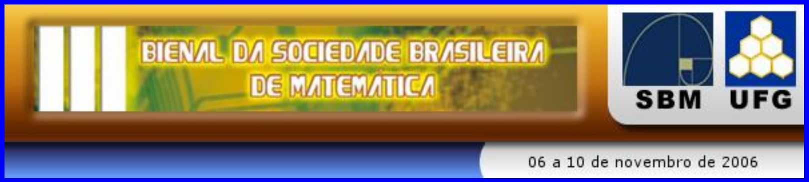
III BIENAL DA SOCIEDADE BRASILEIRA DE MATEMÁTICA
SBM UFG
06 a 10 de novembro de 2006

bilhar de Poncelet e criptografia de curvas elípticas



bilhar de Poncelet e criptografia de curvas elípticas

ou

III BIENAL DA SOCIEDADE BRASILEIRA DE MATEMÁTICA

SBM UFG

06 a 10 de novembro de 2006

bilhar de Poncelet e criptografia de curvas elípticas

ou

a vingança

III BIENAL DA SOCIEDADE BRASILEIRA DE MATEMATICA

SBM UFG

06 a 10 de novembro de 2006

bilhar de Poncelet e criptografia de curvas elípticas

ou

a vingança da

III BIENAL DA SOCIEDADE BRASILEIRA DE MATEMÁTICA

SBM UFG

06 a 10 de novembro de 2006

bilhar de Poncelet e criptografia de curvas elípticas

ou

a vingança da matematica pura

III BIENAL DA SOCIEDADE BRASILEIRA DE MATEMÁTICA
SBM UFG
06 a 10 de novembro de 2006

bilhar de Poncelet e criptografia de curvas elípticas

ou

a vingança da matematica pura

Israel Vainsencher UFMG

III BIENAL DA SOCIEDADE BRASILEIRA DE MATEMATICA

SBM UFG

06 a 10 de novembro de 2006

bilhar de Poncelet e criptografia de curvas elípticas

ou

a vingança da matematica pura

Israel Vainsencher UFMG

http://www.mat.ufmg.br/∼israel

bilhar de Poncelet e criptografia de curvas elípticas

ou

a vingança da matemática pura

Israel Vainsencher

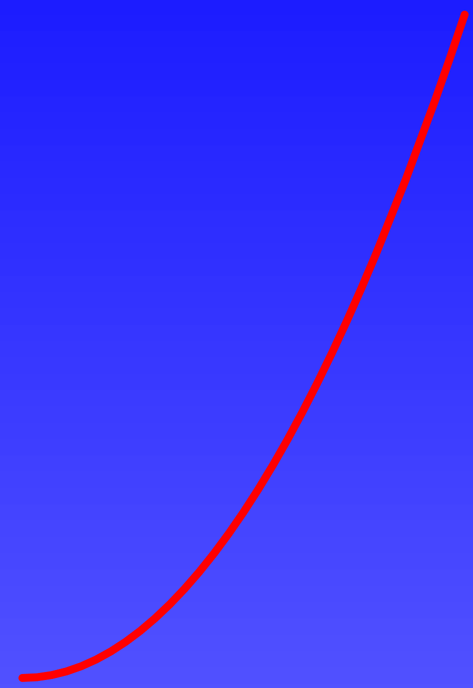
http://www.mat.ufmg.br/∼israel

laptop financiado pelo

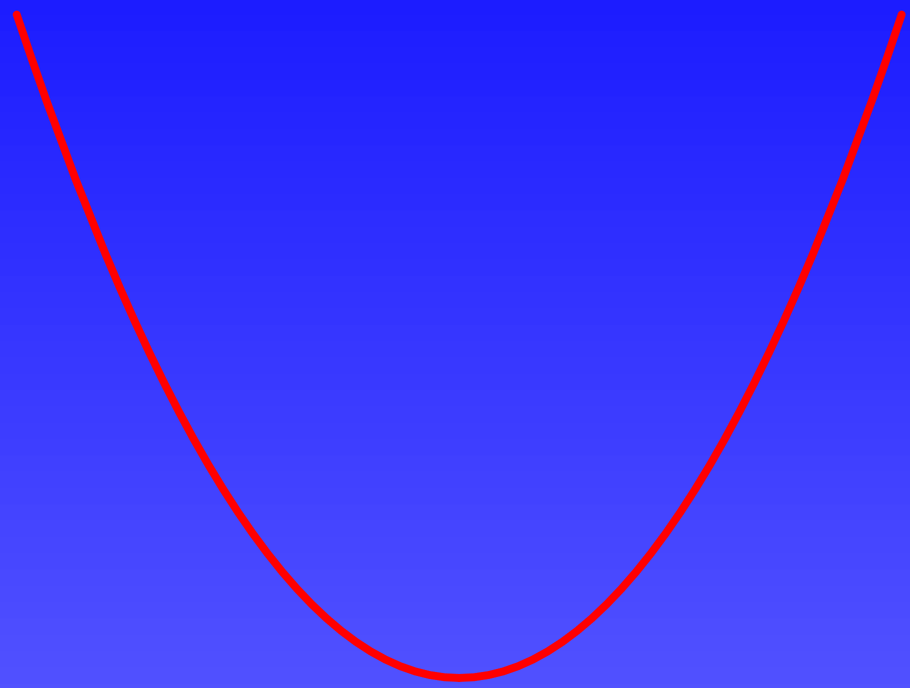
à guisa de aquecimento,

à guisa de aquecimento, “para casa”

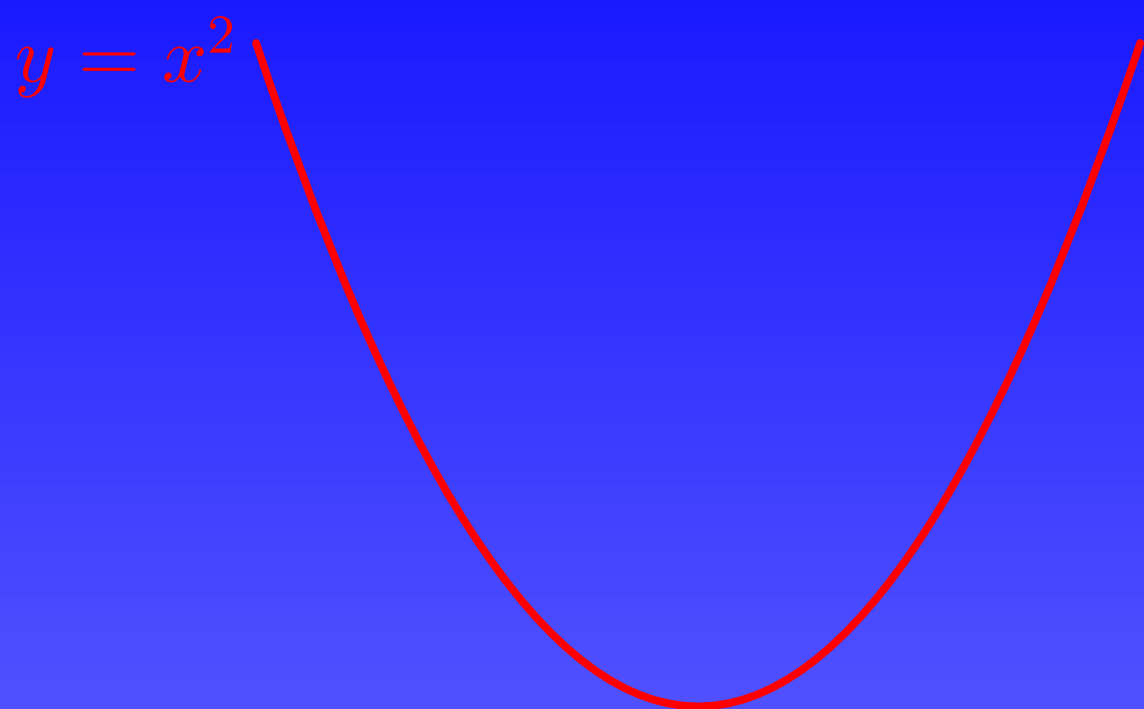
à guisa de aquecimento, “para casa”. . .



à guisa de aquecimento, “para casa”. . .

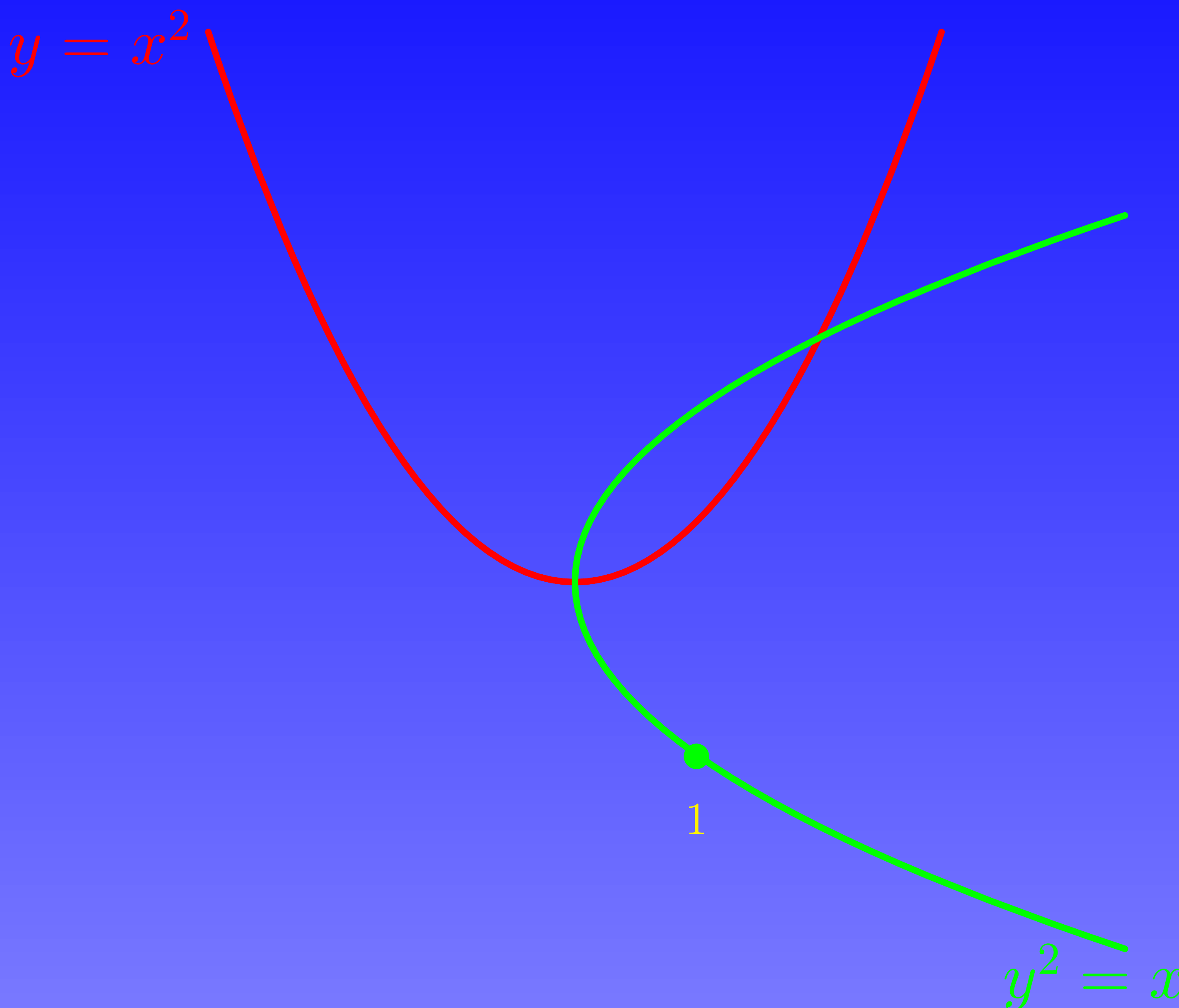


à guisa de aquecimento, “para casa”. . .

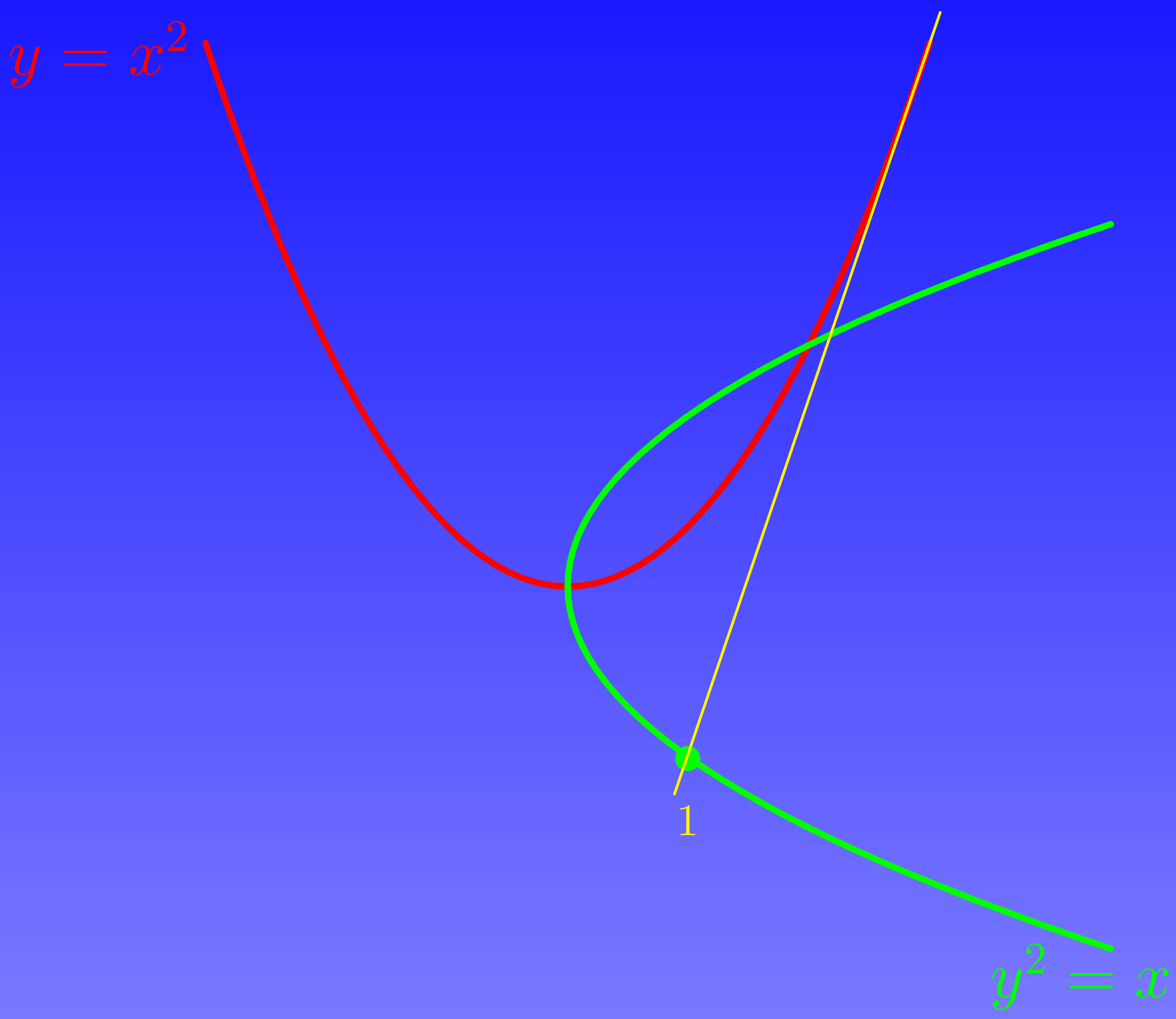


à guisa de aquecimento, “para casa”. . .

