembrando as relações entre o produto das raízes e os coeficientes na equação do 2º grau,

$$t^2 - 2s^2t + s = 0,$$

um cálculo simples fornece

$$\sigma(s,t) = (\overbrace{-t/(2s)}^{s'}, t)$$

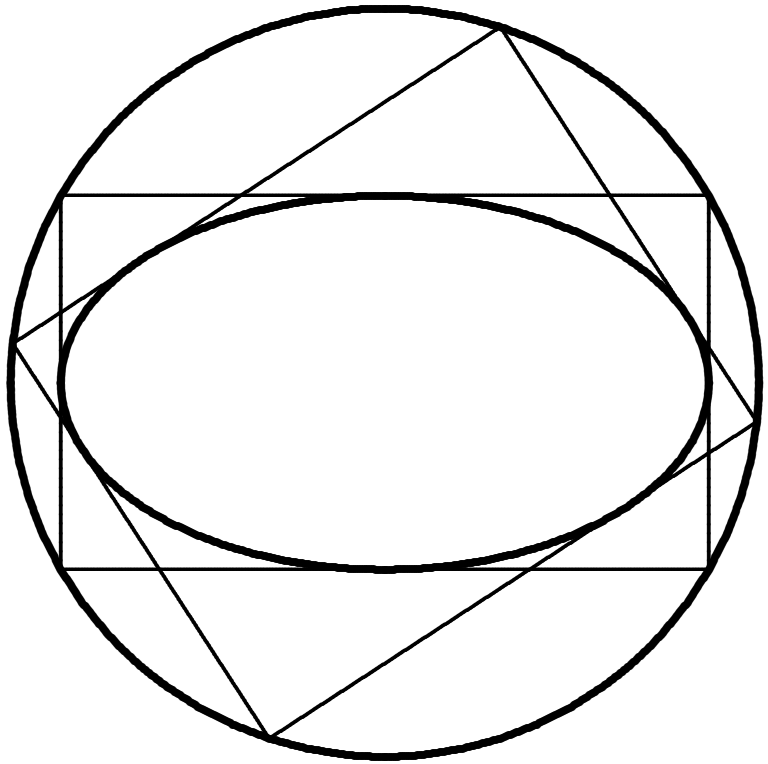
$$\tau(s,t) = (s, \underbrace{s/t}_{t'})$$