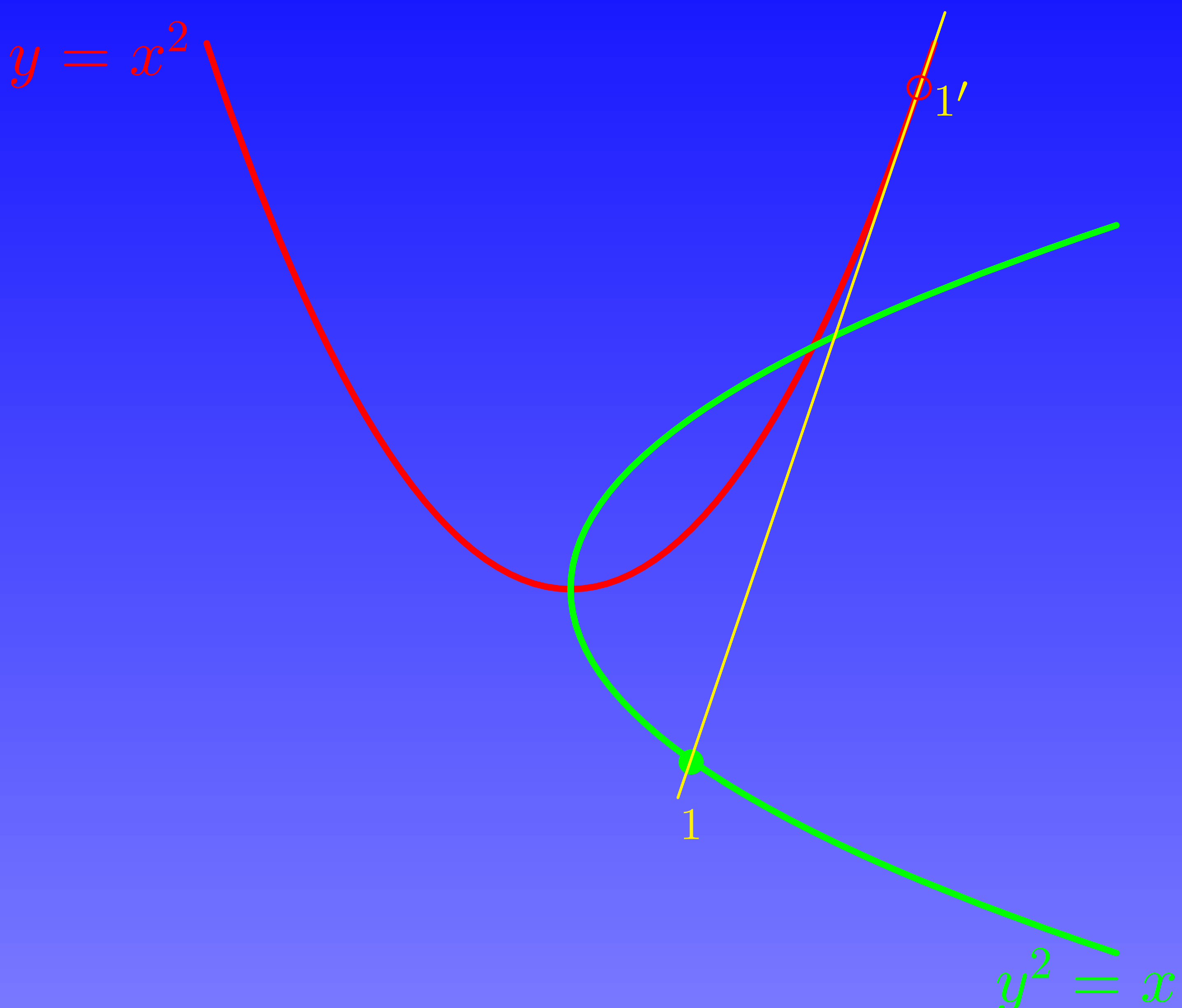
à guisa de aquecimento, “para casa”. . .



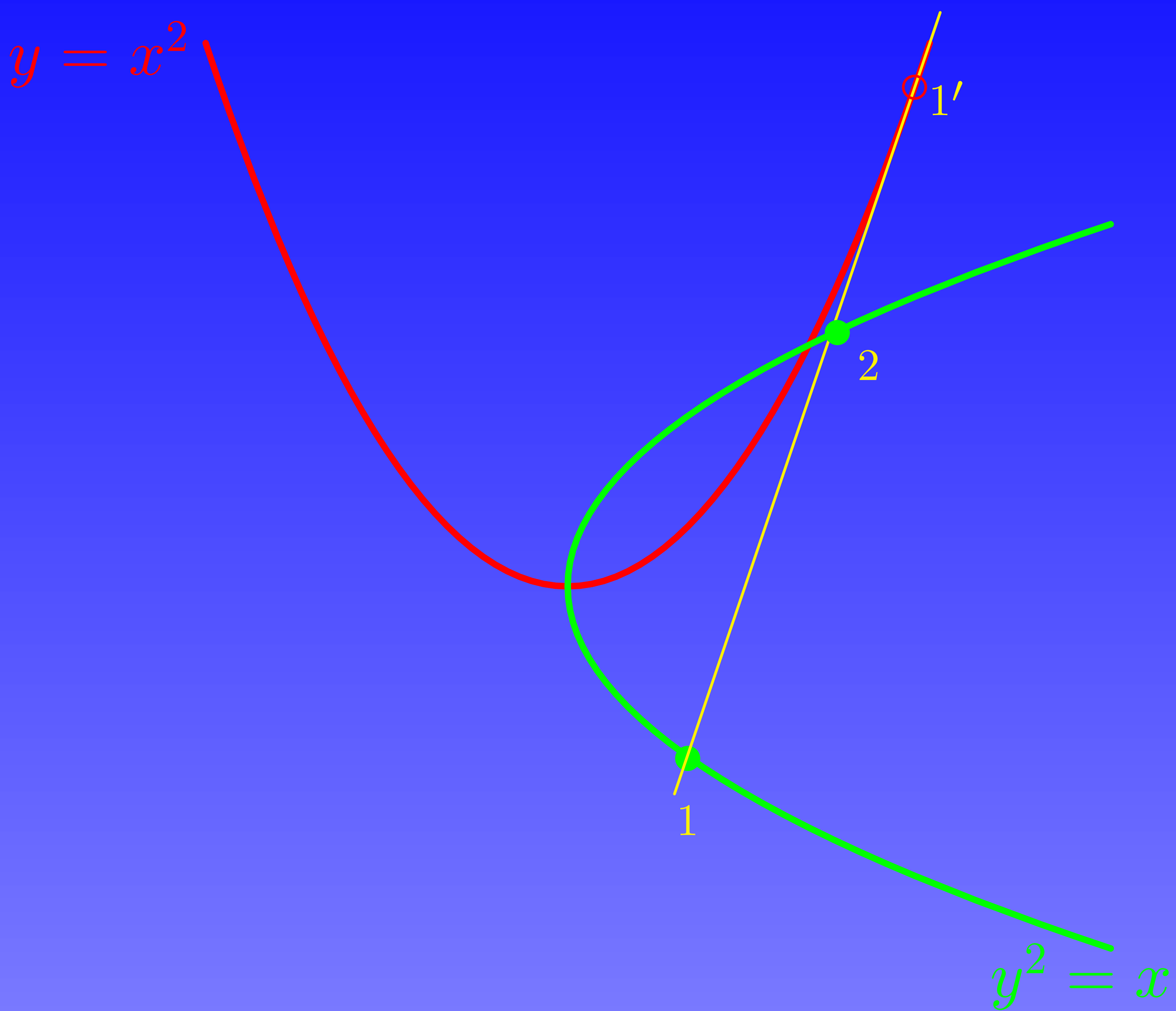
à guisa de aquecimento, “para casa”. . .



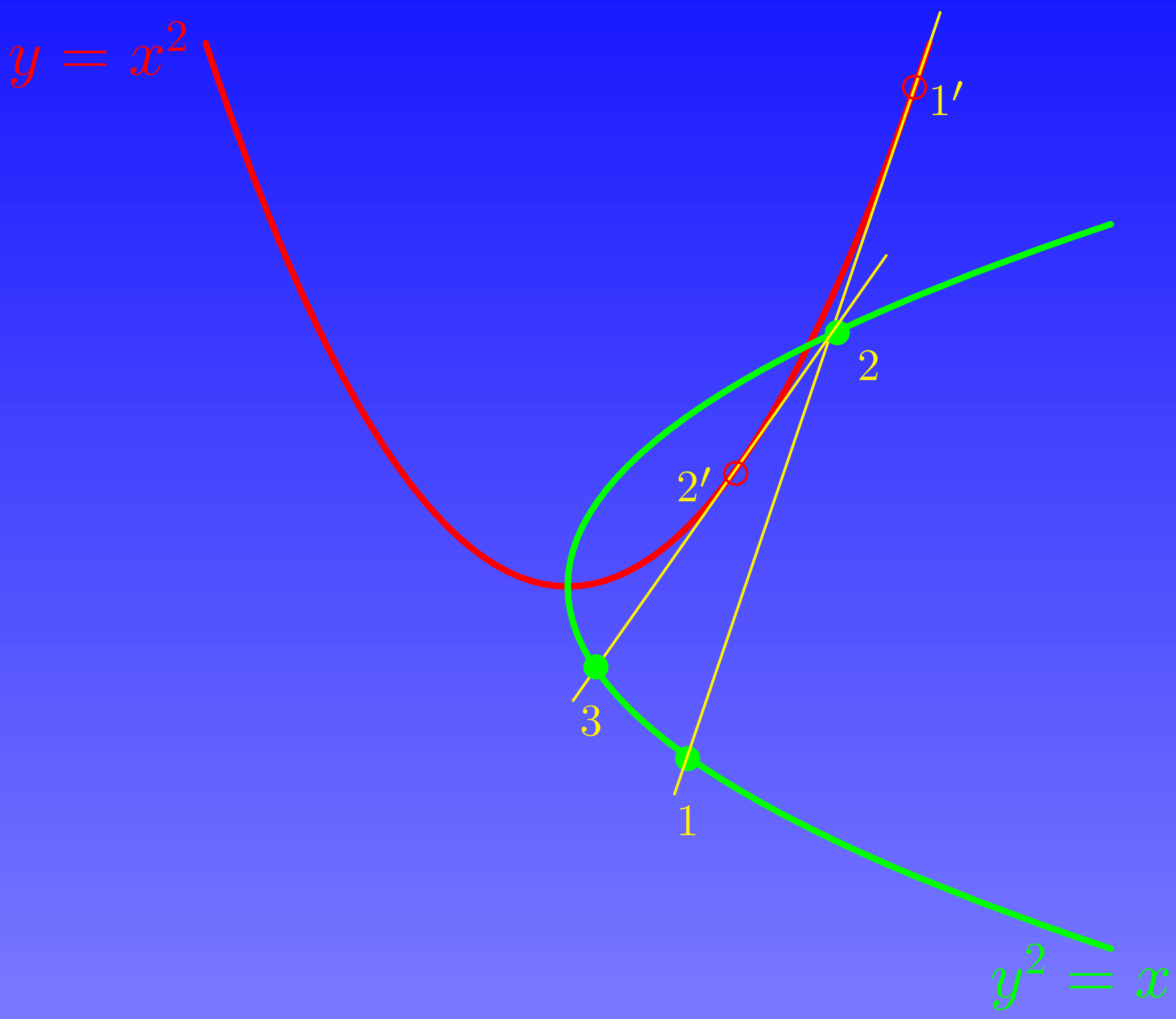
à guisa de aquecimento, “para casa”. . .



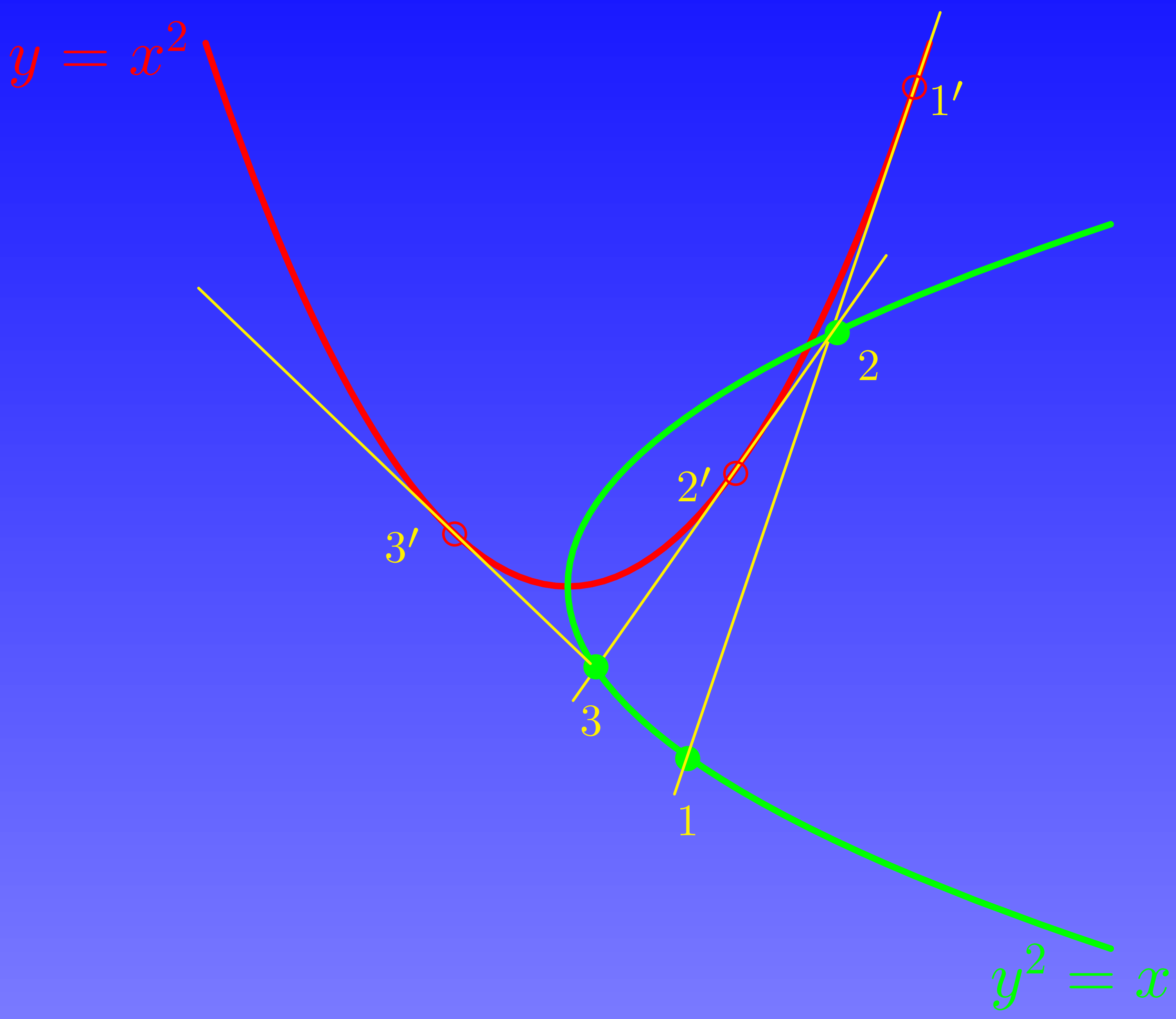
à guisa de aquecimento, "para casa"...



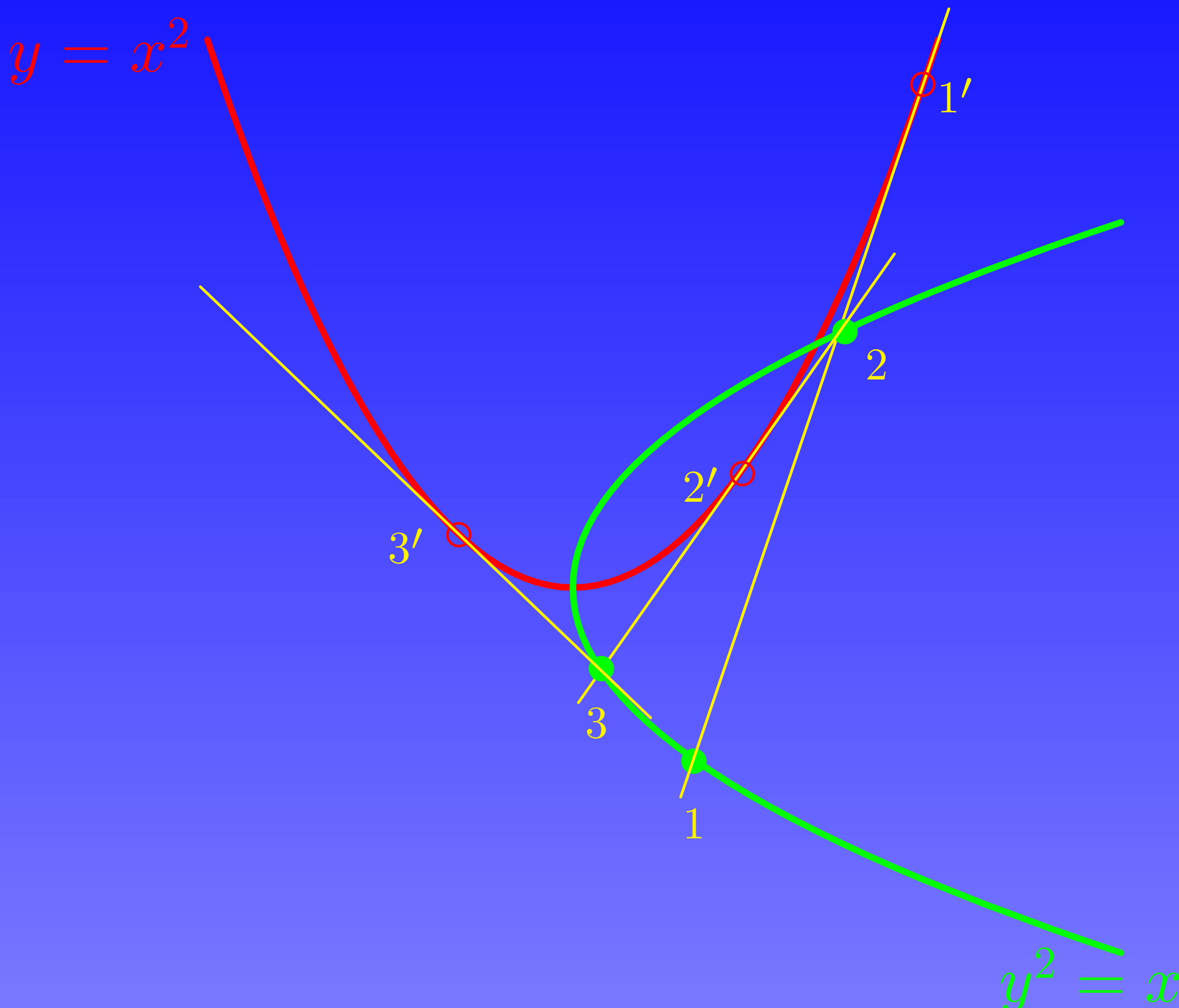
à guisa de aquecimento, "para casa". . .



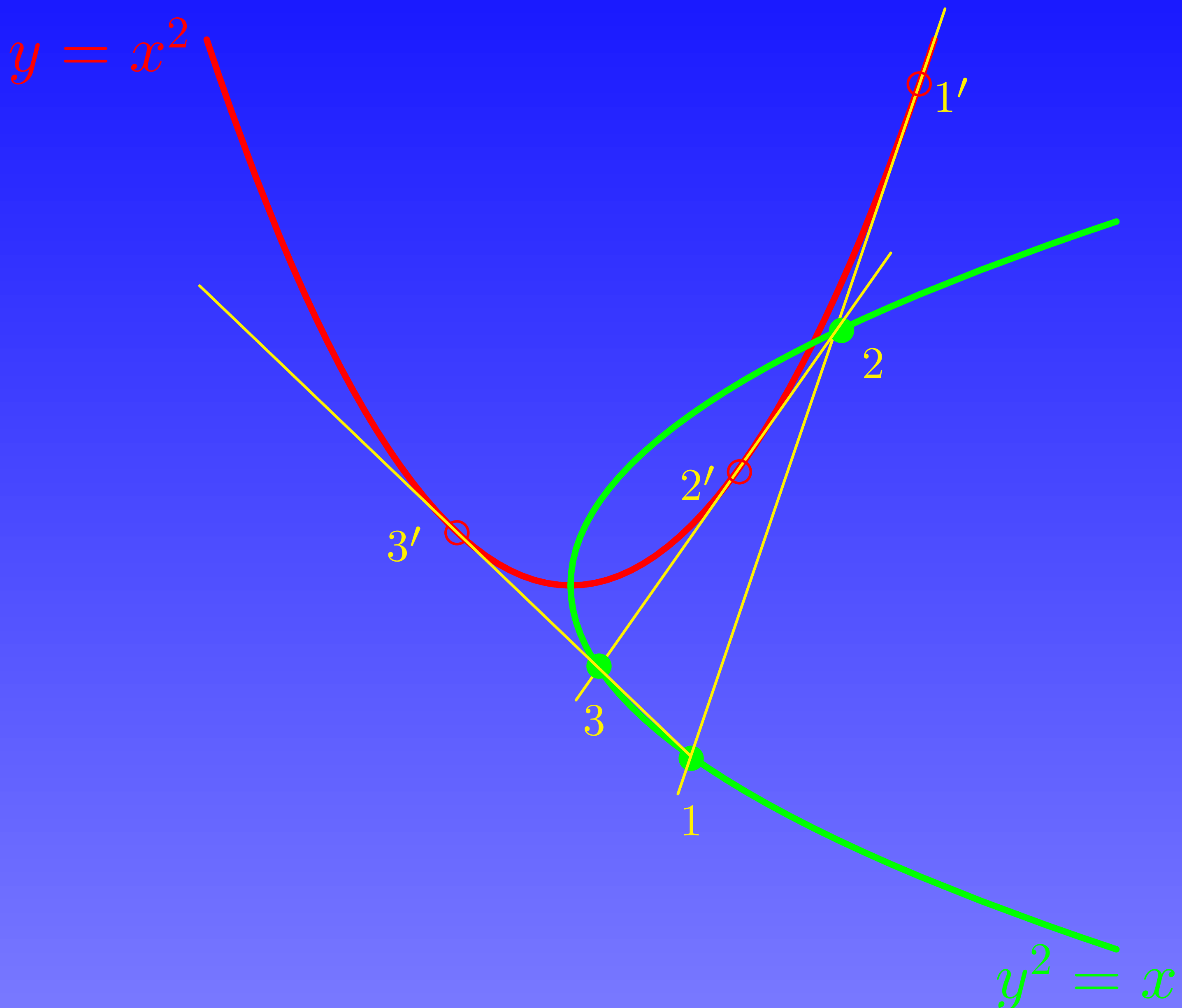
à guisa de aquecimento, "para casa". . .



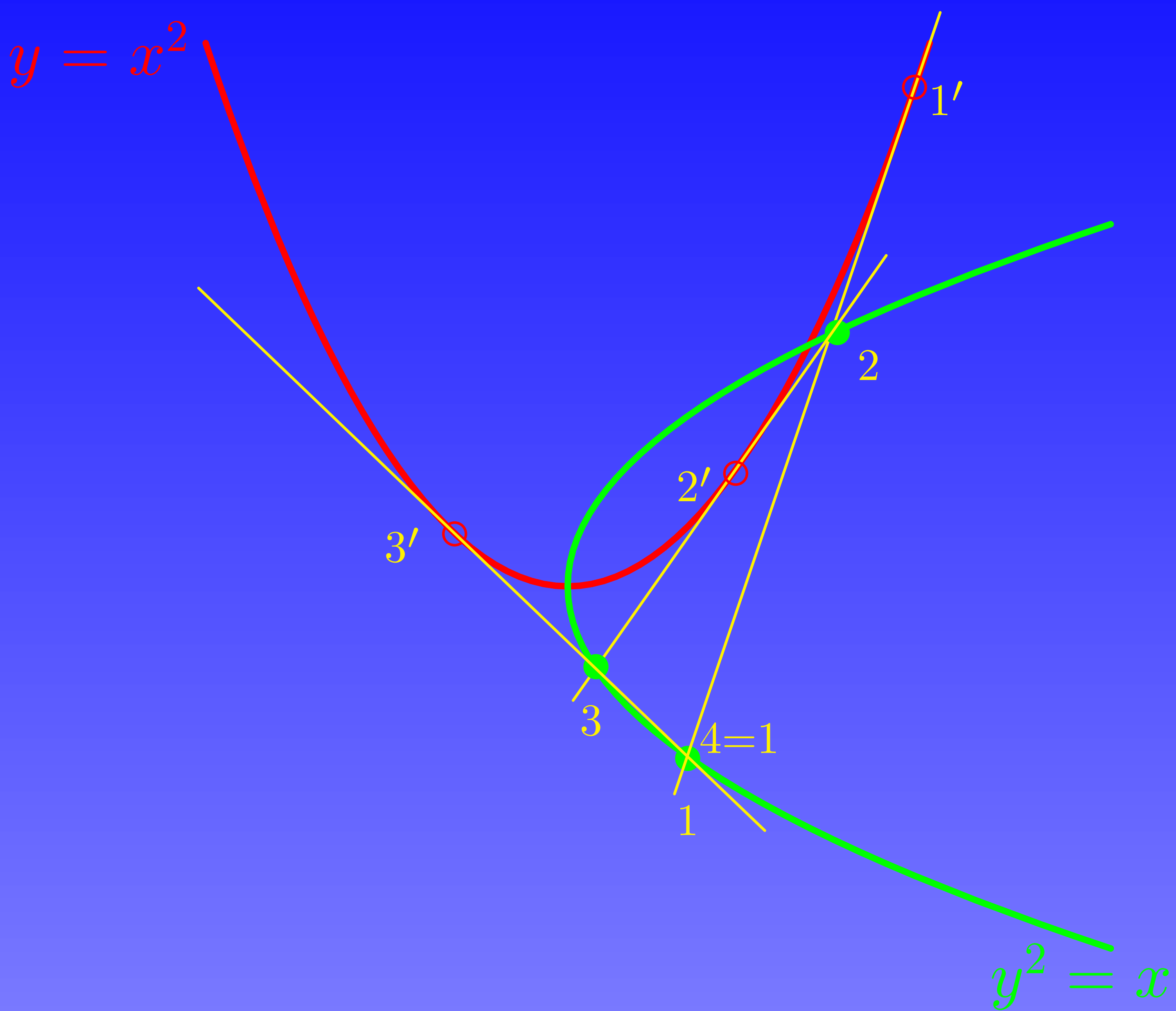
à guisa de aquecimento, “para casa”. . .



à guisa de aquecimento, “para casa”. . .



à guisa de aquecimento, "para casa". . .



à guisa de aquecimento, “para casa”. . .

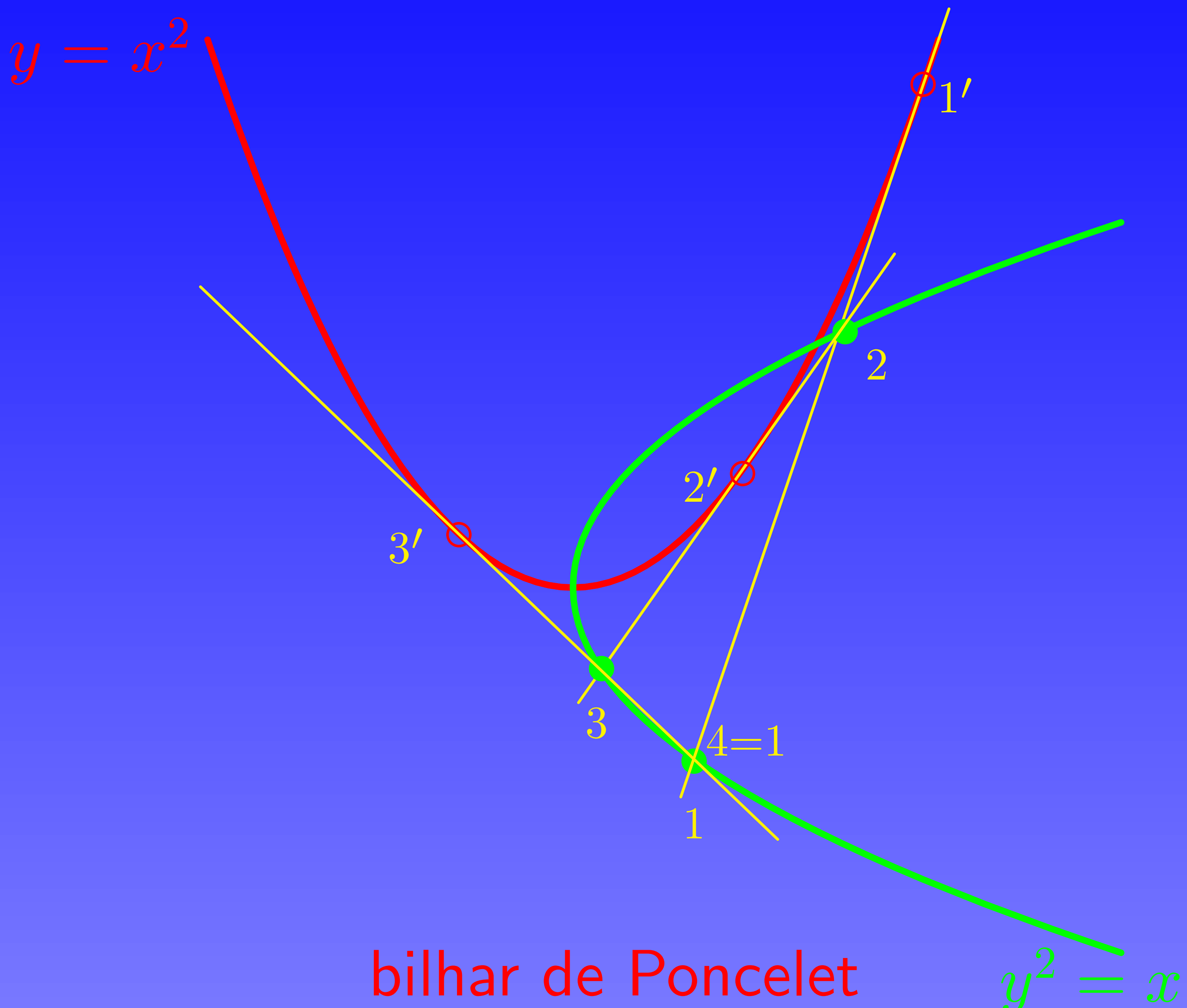


fig1

bilhar de Poncelet

Algebricamente, escrevemos as parametrizações

$$t \longmapsto \underbrace{(t, t^2)}_{y=x^2},$$

Algebricamente, escrevemos as parametrizações

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

Algebricamente, escrevemos as parametrizações

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

Exigimos que a reta tangente

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

Algebricamente, escrevemos as parametrizações

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

Exigimos que a reta tangente

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

passe pelo ponto (s^2, s), ou seja,

Algebricamente, escrevemos as parametrizações

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

Exigimos que a reta tangente

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

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

$$\boxed{t^2 - 2s^2t + s = 0.}$$

Algebricamente, escrevemos as parametrizações

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

Exigimos que a reta tangente

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

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

$$\boxed{t^2 - 2s^2t + s = 0.}$$

O movimento $\overrightarrow{11}' \mapsto$

Algebricamente, escrevemos as parametrizações

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

Exigimos que a reta tangente

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

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

$$\boxed{t^2 - 2s^2t + s = 0.}$$

O movimento $\overrightarrow{11'} \mapsto \overrightarrow{22'} \mapsto$

Algebricamente, escrevemos as parametrizações

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

Exigimos que a reta tangente

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

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

$$\boxed{t^2 - 2s^2 t + s = 0.}$$

O movimento $\overrightarrow{11'} \mapsto \overrightarrow{22'} \mapsto \overrightarrow{33'}$

Algebricamente, escrevemos as parametrizações

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

Exigimos que a reta tangente

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

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

$$\boxed{t^2 - 2s^2t + s = 0.}$$

O movimento $\overrightarrow{11'} \mapsto \overrightarrow{22'} \mapsto \overrightarrow{33'}$ na fig1 da p. anterior

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

$$\boxed{t^2 - 2s^2 t + s = 0.}$$

O movimento $\overrightarrow{11'} \mapsto \overrightarrow{22'} \mapsto \overrightarrow{33'}$ na fig1 da p. anterior

corresponde ao mapeamento

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

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

$$\boxed{t^2 - 2s^2t + s = 0.}$$

O movimento $\overrightarrow{11'} \mapsto \overrightarrow{22'} \mapsto \overrightarrow{33'}$ na fig1 da p. anterior

corresponde ao mapeamento

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

(bilhar de Poncelet)

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

$$\boxed{t^2 - 2s^2 t + s = 0.}$$

O movimento $\overrightarrow{11'} \mapsto \overrightarrow{22'} \mapsto \overrightarrow{33'}$ na fig1 da p. anterior

corresponde ao mapeamento

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

(bilhar de Poncelet) onde s' denota a 2ª raiz;

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

$$\boxed{t^2 - 2s^2 t + s = 0.}$$

O movimento $\overrightarrow{11'} \mapsto \overrightarrow{22'} \mapsto \overrightarrow{33'}$ na fig1 da p. anterior

corresponde ao mapeamento

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

(bilhar de Poncelet) onde s' denota a 2ª raiz; idem t'.

Algebricamente, escrevemos as parametrizações

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

Exigimos que a reta tangente

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

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

$$\boxed{t^2 - 2s^2t + s = 0.}$$

O movimento $\overrightarrow{11'} \mapsto \overrightarrow{22'} \mapsto \overrightarrow{33'}$ na fig1 da p. anterior

corresponde ao mapeamento

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

Algebricamente, escrevemos as parametrizações

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

Exigimos que a reta tangente

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

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

$$\boxed{t^2 - 2s^2 t + s = 0.}$$

O movimento $\overrightarrow{11'} \mapsto \overrightarrow{22'} \mapsto \overrightarrow{33'}$ na fig1 da p. anterior

corresponde ao mapeamento

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

(bilhar de Poncelet)

Algebricamente, escrevemos as parametrizações

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

Exigimos que a reta tangente

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

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

$$\boxed{t^2 - 2s^2 t + s = 0.}$$

O movimento $\overrightarrow{11'} \mapsto \overrightarrow{22'} \mapsto \overrightarrow{33'}$ na fig1 da p. anterior

corresponde ao mapeamento

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

(bilhar de Poncelet) onde s' denota a 2ª raiz;

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

$$\boxed{t^2 - 2s^2 t + s = 0.}$$

O movimento $\overrightarrow{11'} \mapsto \overrightarrow{22'} \mapsto \overrightarrow{33'}$ na fig1 da p. anterior

corresponde ao mapeamento

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

(bilhar de Poncelet) onde s' denota a 2ª raiz; idem t'.