Segue

$$\pi(\pi(\pi(s,t))) = (s,t)$$

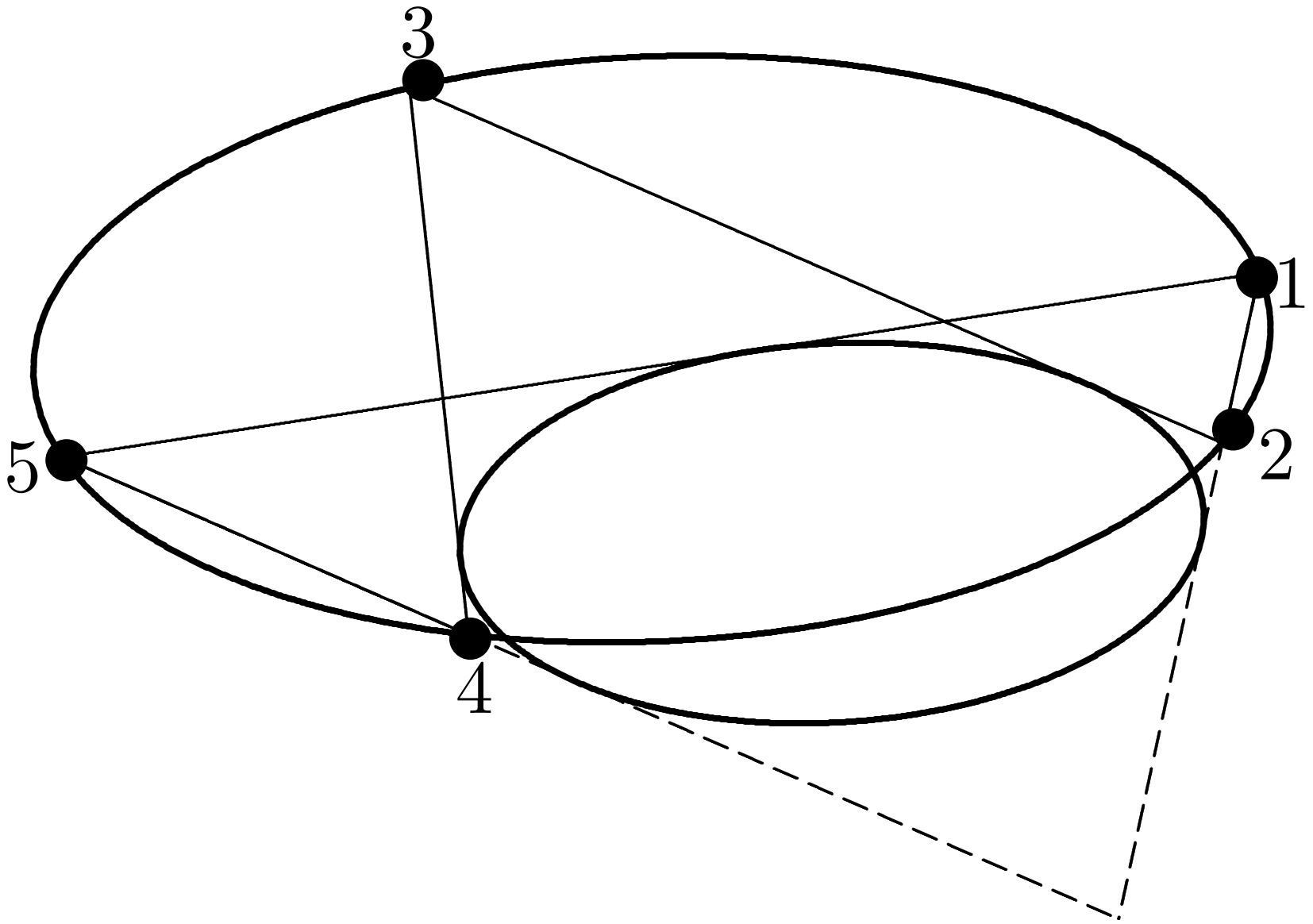
Conclusão: a poligonal inscrita/circunscrita fecha em 3 "tacadas", independente do ponto inicial.

quadriláteros



Aqui, fecha em 4 etapas. . .
independente do ponto inicial!

cinco pontos ainda é de graça



Já não se faz criptografia
como antigamente

Criptografia
do grego Kryptos: escondido,
e
Graphos: escritura

é a ciência que estuda formas de
codificar uma mensagem,
tornando-a jodpnqsffotjxfm
para quem não
deveria ter acesso a ela.