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

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

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

$$\boxed{\begin{aligned} \sigma(s,t) &= (\overbrace{-t/(2s)}^{s'}, t) \\ \tau(s,t) &= (s, \underbrace{s/t}_{t'}) \end{aligned}}$$

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

$$\boxed{\begin{array}{c} \sigma(s,t) = (\overbrace{-t/(2s)}^{s'}, t) \\ \tau(s,t) = (s, \underbrace{s/t}_{t'}) \end{array}}$$

e portanto,

$$\boxed{\underbrace{\tau \circ \sigma}_{\pi}(s,t) = (-t/(2s), -1/(2s)).}$$

Segue

$$\pi(\pi(s,t)) = (-1/(2t), s/t);$$

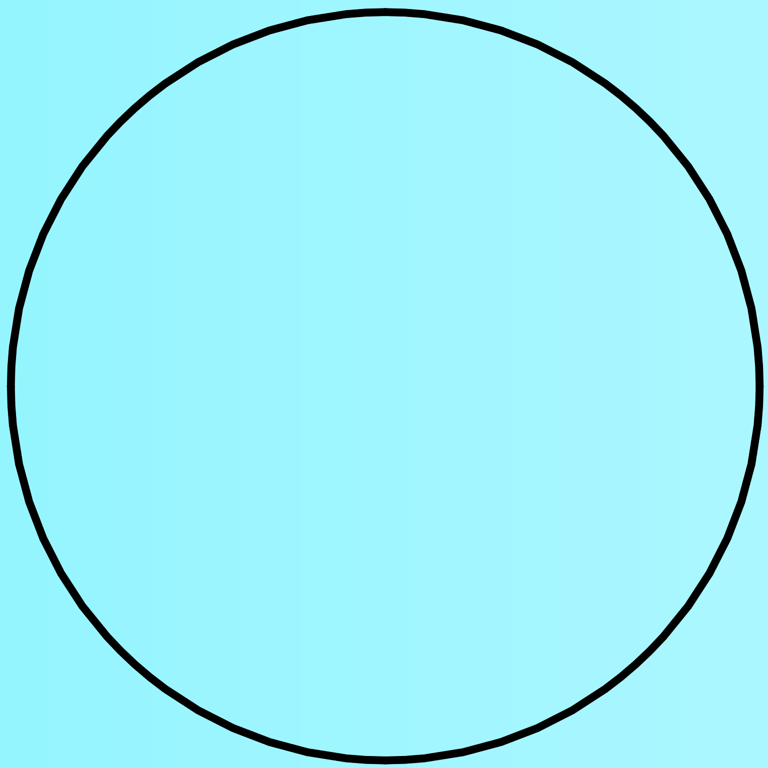
Segue

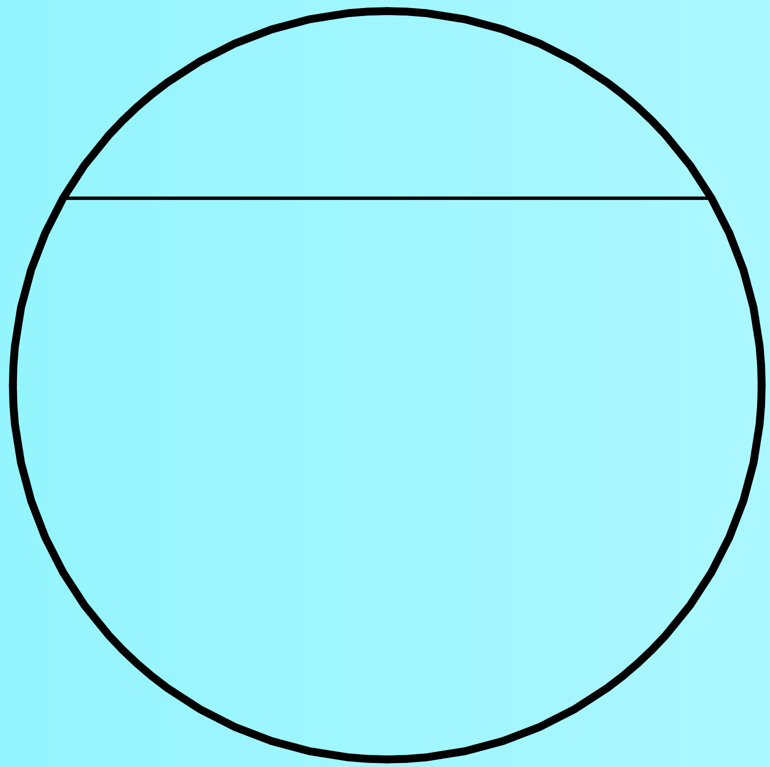
$$\pi(\pi(s,t)) = (-1/(2t), s/t);$$
$$\pi(\pi(\pi(s,t))) = (s,t).$$

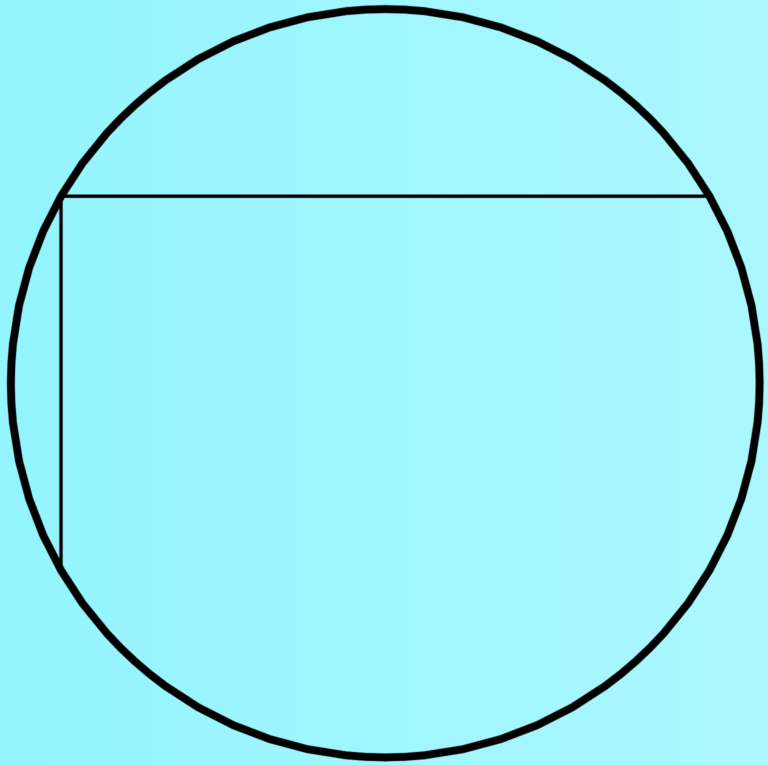
Segue

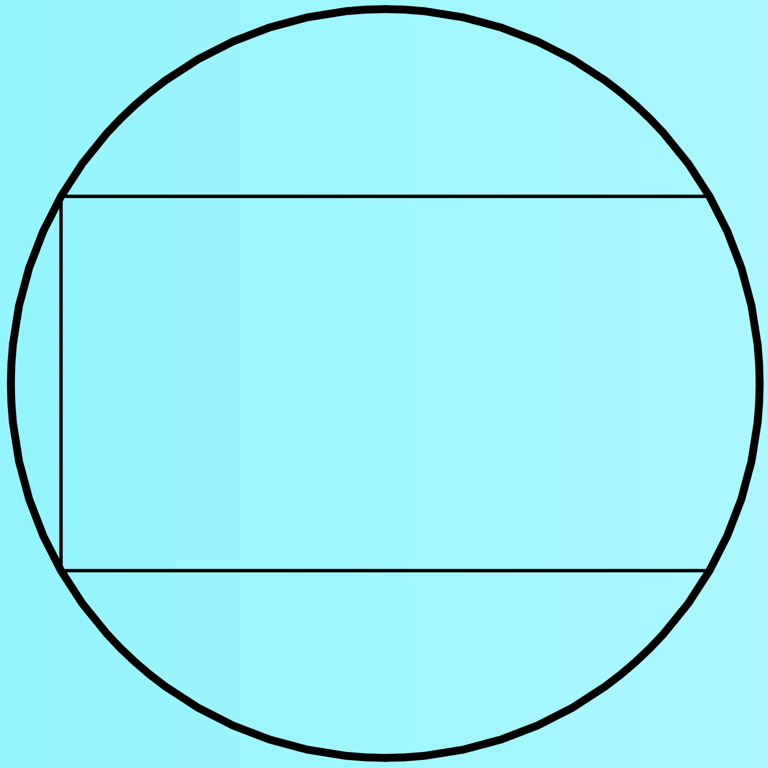
$$\pi(\pi(s,t)) = (-1/(2t), s/t);$$
$$\pi(\pi(\pi(s,t))) = (s,t).$$

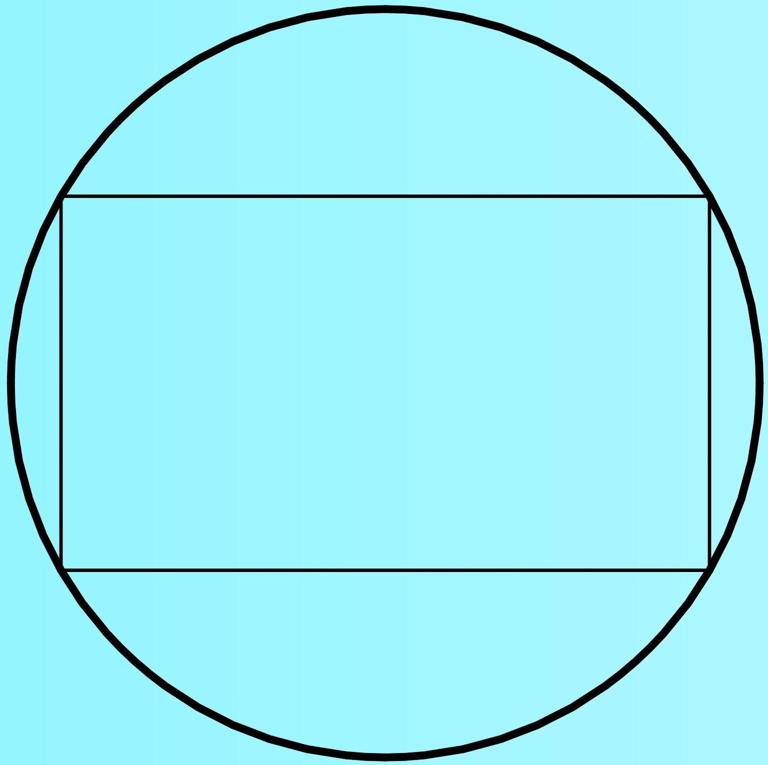
Conclusão: a poligonal inscrita/circunscrita fecha em 3 etapas, independente do ponto inicial.

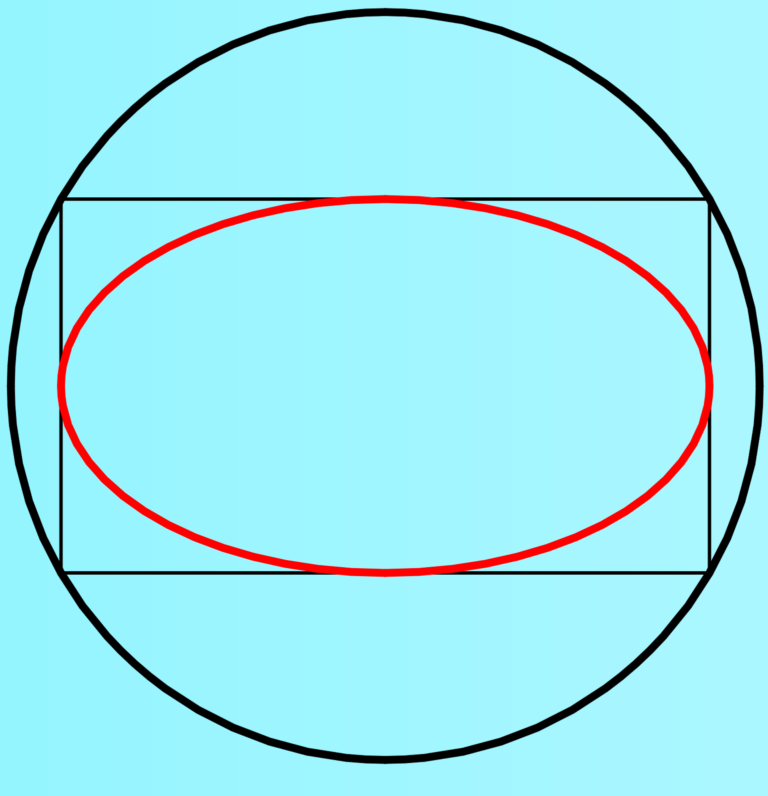


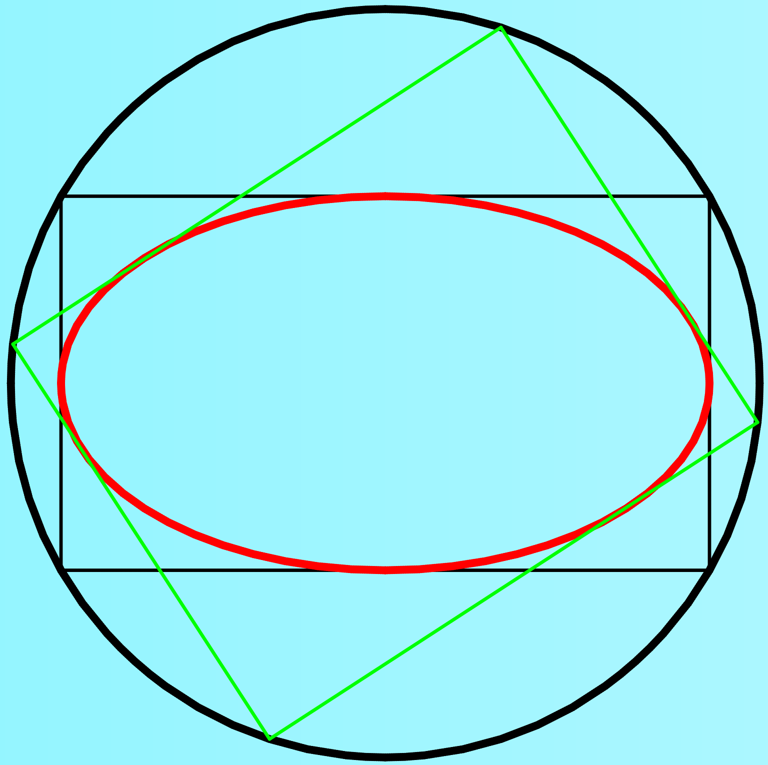












Aqui, fecha em 4 etapas. . .

Matemática $\times$ ciências naturais

Matemática$\times$ciências naturais

A maneira como a Matemática intervém nas demais ciências naturais,

Matemática$\times$ciências naturais

A maneira como a Matemática intervém
nas demais ciências naturais,
em tantas situações aparentemente desconexas,

Matemática × ciências naturais

A maneira como a Matemática intervém
nas demais ciências naturais,
em tantas situações aparentemente desconexas,
é algo que beira o irracional.

Matemática$\times$ciências naturais

A maneira como a Matemática intervém
nas demais ciências naturais,
em tantas situações aparentemente desconexas,
é algo que beira o irracional.
Não se conhece explicação plausível para

Matemática $\times$ ciências naturais

A maneira como a Matemática intervém
nas demais ciências naturais,
em tantas situações aparentemente desconexas,
é algo que beira o irracional.
Não se conhece explicação plausível para

- a habilidade do cérebro humano formar cadeias de milhares de conclusões “corretas”

Matemática×ciências naturais

A maneira como a Matemática intervém
nas demais ciências naturais,
em tantas situações aparentemente desconexas,
é algo que beira o irracional.
Não se conhece explicação plausível para

- a habilidade do cérebro humano formar cadeias de milhares de conclusões “corretas” e isentas de contradição;

Matemática $\times$ ciências naturais

A maneira como a Matemática intervém
nas demais ciências naturais,
em tantas situações aparentemente desconexas,
é algo que beira o irracional.
Não se conhece explicação plausível para

- a habilidade do cérebro humano formar cadeias de milhares de conclusões "corretas" e isentas de contradição;
- e muito menos,

Matemática $\times$ ciências naturais

A maneira como a Matemática intervém
nas demais ciências naturais,
em tantas situações aparentemente desconexas,
é algo que beira o irracional.
Não se conhece explicação plausível para

- a habilidade do cérebro humano formar cadeias de milhares de conclusões “corretas” e isentas de contradição;
- e muito menos, para essa estranha capacidade de se “adivinhar” leis da natureza.

-Eugene Wigner, *The Unreasonable Effectiveness of Mathematics in the Natural Sciences*,
Communications in Pure and Applied Mathematics,
vol. 13, No. I (February 1960).
John Wiley & Sons, Inc.

teoria × prática

teoria $\times$ prática

Admitimos que muitos dos problemas clássicos importantes são ligados a questões ditas objetivas.

teoria $\times$ prática

Admitimos que muitos dos problemas clássicos importantes são ligados a questões ditas objetivas. Entretanto, parcela considerável da motivação imediata do matemático no exercício de sua profissão,

teoria $\times$ prática

Admitimos que muitos dos problemas clássicos importantes são ligados a questões ditas objetivas. Entretanto, parcela considerável da motivação imediata do matemático no exercício de sua profissão, parece se processar em um nível muito mais íntimo,

teoria × prática

Admitimos que muitos dos problemas clássicos importantes são ligados a questões ditas objetivas. Entretanto, parcela considerável da motivação imediata do matemático no exercício de sua profissão, parece se processar em um nível muito mais íntimo, semelhante, digamos, ao do compositor

teoria $\times$ prática

Admitimos que muitos dos problemas clássicos
importantes são ligados a questões ditas objetivas.
Entretanto, parcela considerável da motivação imediata
do matemático no exercício de sua profissão,
parece se processar em um nível muito mais íntimo,
semelhante, digamos, ao do compositor ou artista
que se encanta mais com sua própria apreciação estética.

teoria $\times$ prática

Admitimos que muitos dos problemas clássicos
importantes são ligados a questões ditas objetivas.
Entretanto, parcela considerável da motivação imediata
do matemático no exercício de sua profissão,
parece se processar em um nível muito mais íntimo,
semelhante, digamos, ao do compositor ou artista
que se encanta mais com sua própria apreciação estética.

A aceitação ou reconhecimento do grande público
passa a segundo plano.

O matemático “típico” não tenta em seu dia-a-dia ser “útil”.

O matemático “típico” não tenta em seu dia-a-dia ser “útil”.

Seríamos movidos a

Seríamos movidos a

60% de curiosidade intelectual,

Seríamos movidos a

60% de curiosidade intelectual,

30% de ambição,

Seríamos movidos a

60% de curiosidade intelectual,

30% de ambição, mais uns

20% de café...

Seríamos movidos a

60% de curiosidade intelectual,

30% de ambição, mais uns

20% de café...

Seríamos movidos a

60% de curiosidade intelectual,

30% de ambição, mais uns

20% de café...

Seríamos movidos a

60% de curiosidade intelectual,

30% de ambição, mais uns

20% de café...

(Só conheço três tipos de cientistas:

Seríamos movidos a

60% de curiosidade intelectual,

30% de ambição, mais uns

20% de café...

(Só conheço três tipos de cientistas:

os que sabem Matemática

Seríamos movidos a

60% de curiosidade intelectual,

30% de ambição, mais uns

20% de café...

(Só conheço três tipos de cientistas:
os que sabem Matemática e ...

Seríamos movidos a

60% de curiosidade intelectual,

30% de ambição, mais uns

20% de café...

(Só conheço três tipos de cientistas:
os que sabem Matemática e ... os que não...:-)

Com isso em mente, confesso minha perplexidade

Com isso em mente, confesso minha perplexidade diante da rapidez com que vários tópicos,

Com isso em mente, confesso minha perplexidade
diante da rapidez com que vários tópicos,
que até bem pouco eram estudados por razões
plausíveis apenas para o especialista,

Com isso em mente, confesso minha perplexidade
diante da rapidez com que vários tópicos,
que até bem pouco eram estudados por razões
plausíveis apenas para o especialista,
passam a ser de enorme relevo

Com isso em mente, confesso minha perplexidade
diante da rapidez com que vários tópicos,
que até bem pouco eram estudados por razões
plausíveis apenas para o especialista,
passam a ser de enorme relevo
–impiedosamente presentes, quem diria,

Com isso em mente, confesso minha perplexidade
diante da rapidez com que vários tópicos,
que até bem pouco eram estudados por razões
plausíveis apenas para o especialista,
passam a ser de enorme relevo
–impiedosamente presentes, quem diria,
em cada conversação telefônica,

Com isso em mente, confesso minha perplexidade
diante da rapidez com que vários tópicos,
que até bem pouco eram estudados por razões
plausíveis apenas para o especialista,
passam a ser de enorme relevo
–impiedosamente presentes, quem diria,
em cada conversação telefônica,
ou acesso à internet.

caixa de surpresas

caixa de surpresas

Exemplo marcante dessa caixa de surpresas,

caixa de surpresas

Exemplo marcante dessa caixa de surpresas,
até para o mais otimista dos matemáticos

caixa de surpresas

Exemplo marcante dessa caixa de surpresas,
até para o mais otimista dos matemáticos
é o que vamos expor, em linhas muito gerais:

caixa de surpresas

Exemplo marcante dessa caixa de surpresas,
até para o mais otimista dos matemáticos
é o que vamos expor, em linhas muito gerais:

a intervenção, no nosso dia a dia,

caixa de surpresas

Exemplo marcante dessa caixa de surpresas,
até para o mais otimista dos matemáticos
é o que vamos expor, em linhas muito gerais:

a intervenção, no nosso dia a dia,
das venerandas *curvas elípticas*.

Já não se faz criptografia como antigamente

Já não se faz criptografia como antigamente

A *criptografia*

Já não se faz criptografia como antigamente

A *criptografia*

$\boxed{\text{do grego Kryptos: escondido,}}$

Já não se faz criptografia como antigamente

A *criptografia*

$\boxed{\text{do grego Kryptos: escondido,}}$

e

$\boxed{\text{Graphos: escritura}}$

Já não se faz criptografia como antigamente

A *criptografia*

$\boxed{\text{do grego Kryptos: escondido,}}$

e

$\boxed{\text{Graphos: escritura}}$

é a ciência que estuda formas de codificar uma mensagem,

Já não se faz criptografia como antigamente

A *criptografia*

do grego Kryptos: escondido,

e

Graphos: escritura

é a ciência que estuda formas de codificar uma mensagem, tornando-a jodpnqsffotjxfm

Já não se faz criptografia como antigamente

A *criptografia*

$\boxed{\text{do grego Kryptos: escondido,}}$

e

$\boxed{\text{Graphos: escritura}}$

é a ciência que estuda formas de codificar uma mensagem, tornando-a jodpnqsffotjxfm para quem não

Já não se faz criptografia como antigamente

A *criptografia*

$\boxed{\text{do grego Kryptos: escondido,}}$

e

$\boxed{\text{Graphos: escritura}}$

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

Já não se faz criptografia como antigamente

A *criptografia*

$\boxed{\text{do grego Kryptos: escondido,}}$

e

$\boxed{\text{Graphos: escritura}}$

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

Já não se faz criptografia como antigamente

A *criptografia*

do grego Kryptos: escondido,

e

Graphos: escritura

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

Trata-se, em suma,

Já não se faz criptografia como antigamente

A *criptografia*

$\boxed{\text{do grego Kryptos: escondido,}}$

e

$\boxed{\text{Graphos: escritura}}$

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

incompreensível

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

(entre parênteses

Mencionemos brevemente,

(entre parênteses

Mencionemos brevemente,
a título de + propaganda que,

(entre parênteses

Mencionemos brevemente,
a título de $+$ propaganda que,
as curvas elípticas acima mencionadas,

(entre parênteses

Mencionemos brevemente,
a título de + propaganda que,
as curvas elípticas acima mencionadas,
aparecem na solução do "último teorema de Fermat".

Cubum autem in duos cubos **Cubo em dois cubos,**

Cubum autem in duos cubos aut quadratoquadratum in

Cubo em dois cubos, quadrado de um quadrado em

Cubum autem in duos cubos aut quadratoquadratum in duos quadratoquadratos

Cubo em dois cubos, quadrado de um quadrado em dois quadrados de quadrados

Cubum autem in duos cubos aut quadratoquadratum in duos quadratoquadratos et generaliter nullam

Cubo em dois cubos, quadrado de um quadrado em dois quadrados de quadrados e mais geralmente, nenhuma

Cubum autem in duos cubos aut quadratoquadratum in duos quadratoquadratos et generaliter nullam in infinitum ultra quadratum	**Cubo em dois cubos, quadrado de um quadrado em dois quadrados de quadrados e mais geralmente, nenhuma potência maior que dois**

Cubum autem in duos cubos aut quadratoquadratum in duos quadratoquadratos et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem

Cubo em dois cubos, quadrado de um quadrado em dois quadrados de quadrados e mais geralmente, nenhuma potência maior que dois em duas potências de mesmo

Cubum autem in duos cubos aut quadratoquadratum in duos quadratoquadratos et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere:

Cubo em dois cubos, quadrado de um quadrado em dois quadrados de quadrados e mais geralmente, nenhuma potência maior que dois em duas potências de mesmo expoente se pode dividir:

Cubum autem in duos cubos
aut quadratoquadratum in
duos quadratoquadratos
et generaliter nullam
in infinitum ultra quadratum
potestatem in duos ejusdem
nominis fas est dividere:
cujus rei demonstrationem

Cubo em dois cubos,
quadrado de um quadrado em
dois quadrados de quadrados
e mais geralmente, nenhuma
potência maior que dois
em duas potências de mesmo
expoente se pode dividir:
achei uma demonstração

Cubum autem in duos cubos
aut quadratoquadratum in
duos quadratoquadratos
et generaliter nullam
in infinitum ultra quadratum
potestatem in duos ejusdem
nominis fas est dividere:
cujus rei demonstrationem
mirabilem sane detexi.

Cubo em dois cubos,
quadrado de um quadrado em
dois quadrados de quadrados
e mais geralmente, nenhuma
potência maior que dois
em duas potências de mesmo
expoente se pode dividir:
achei uma demonstração
extraordinária. Mas

Cubum autem in duos cubos
aut quadratoquadratum in
duos quadratoquadratos
et generaliter nullam
in infinitum ultra quadratum
potestatem in duos ejusdem
nominis fas est dividere:
cujus rei demonstrationem
mirabilem sane detexi.

Hanc
marginis
exiguitas
non

Cubo em dois cubos,
quadrado de um quadrado em
dois quadrados de quadrados
e mais geralmente, nenhuma
potência maior que dois
em duas potências de mesmo
expoente se pode dividir:
achei uma demonstração
extraordinária. Mas

nesta
margem
exígua
não

Cubum autem in duos cubos
aut quadratoquadratum in
duos quadratoquadratos
et generaliter nullam
in infinitum ultra quadratum
potestatem in duos ejusdem
nominis fas est dividere:
cujus rei demonstrationem
mirabilem sane detexi.

Hanc
marginis
exiguitas
non caperet.

Cubo em dois cubos,
quadrado de um quadrado em
dois quadrados de quadrados
e mais geralmente, nenhuma
potência maior que dois
em duas potências de mesmo
expoente se pode dividir:
achei uma demonstração
extraordinária. Mas

nesta
margem
exígua
não cabe.

Hoje em dia, diríamos. . .

se $n \geq 3$, a equação

$$X^n + Y^n = Z^n$$

não admite solução

com X, Y, Z, n

números inteiros > 0.

Os meandros que,

Os meandros que, em meados da década passada[1],

[1] André Wiles, *Modular elliptic curves and Fermat's Last Theorem.* Ann. Math. (2) 141, No.3, 443-551 (1995).

Os meandros que, em meados da década passada[1],

[1] André Wiles, *Modular elliptic curves and Fermat's Last Theorem.* Ann. Math. (2) 141, No.3, 443-551 (1995).
Richard Taylor & Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras.* Ann. Math. (2) 141, No.3, 553-572 (1995)

Os meandros que, em meados da década passada[1], levaram à demonstração do célebre "último teorema de Fermat",

---

[1] André Wiles, *Modular elliptic curves and Fermat's Last Theorem.* Ann. Math. (2) 141, No.3, 443-551 (1995).
Richard Taylor & Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras.* Ann. Math. (2) 141, No.3, 553-572 (1995)

Os meandros que, em meados da década passada[1],
levaram à demonstração do célebre
"último teorema de Fermat",
não caberiam naquela,

[1] André Wiles, *Modular elliptic curves and Fermat's Last Theorem.*
Ann. Math. (2) 141, No.3, 443-551 (1995).
Richard Taylor & Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras.*
Ann. Math. (2) 141, No.3, 553-572 (1995)

Os meandros que, em meados da década passada[1],
levaram à demonstração do célebre
"último teorema de Fermat",
não caberiam naquela,
nem em muito mais generosas margens...

---

[1] André Wiles, *Modular elliptic curves and Fermat's Last Theorem.* Ann. Math. (2) 141, No.3, 443-551 (1995).
Richard Taylor & Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras.* Ann. Math. (2) 141, No.3, 553-572 (1995)

Na argumentação de Wiles & Taylor,

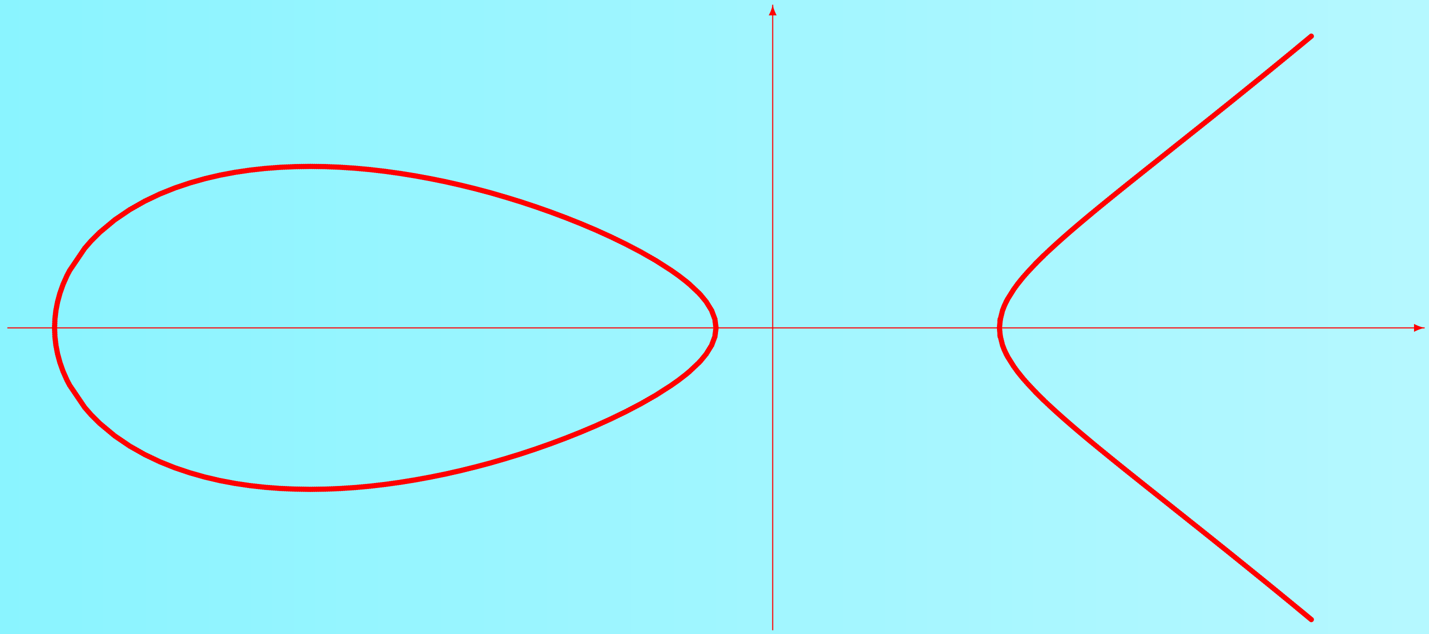
Na argumentação de Wiles & Taylor,
já popularizada com toques novelescos ,

Na argumentação de Wiles & Taylor,
já popularizada com toques novelescos,[2]