é a ciência que estuda formas de codificar uma mensagem,

tornando-a incompreensível

para quem não

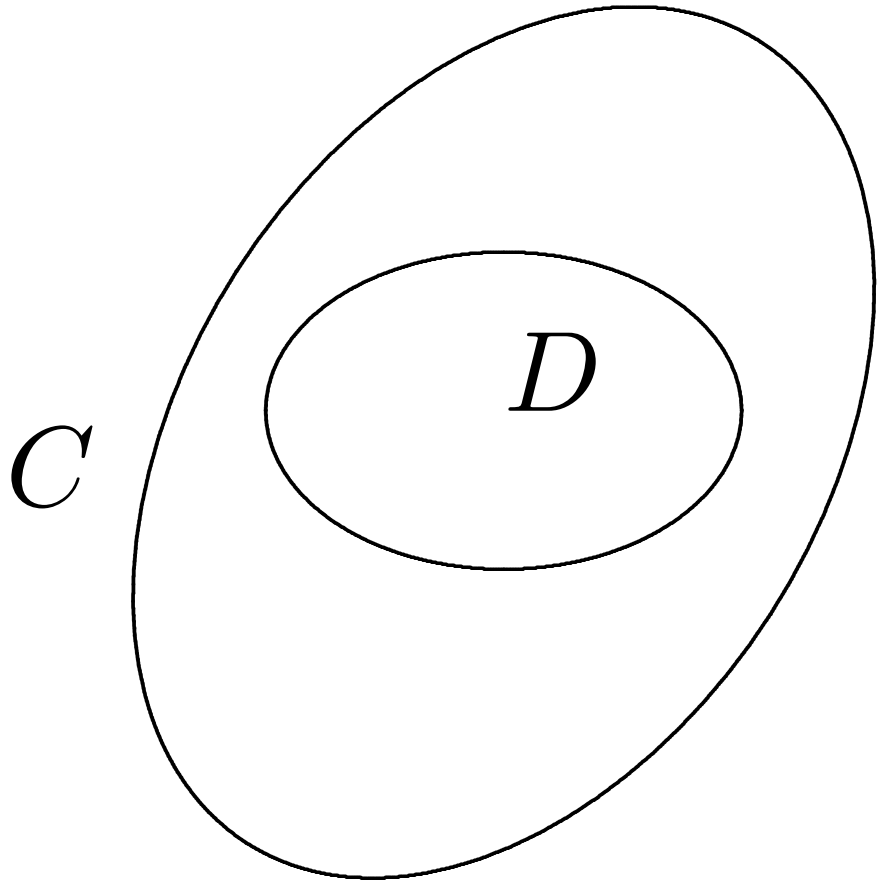
deveria ter acesso a ela.

Trata-se, em suma, da disciplina que cuida da privacidade na transmissão de dados.

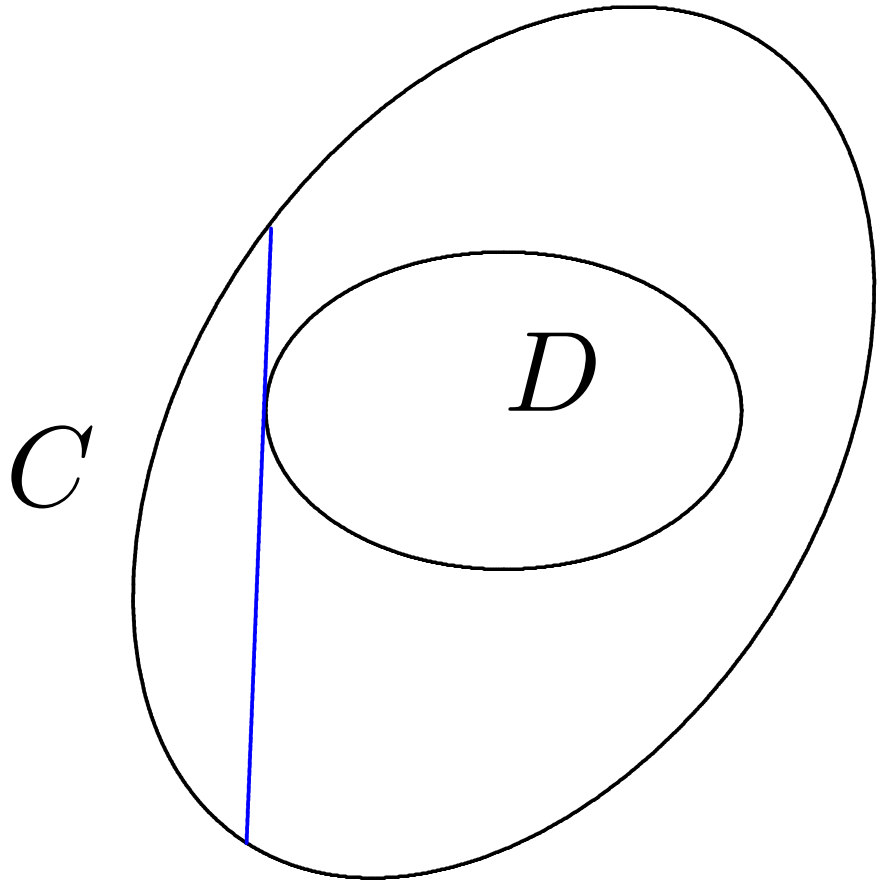
Ana, Bruno, bilhar?