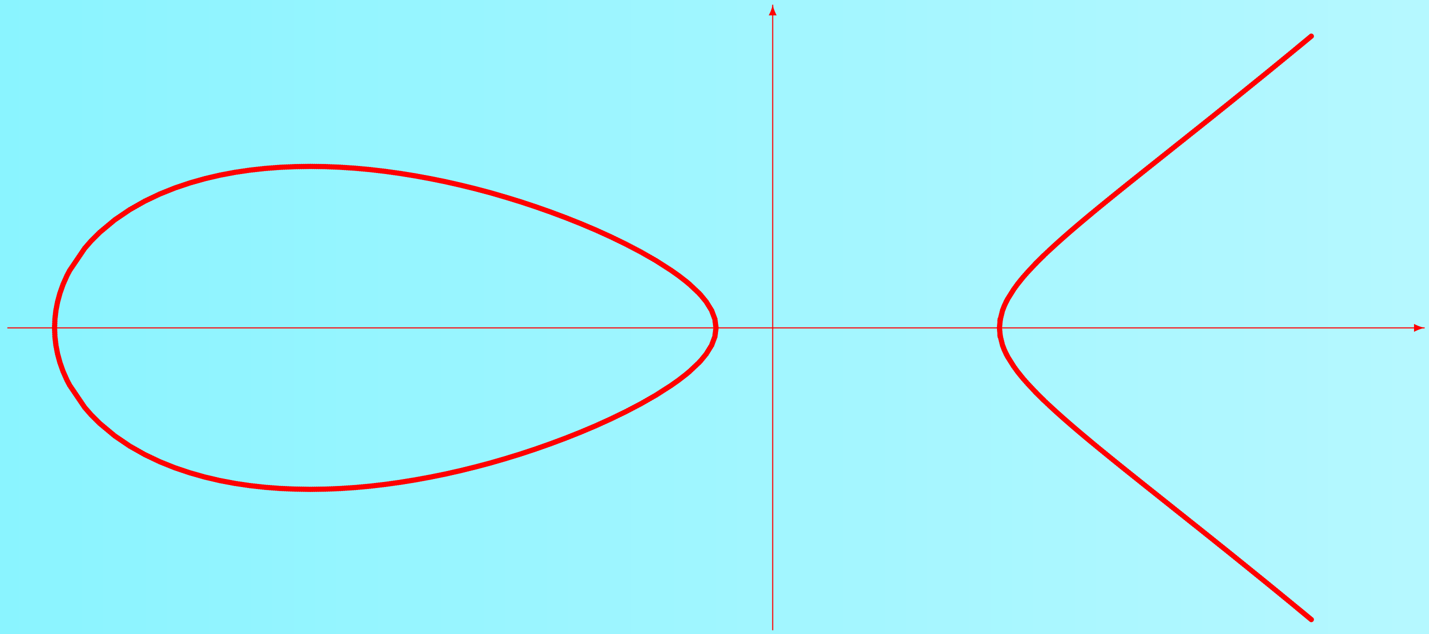
[2] Simon Singh, *O Último Teorema De Fermat*

Na argumentação de Wiles & Taylor,
já popularizada com toques novelescos,[2]
desempenha papel central
uma certa curva plana de grau três:

[2] Simon Singh, *O Último Teorema De Fermat*

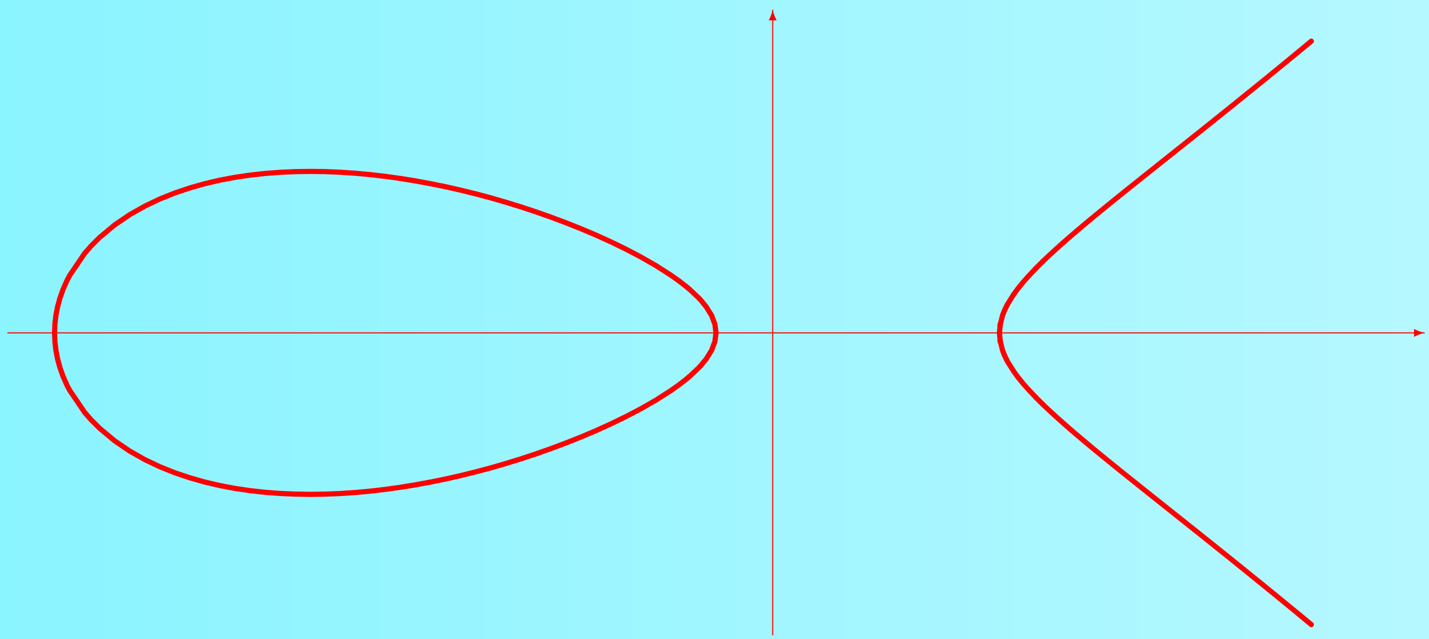


A cúbica $y^2 = (x-a)(x-b)(x-c)$.



A cúbica $y^2 = (x-a)(x-b)(x-c)$.

Este é o tipo de curva elíptica acima aludida.



A cúbica $y^2 = (x-a)(x-b)(x-c)$.

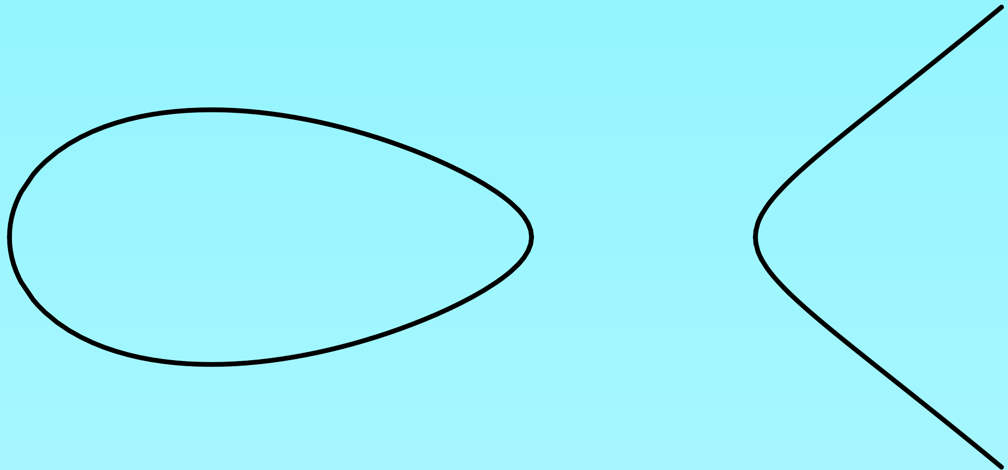
Este é o tipo de curva elíptica acima aludida.

FECHA PARÊNTESES! :-)

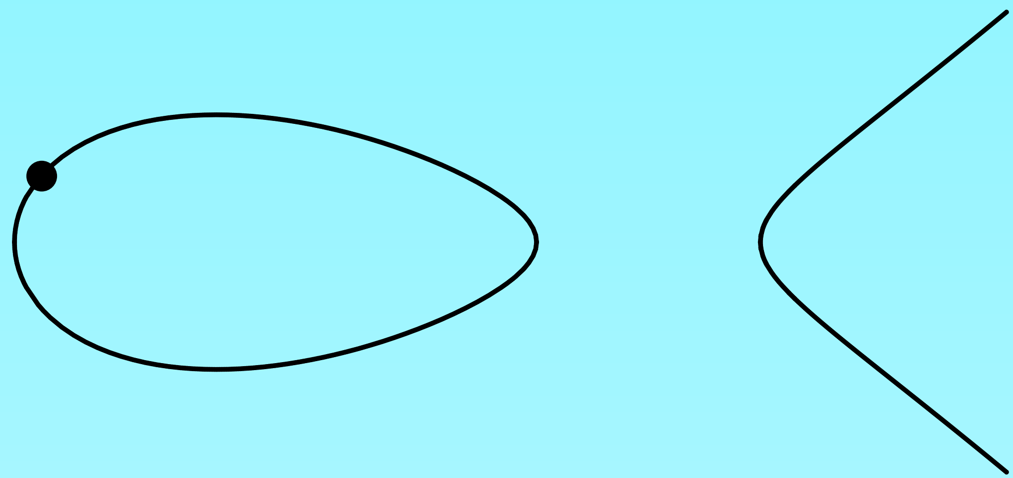
Por motivos diversos, o sucesso da utilização de curvas elípticas em criptografia deve-se ao fato de que

Por motivos diversos, o sucesso da utilização de curvas elípticas em criptografia deve-se ao fato de que elas admitem uma operação binária natural:

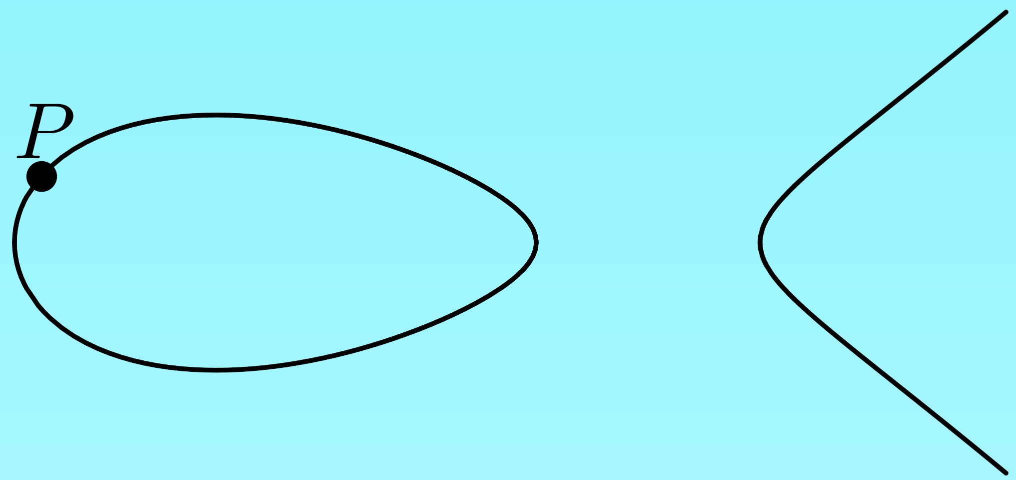
Por motivos diversos, o sucesso da utilização de curvas elípticas em criptografia deve-se ao fato de que elas admitem uma operação binária natural:



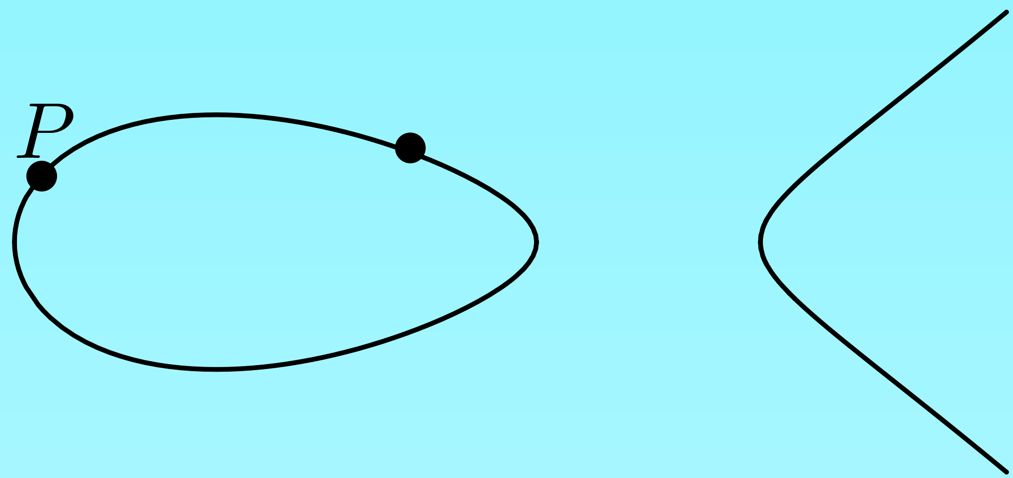
Por motivos diversos, o sucesso da utilização de curvas elípticas em criptografia deve-se ao fato de que elas admitem uma operação binária natural:



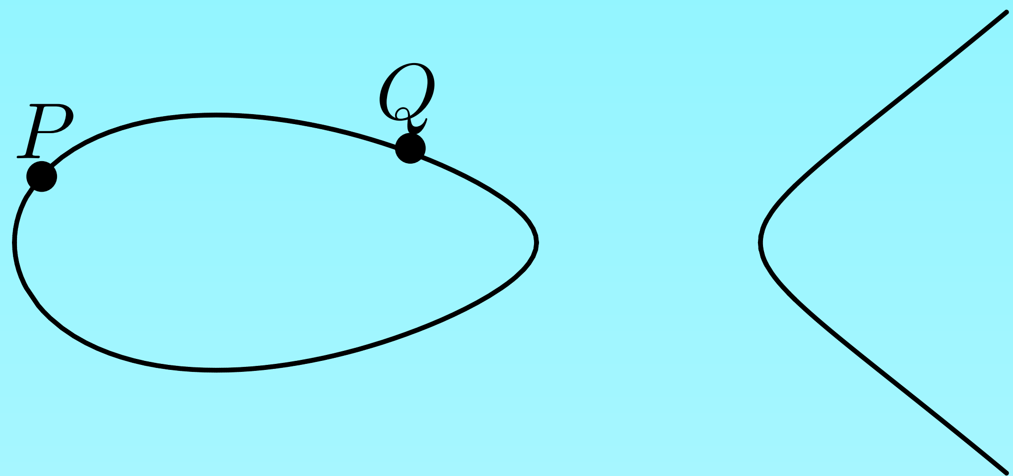
Por motivos diversos, o sucesso da utilização de curvas elípticas em criptografia deve-se ao fato de que elas admitem uma operação binária natural:



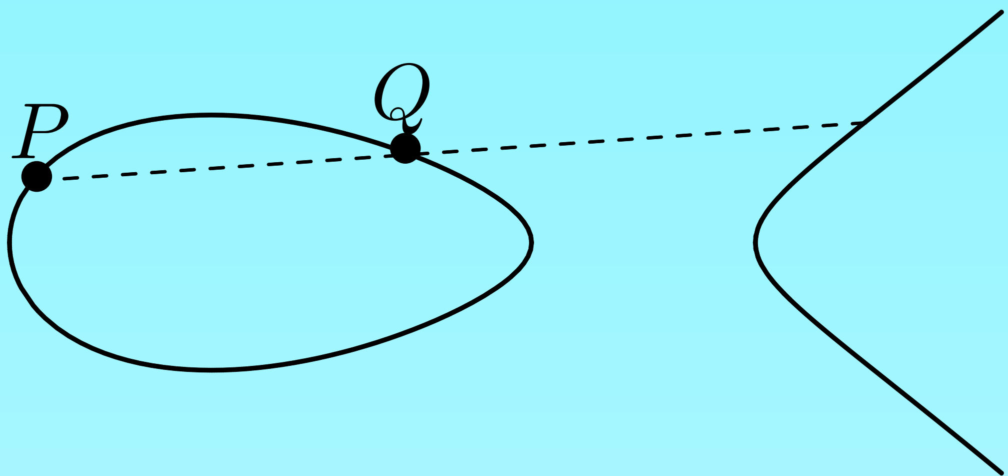
Por motivos diversos, o sucesso da utilização de curvas elípticas em criptografia deve-se ao fato de que elas admitem uma operação binária natural:



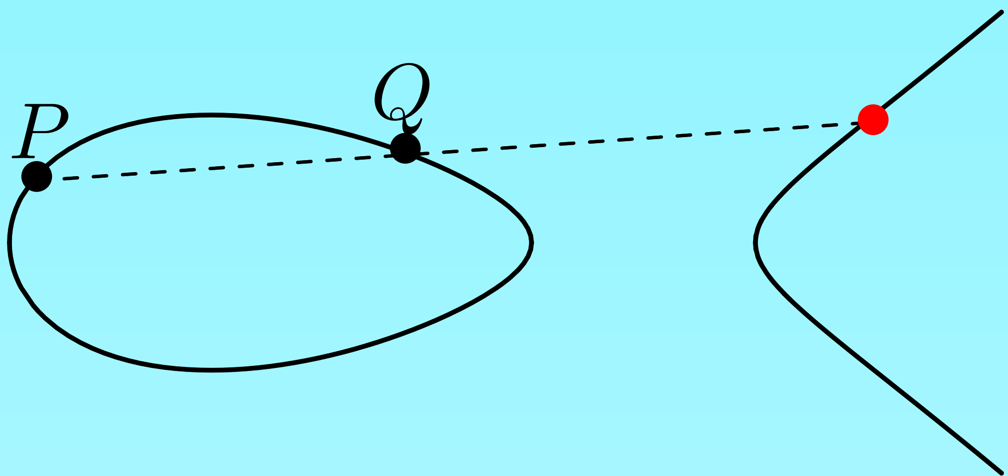
Por motivos diversos, o sucesso da utilização de curvas elípticas em criptografia deve-se ao fato de que elas admitem uma operação binária natural:



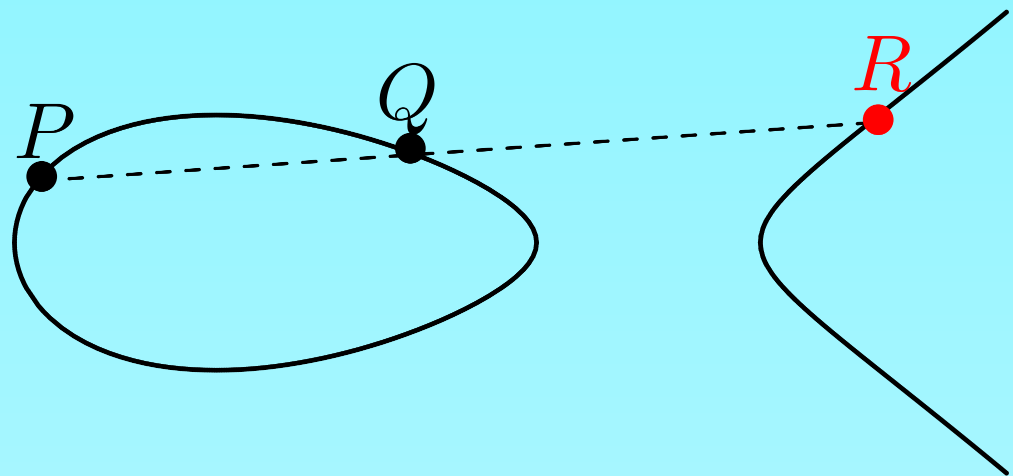
Por motivos diversos, o sucesso da utilização de curvas elípticas em criptografia deve-se ao fato de que elas admitem uma operação binária natural:



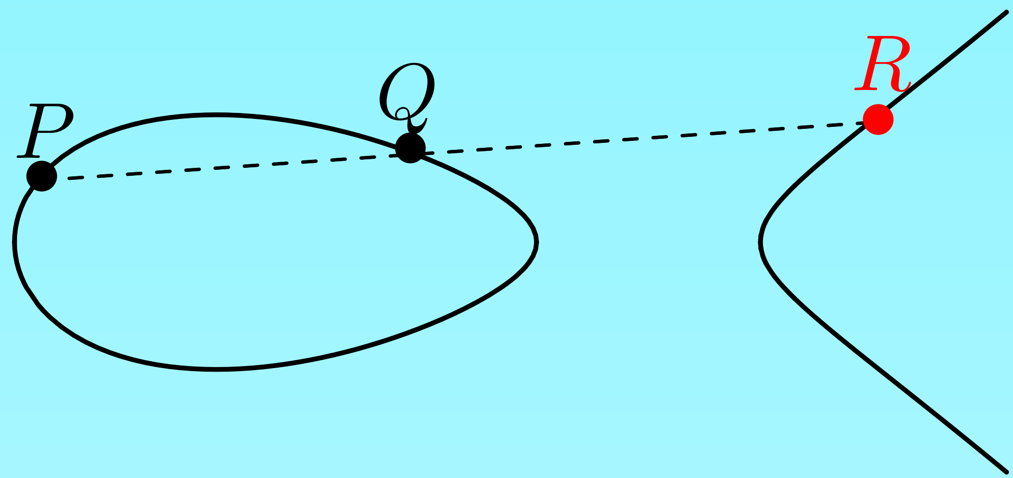
Por motivos diversos, o sucesso da utilização de curvas elípticas em criptografia deve-se ao fato de que elas admitem uma operação binária natural:



Por motivos diversos, o sucesso da utilização de curvas elípticas em criptografia deve-se ao fato de que elas admitem uma operação binária natural:

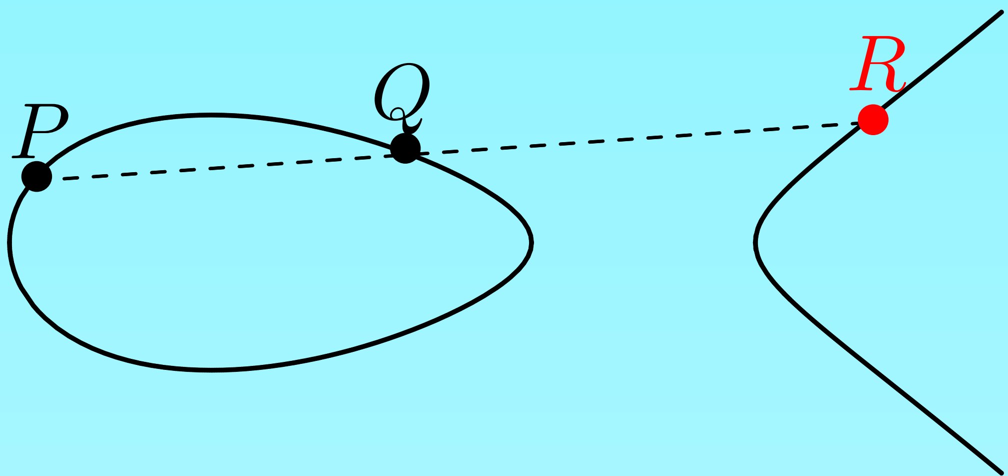


Por motivos diversos, o sucesso da utilização de curvas elípticas em criptografia deve-se ao fato de que elas admitem uma operação binária natural:



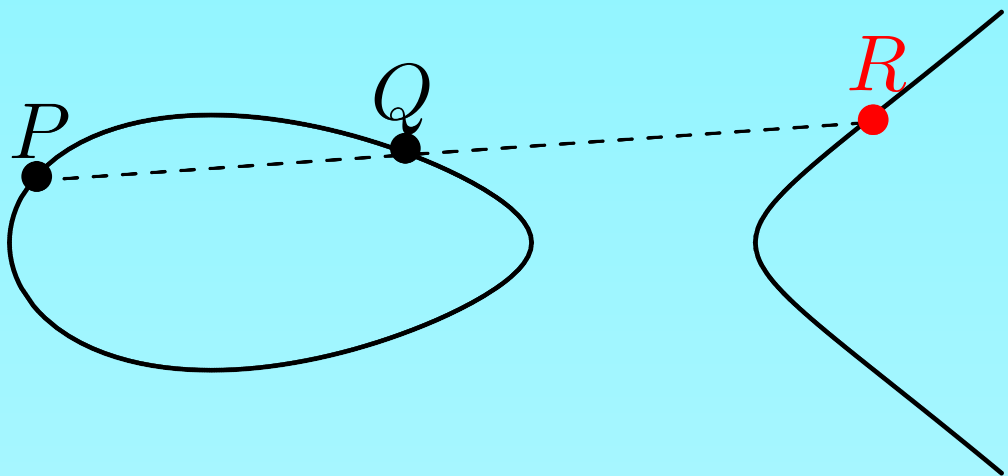
A cada par de pontos, P, Q na curva,

Por motivos diversos, o sucesso da utilização de curvas elípticas em criptografia deve-se ao fato de que elas admitem uma operação binária natural:



A cada par de pontos, P, Q na curva, associa-se o terceiro ponto de interseção da reta $\overline{PQ}$

Por motivos diversos, o sucesso da utilização de curvas elípticas em criptografia deve-se ao fato de que elas admitem uma operação binária natural:



A cada par de pontos, P, Q na curva, associa-se o terceiro ponto de interseção da reta $\overline{PQ}$ com a curva de grau três, $y^2 = (x-a)(x-b)(x-c)$.

Esta regra simples fornece uma maneira eficiente de “embaralhar”

Esta regra simples fornece uma maneira eficiente
de “embaralhar” *i.e.*, codificar dados
para transmissão e posterior decodificação.

Esta regra simples fornece uma maneira eficiente de “embaralhar” *i.e.*, codificar dados para transmissão e posterior decodificação.

Notável nessa história é que,

Esta regra simples fornece uma maneira eficiente
de "embaralhar" *i.e.*, codificar dados
para transmissão e posterior decodificação.

Notável nessa história é que,
enquanto a raiz da motivação (intra-matemática)
é de natureza geométrica

Esta regra simples fornece uma maneira eficiente
de "embaralhar" *i.e.*, codificar dados
para transmissão e posterior decodificação.

Notável nessa história é que,
enquanto a raiz da motivação (intra-matemática)
é de natureza geométrica
(interseções de retas e curvas planas),

Esta regra simples fornece uma maneira eficiente
de “embaralhar” *i.e.*, codificar dados
para transmissão e posterior decodificação.

Notável nessa história é que,
enquanto a raiz da motivação (intra-matemática)
é de natureza geométrica
(interseções de retas e curvas planas),
o ambiente em que se passam as operações de
ciframento é de caráter aritmético (modular, de fato).

A criptografia, na forma que vem sendo desenvolvida nos últimos anos, depende, por um lado,

A criptografia, na forma que vem sendo desenvolvida nos últimos anos, depende, por um lado,

- da produção de números primos grandes
  $(2, 3, 5, 7, 11, 13, 17,$

A criptografia, na forma que vem sendo desenvolvida nos últimos anos, depende, por um lado,

- da produção de números primos grandes ($2, 3, 5, 7, 11, 13, 17$, . . . ,2963, 2969, 2971, 2.999,. . . , $\Large 122.921$,. . . ,

A criptografia, na forma que vem sendo desenvolvida nos últimos anos, depende, por um lado,

- da produção de números primos grandes ($2, 3, 5, 7, 11, 13, 17$, . . . ,$2963, 2969, 2971$, 2.999,. . . , 122.921,. . . , $10.000.000.019$,...),

A criptografia, na forma que vem sendo desenvolvida nos últimos anos, depende, por um lado,

- da produção de números primos grandes ($2, 3, 5, 7, 11, 13, 17,$ . . . ,2963, 2969, 2971, 2.999,. . . , 122.921,. . . , 10.000.000.019,...),

e por outro,

- da dificuldade prática de fatorar números grandes.

Em linhas muito gerais, os sistemas de criptografia são baseados em *grupos finitos abelianos*.

Em linhas muito gerais, os sistemas de criptografia são baseados em *grupos finitos abelianos*.

A segurança do sistema depende da dificuldade na resolução do chamado

Em linhas muito gerais, os sistemas de criptografia são baseados em $grupos\ finitos\ abelianos$.

A segurança do sistema depende da dificuldade na resolução do chamado

problema do logaritmo discreto (PLD):

dados elementos h e g em um grupo cíclico G,

Em linhas muito gerais, os sistemas de criptografia são baseados em *grupos finitos abelianos*.

A segurança do sistema depende da dificuldade na resolução do chamado

problema do logaritmo discreto (PLD):

dados elementos h e g em um grupo cíclico G,
deve-se resolver a equação

$$h = g^{x}$$

com x número inteiro positivo, menor possível.

PLD para alguns grupos, *e.g.*, o grupo aditivo de um corpo finito é considerado computacionalmente trivial.

PLD para alguns grupos, *e.g.*, o grupo aditivo de um corpo finito é considerado computacionalmente trivial.

O tipo de grupo comumente usado é o grupo multiplicativo $\mathbb{F}_q^*$.

PLD para alguns grupos, *e.g.*, o grupo aditivo de um corpo finito é considerado computacionalmente trivial.

O tipo de grupo comumente usado é o grupo multiplicativo $\mathbb{F}_q^*$.

No entanto aqui, o item "segurança" só funciona para q enorme,

PLD para alguns grupos, *e.g.*, o grupo aditivo de um corpo finito é considerado computacionalmente trivial.

O tipo de grupo comumente usado é o grupo multiplicativo $\mathbb{F}_q^*$.

No entanto aqui, o item "segurança" só funciona para q enorme, pois são conhecidos métodos "sub-exponenciais" para PLD.

PLD para alguns grupos, *e.g.*, o grupo aditivo de um corpo finito é considerado computacionalmente trivial.

O tipo de grupo comumente usado é o grupo multiplicativo $\mathbb{F}_q^*$.

No entanto aqui, o item “segurança” só funciona para q enorme, pois são conhecidos métodos “sub-exponenciais” para PLD.

No caso do grupo associado a uma curva elíptica sobre um corpo finito

PLD para alguns grupos, *e.g.*, o grupo aditivo de um corpo finito é considerado computacionalmente trivial.

O tipo de grupo comumente usado é o grupo multiplicativo $\mathbb{F}_q^*$.

No entanto aqui, o item “segurança” só funciona para q enorme, pois são conhecidos métodos “sub-exponenciais” para PLD.

No caso do grupo associado a uma curva elíptica sobre um corpo finito o melhor método conhecido para PLD é de complexidade exponencial no tamanho $n = [\log_2 q]$.

Na CCE clássica, é importante produzir com eficiência equações da forma

Na CCE clássica, é importante produzir com eficiência equações da forma

$$E: \; y^2 = x^3 + ax + b$$

Na CCE clássica, é importante produzir com eficiência equações da forma

$$E: \; y^2 = x^3 + ax + b$$

com $a, b \in \mathbb{F}_q$, o corpo finito,

Na CCE clássica, é importante produzir com eficiência equações da forma

$$E: \; y^2 = x^3 + ax + b$$

com $a, b \in \mathbb{F}_q$, o corpo finito, onde

$$\boxed{q = p^N,\ p = \text{número primo ímpar.}}$$

Na CCE clássica, é importante produzir com eficiência equações da forma

$$E: \; y^2 = x^3 + ax + b$$

com $a, b \in \mathbb{F}_q$, o corpo finito, onde

$$\boxed{q = p^N,\ p = \text{número primo ímpar.}}$$

(o caso $p = 2$ é similar, mas a forma da equação acima muda.)

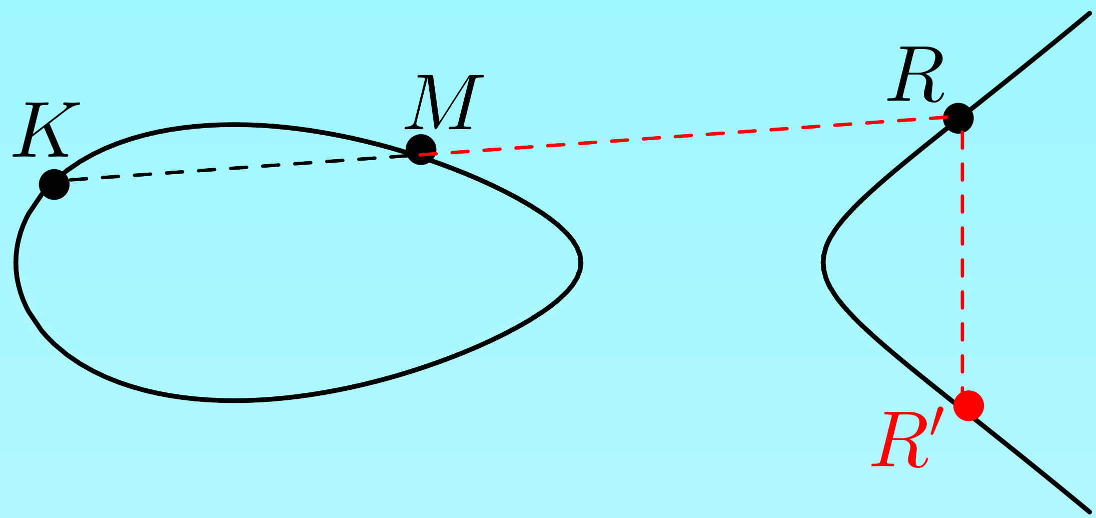
Grosso modo, cada mensagem se representa
por um ponto da curva, *i.e.*,
um par $M(x, y) \in \mathbb{F}_q^2$ satisfazendo a referida equação.

Grosso modo, cada mensagem se representa
por um ponto da curva, *i.e.*,
um par $M(x, y) \in \mathbb{F}_q^2$ satisfazendo a referida equação.