O bilhar pode ser usado para fornecer uma regra de embaralhamento.

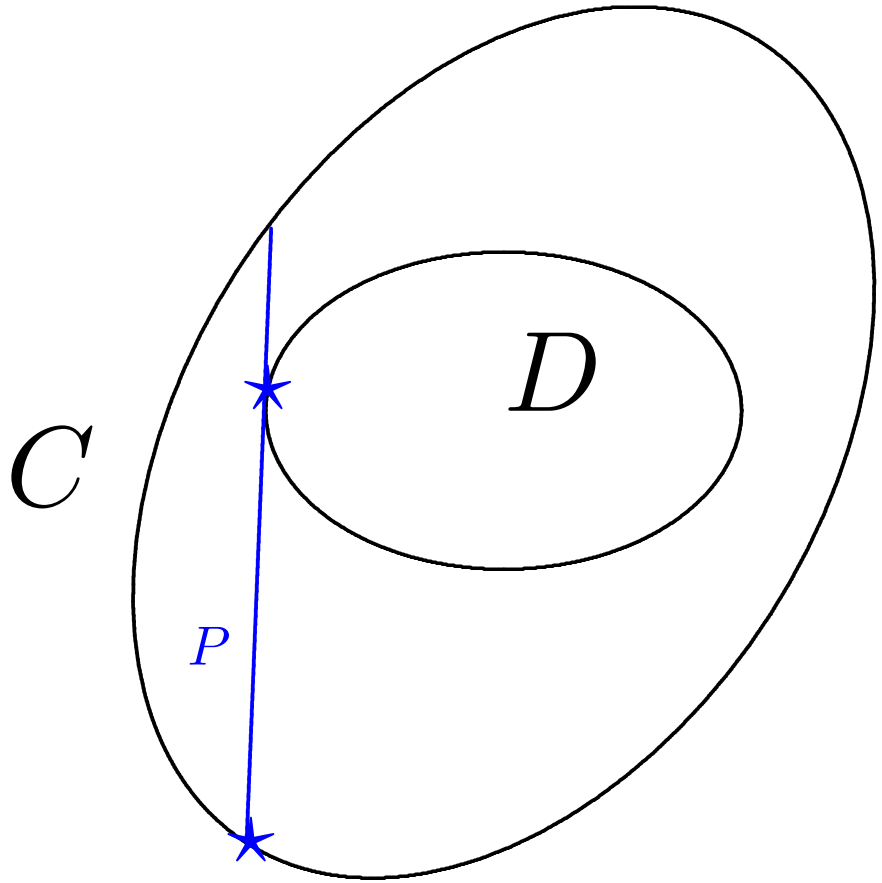
Tome um par de cônicas:



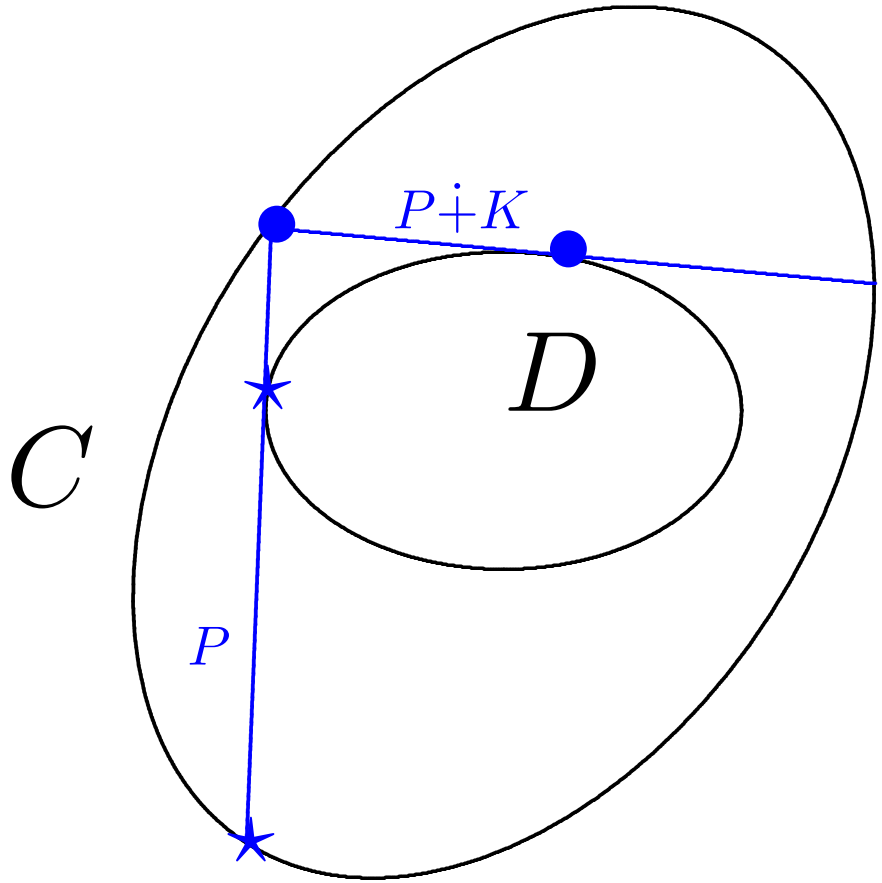
Tome um par de cônicas:



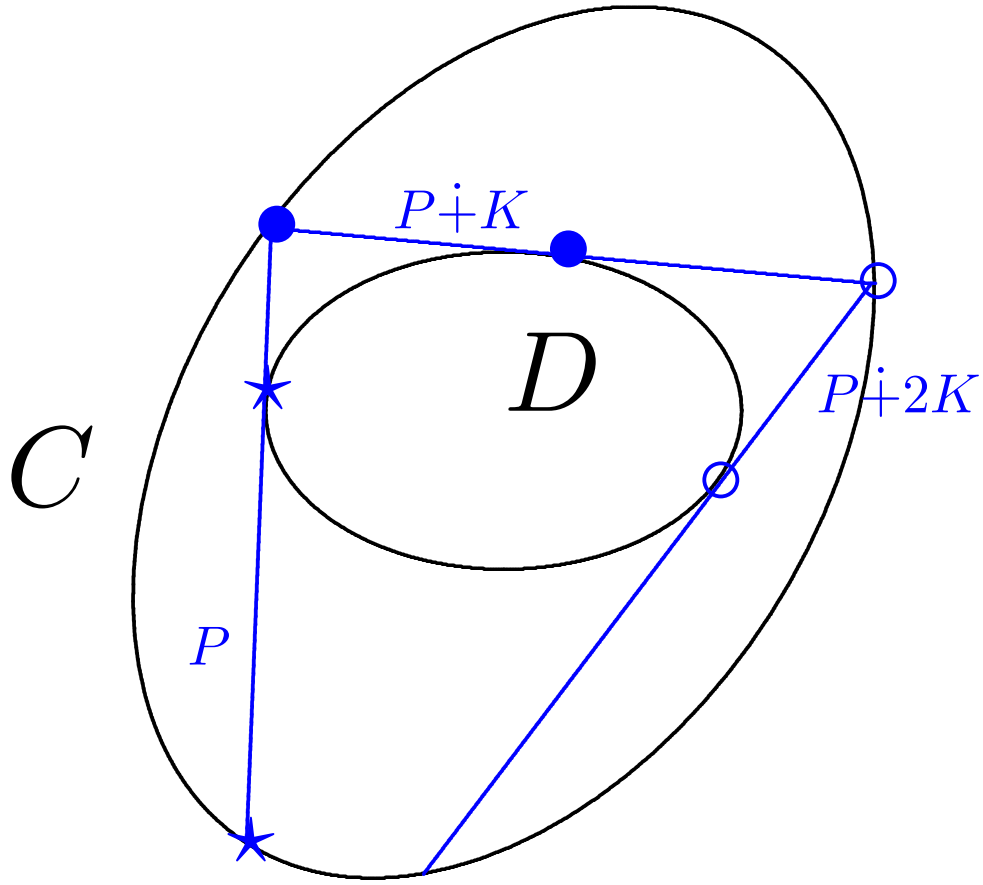
Tome um par de cônicas:



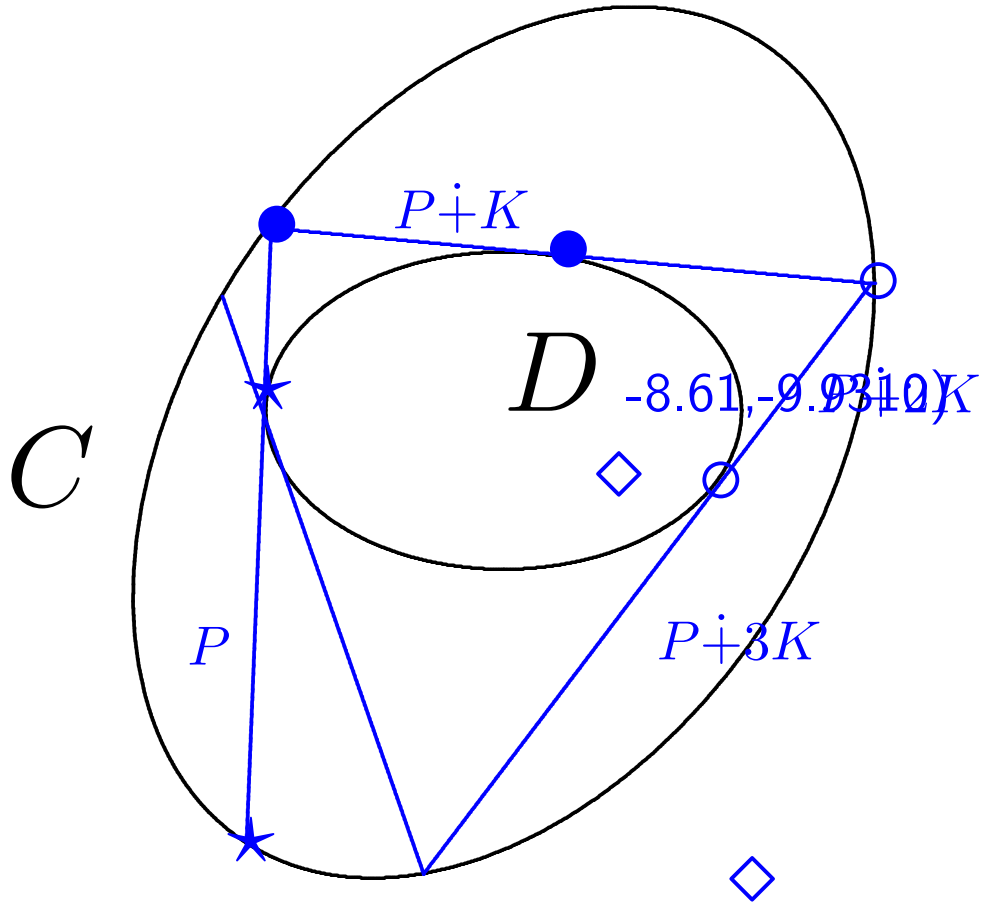
Tome um par de cônicas:



Tome um par de cônicas:



Tome um par de cônicas:



Para C, D cônicas "gerais", a poligonal não fecha.

Mas Poncelet descobriu que, se fechar em n etapas a partir de algum $c \in C$,

o mesmo ocorrerá para qualquer outro ponto de C!

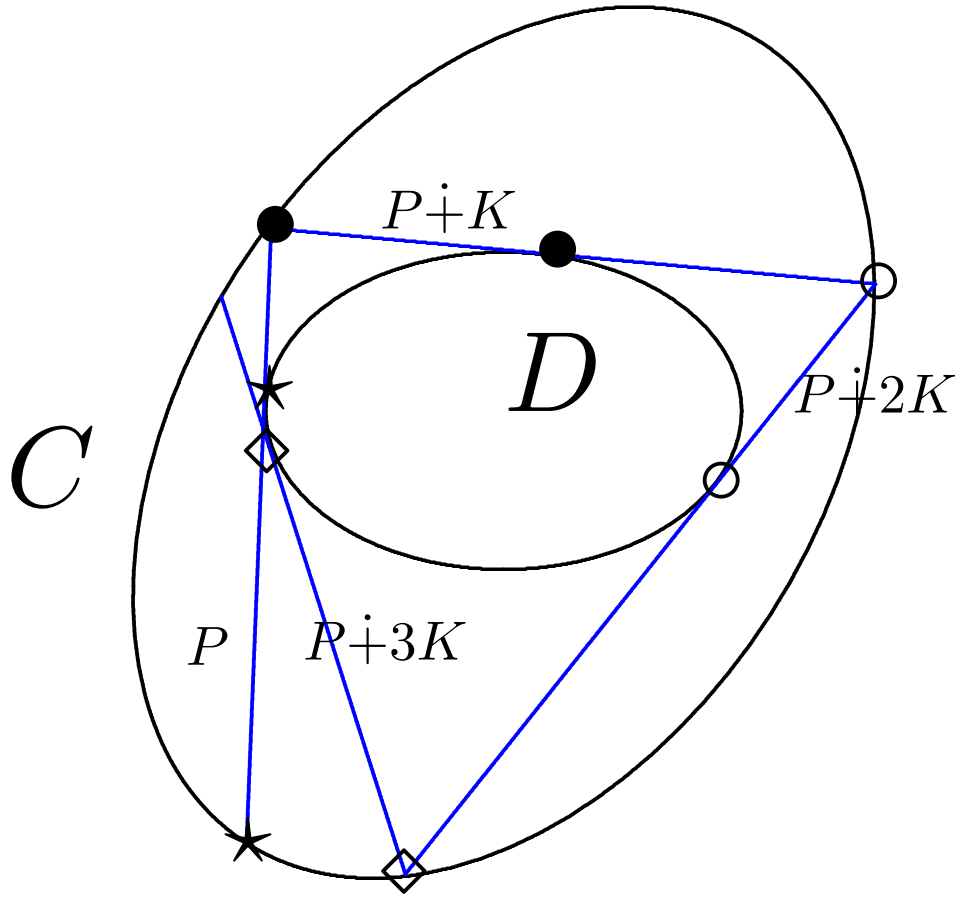
quem foi Poncelet?

1788-1867

O nome de Jean-Victor Poncelet se destaca na Matemática pelos trabalhos em geometria projetiva da qual é considerado um dos fundadores. Seus primeiros estudos naquele tópico foram feitos durante o inverno de 1812-13 e julho de 1814, enquanto era prisioneiro de guerra, em Saratov, por ter participado da campanha russa como tenente-engenheiro do exército invasor

francês. Em 1814 torna-se capitão-engenheiro. De 1815 até 1825 trabalha em projetos militares e a partir daí até 1835, como professor de mecânica. Mas sempre continuou com seus estudos em geometria projetiva e em 1822 é publicado o "Traité des propriétés projectives des figures", primeiro livro dedicado àquela disciplina. Você pode consultar a Wikipedia para mais detalhes.

Usando o bilhar de Poncelet,
cada mensagem é associada a um par
(c, d) : $\star\star$, $\bullet\bullet$, $\circ\circ$, . . .
onde c percorre a cônica "externa" C, e
d denota o ponto de contato
de uma tangente à cônica interna D
traçada por c.


C
D
$P \dot{+} K$
$P \dot{+} 2K$
P
$P \dot{+} 3K$

Esta regra fornece uma maneira
de "embaralhar" *i.e.*, codificar dados
para transmissão e posterior decodificação.
Para funcionar bem, é preciso saber construir
pares de cônicas com poligonal
inscrita/circunscrita fechada com número
arbitrariamente grande de vértices.
As chaves secretas da Ana e do Bruno
agora são os números de "tacadas"
que cada qual vai usar.

epílogo

Geometria, álgebra, aritmética,. . . ,
enfim, a MATEMÁTICA,
são ingredientes para
um dos melhores banquetes de que
a nossa mente pode desfrutar.

A MATEMÁTICA talvez seja o único divertimento que, inexplicavelmente, também serve para avançar o conhecimento sobre o mundo em que vivemos.

TCHAU!