A exemplo do RSA, a codificação é feita usando uma lei de grupo, definida na curva na forma indicada na figura

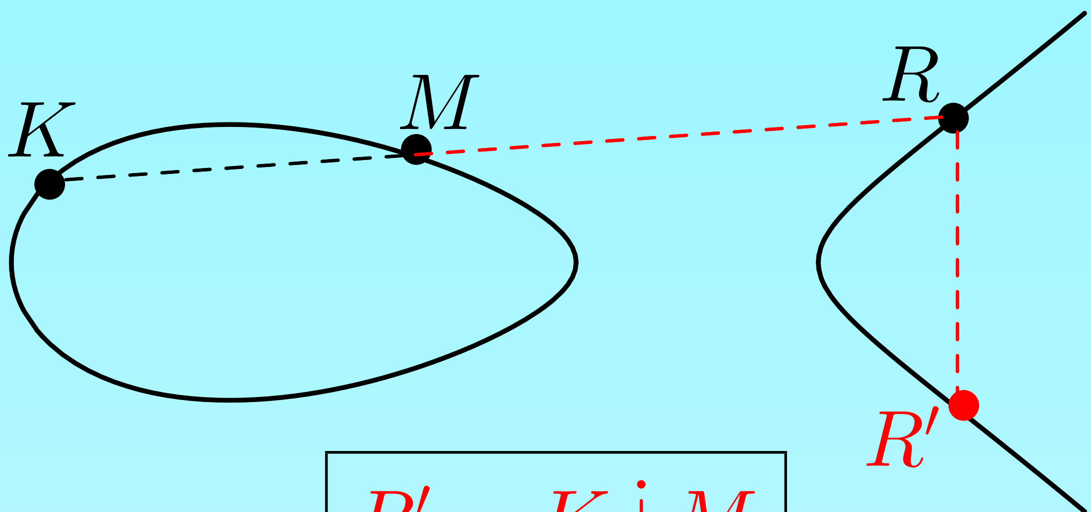
Grosso modo, cada mensagem se representa
por um ponto da curva, *i.e.*,
um par $M(x, y) \in \mathbb{F}_q^2$ satisfazendo a referida equação.

A exemplo do RSA, a codificação é feita usando uma lei de grupo, definida na curva na forma indicada na figura



Grosso modo, cada mensagem se representa por um ponto da curva, *i.e.*, um par $M(x, y) \in \mathbb{F}_q^2$ satisfazendo a referida equação.

A exemplo do RSA, a codificação é feita usando uma lei de grupo, definida na curva na forma indicada na figura



$$\boxed{R' = K \dot{+} M}$$

A chave de codificação é dada pela escolha judiciosa do ponto K.

A chave de codificação é dada pela escolha judiciosa do ponto K.

É desejável que a equação

$$\boxed{nK = 0,\ n \geq 1}$$

A chave de codificação é dada pela escolha judiciosa do ponto K.

É desejável que a equação

$$\boxed{nK = 0,\ n \geq 1}$$

só admita solução $n >> 0$.

A chave de codificação é dada pela escolha judiciosa do ponto K.

É desejável que a equação

$$\boxed{nK = 0,\ n \geq 1}$$

só admita solução $n >> 0$.

A segurança do sistema depende de que,

A chave de codificação é dada pela escolha judiciosa do ponto K.

É desejável que a equação

$$\boxed{nK = 0,\ n \geq 1}$$

só admita solução $n >> 0$.

A segurança do sistema depende de que, conhecidos a curva, o ponto K e um múltiplo mK,

A chave de codificação é dada pela escolha judiciosa do ponto K.

É desejável que a equação

$$\boxed{nK = 0,\ n \geq 1}$$

só admita solução $n >> 0$.

A segurança do sistema depende de que, conhecidos a curva, o ponto K e um múltiplo mK, seja difícil inferir m.

transmissão segura

Ana quer enviar um segredo a Bruno e não confia no portador.

transmissão segura

Ana quer enviar um segredo a Bruno e não confia no portador. Ela remete uma caixa com cadeado inviolável.

transmissão segura

Ana quer enviar um segredo a Bruno e não confia no portador. Ela remete uma caixa com cadeado inviolável. Bruno recebe,

transmissão segura

Ana quer enviar um segredo a Bruno e não confia no portador. Ela remete uma caixa com cadeado inviolável. Bruno recebe, mas não pode abrir o cadeado da Ana :-(.

transmissão segura

Ana quer enviar um segredo a Bruno e não confia no portador. Ela remete uma caixa com cadeado inviolável. Bruno recebe, mas não pode abrir o cadeado da Ana :-(. Põe outro cadeado e devolve a caixa para Ana.

transmissão segura

Ana quer enviar um segredo a Bruno e não confia no portador. Ela remete uma caixa com cadeado inviolável.
Bruno recebe, mas não pode abrir o cadeado da Ana :-(.
Põe outro cadeado e devolve a caixa para Ana.
Ela retira o seu cadeado e re-envia a Bruno!

transmissão segura

Ana quer enviar um segredo a Bruno e não confia no portador. Ela remete uma caixa com cadeado inviolável. Bruno recebe, mas não pode abrir o cadeado da Ana :-(. Põe outro cadeado e devolve a caixa para Ana. Ela retira o seu cadeado e re-envia a Bruno!

Na "prática", o cadeado de Ana é $aK =$

transmissão segura

Ana quer enviar um segredo a Bruno e não confia no portador. Ela remete uma caixa com cadeado inviolável. Bruno recebe, mas não pode abrir o cadeado da Ana :-(. Põe outro cadeado e devolve a caixa para Ana. Ela retira o seu cadeado e re-envia a Bruno!

Na "prática", o cadeado de Ana é $aK = \overbrace{K + \cdots + K}^{a}$;

transmissão segura

Ana quer enviar um segredo a Bruno e não confia no portador. Ela remete uma caixa com cadeado inviolável. Bruno recebe, mas não pode abrir o cadeado da Ana :-(. Põe outro cadeado e devolve a caixa para Ana.
Ela retira o seu cadeado e re-envia a Bruno!

Na "prática", o cadeado de Ana é $aK = \overbrace{K + \cdots + K}^{a}$; o de Bruno, bK.

transmissão segura

Ana quer enviar um segredo a Bruno e não confia no portador. Ela remete uma caixa com cadeado inviolável. Bruno recebe, mas não pode abrir o cadeado da Ana :-(. Põe outro cadeado e devolve a caixa para Ana. Ela retira o seu cadeado e re-envia a Bruno!

Na "prática", o cadeado de Ana é $aK = \overbrace{K + \cdots + K}^{a}$; o de Bruno, bK. A mensagem M (digitalizada) é enviada como $(aK + M)$.

transmissão segura

Ana quer enviar um segredo a Bruno e não confia no portador. Ela remete uma caixa com cadeado inviolável. Bruno recebe, mas não pode abrir o cadeado da Ana :-(. Põe outro cadeado e devolve a caixa para Ana.
Ela retira o seu cadeado e re-envia a Bruno!

Na "prática", o cadeado de Ana é $aK = \overbrace{K + \cdots + K}^{a}$; o de Bruno, bK. A mensagem M (digitalizada) é enviada como $(aK + M)$. Bruno devolve $(bK + aK + M)$;

transmissão segura

Ana quer enviar um segredo a Bruno e não confia no portador. Ela remete uma caixa com cadeado inviolável. Bruno recebe, mas não pode abrir o cadeado da Ana :-(. Põe outro cadeado e devolve a caixa para Ana. Ela retira o seu cadeado e re-envia a Bruno!

Na "prática", o cadeado de Ana é $aK = \overbrace{K + \cdots + K}^{a}$; o de Bruno, bK. A mensagem M (digitalizada) é enviada como $(aK + M)$. Bruno devolve $(bK + aK + M)$; Ana re-envia $(-aK + (bK + aK + M))$.

transmissão segura

Ana quer enviar um segredo a Bruno e não confia no portador. Ela remete uma caixa com cadeado inviolável. Bruno recebe, mas não pode abrir o cadeado da Ana :-(. Põe outro cadeado e devolve a caixa para Ana. Ela retira o seu cadeado e re-envia a Bruno!

Na "prática", o cadeado de Ana é $aK = \overbrace{K + \cdots + K}^{a}$; o de Bruno, bK. A mensagem M (digitalizada) é enviada como $(aK + M)$. Bruno devolve $(bK + aK + M)$; Ana re-envia $(-aK + (bK + aK + M))$. Daqui Bruno recupera seguramente a mensagem M.

transmissão segura

Ana quer enviar um segredo a Bruno e não confia no portador. Ela remete uma caixa com cadeado inviolável. Bruno recebe, mas não pode abrir o cadeado da Ana :-(. Põe outro cadeado e devolve a caixa para Ana. Ela retira o seu cadeado e re-envia a Bruno!

Na "prática", o cadeado de Ana é $aK = \overbrace{K + \cdots + K}^{a}$; o de Bruno, bK. A mensagem M (digitalizada) é enviada como $(aK + M)$. Bruno devolve $(bK + aK + M)$; Ana re-envia $(-aK + (bK + aK + M))$. Daqui Bruno recupera seguramente a mensagem M.

(Simon Singh, *The Code Book.*)

Dados

$$\boxed{P_1 = (x_1, y_1),\ P_2 = (x_2, y_2) \in E,}$$

Dados

$$\boxed{P_1 = (x_1, y_1),\ P_2 = (x_2, y_2) \in E,}$$

para o cálculo efetivo de

$$\boxed{P_3 = P_1 \dot{+} P_2}$$

Dados

$$\boxed{P_1 = (x_1, y_1),\ P_2 = (x_2, y_2) \in E,}$$

para o cálculo efetivo de

$$\boxed{P_3 = P_1 \dot{+} P_2}$$

achamos a interseção da curva elíptica E com a reta $\overline{P_1 P_2}$,

$$\overline{P_1P_2} \; : \; \begin{vmatrix} x_1 & x_2 & x \\ y_1 & y_2 & y \\ 1 & 1 & 1 \end{vmatrix}$$

$$\overline{P_1 P_2} : \begin{vmatrix} x_1 & x_2 & x \\ y_1 & y_2 & y \\ 1 & 1 & 1 \end{vmatrix} =$$

$$\boxed{(y_1 - y_2)x - (x_1 - x_2)y + (x_1 y_2 - x_2 y_1) = 0.}$$

$$\overline{P_1P_2} : \begin{vmatrix} x_1 & x_2 & x \\ y_1 & y_2 & y \\ 1 & 1 & 1 \end{vmatrix} =$$

$$\boxed{(y_1 - y_2)x - (x_1 - x_2)y + (x_1y_2 - x_2y_1) = 0.}$$

Abreviamos

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2},\ \mu = \frac{x_1y_2 - x_2y_1}{x_1 - x_2}\ .$$

$$\overline{P_1P_2}\ : \left| \begin{array}{ccc} x_1 & x_2 & x \\ y_1 & y_2 & y \\ 1 & 1 & 1 \end{array} \right| =$$

$$\boxed{(y_1 - y_2)x - (x_1 - x_2)y + (x_1y_2 - x_2y_1) = 0.}$$

Abreviamos

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2},\ \mu = \frac{x_1y_2 - x_2y_1}{x_1 - x_2}\ .$$

Substituindo $y = \lambda x + \mu$ na curva E, resulta uma eq. do $3^{\underline{o}}$ grau em x,

resulta uma eq. do 3º grau em x,

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)\, x + \left(b - \mu^2\right) = 0$$

resulta uma eq. do 3º grau em x,

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)\, x + \left(b - \mu^2\right) = 0$$

da qual $x = x_1, x = x_2$ já são raízes, por hipótese.

resulta uma eq. do 3º grau em x,

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)\, x + \left(b - \mu^2\right) = 0$$

da qual $x = x_1, x = x_2$ já são raízes, por hipótese.
A 3ª raiz, x_3, se calcula coletando coeficiente

resulta uma eq. do 3º grau em x,

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)\, x + \left(b - \mu^2\right) = 0$$

da qual $x = x_1, x = x_2$ já são raízes, por hipótese.
A 3ª raiz, x_3, se calcula coletando coeficiente

$$x_3 = \lambda^2 - x_1 - x_2$$

resulta uma eq. do 3º grau em x,

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)\, x + \left(b - \mu^2\right) = 0$$

da qual $x = x_1, x = x_2$ já são raízes, por hipótese.
A 3ª raiz, x_3, se calcula coletando coeficiente

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ &\therefore \\ y_3 &= -\left(\lambda\left(\lambda^2 - (x_1 + x_2)\right) + \mu\right) \\ &= -(\lambda(x_3 - x_1) + y_1) \ \text{(troca sinal.)} \end{aligned}$$

Para “dobrar”, *i.e.*, calcular $2P$,

Para “dobrar”, *i.e.*, calcular $2P$, a reta $\overline{P_1P_2}$ usada acima é substituída pela tangente no ponto P, com coeficiente angular

Para "dobrar", *i.e.*, calcular $2P$, a reta $\overline{P_1P_2}$ usada acima é substituída pela tangente no ponto P, com coeficiente angular

$$\begin{aligned} \lambda &= -\left(\partial E/\partial x\right)\Big/\left(\partial E/\partial y\right) \\ &= \tfrac{a+3x_1^2}{2y_1}; \end{aligned}$$

Para “dobrar”, *i.e.*, calcular $2P$, a reta $\overline{P_1P_2}$ usada acima é substituída pela tangente no ponto P, com coeficiente angular

$$\begin{aligned} \lambda &= -\left(\partial E/\partial x\right) \big/ \left(\partial E/\partial y\right) \\ &= \tfrac{a+3x_1^2}{2y_1}; \\ y &= y_1 + \lambda(x - x_1). \ \text{(reta tg.)} \end{aligned}$$

Para “dobrar”, *i.e.*, calcular $2P$, a reta $\overline{P_1P_2}$ usada acima é substituída pela tangente no ponto P, com coeficiente angular

$$\begin{aligned} \lambda &= -\left(\partial E/\partial x\right)\Big/\left(\partial E/\partial y\right) \\ &= \tfrac{a+3x_1^2}{2y_1}; \\ y &= y_1 + \lambda(x - x_1). \ \text{(reta tg.)} \end{aligned}$$

Como antes, resulta

$$\begin{aligned} x_3 &= \lambda^2 - 2x_1 \\ &\therefore \\ y_3 &= -\left(\lambda\left(\lambda^2 - 2x_1\right) + \mu\right) \\ &= -\left(\lambda(x_3 - x_1) + y_1\right) \end{aligned}$$

Existem fórmulas recursivas, polinomiais, para o cálculo de $m \cdot P$. Veja a 1ª das referências.

Por fim, volta a Poncelet

Por fim, volta a Poncelet

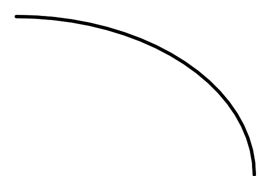
Mencionemos um modelo geométrico alternativo para CCE,

Por fim, volta a Poncelet

Mencionemos um modelo geométrico alternativo para CCE, no qual a cúbica é substituída por um par de cônicas:

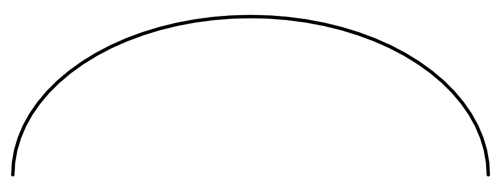
Por fim, volta a Poncelet

Mencionemos um modelo geométrico alternativo para CCE, no qual a cúbica é substituída por um par de cônicas:



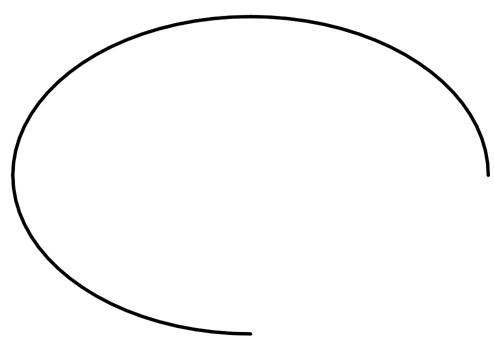
Por fim, volta a Poncelet

Mencionemos um modelo geométrico alternativo para CCE, no qual a cúbica é substituída por um par de cônicas:



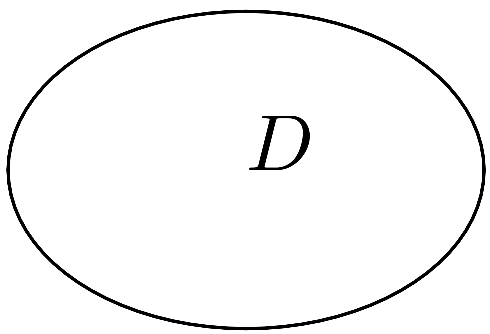
Por fim, volta a Poncelet

Mencionemos um modelo geométrico alternativo para CCE, no qual a cúbica é substituída por um par de cônicas:



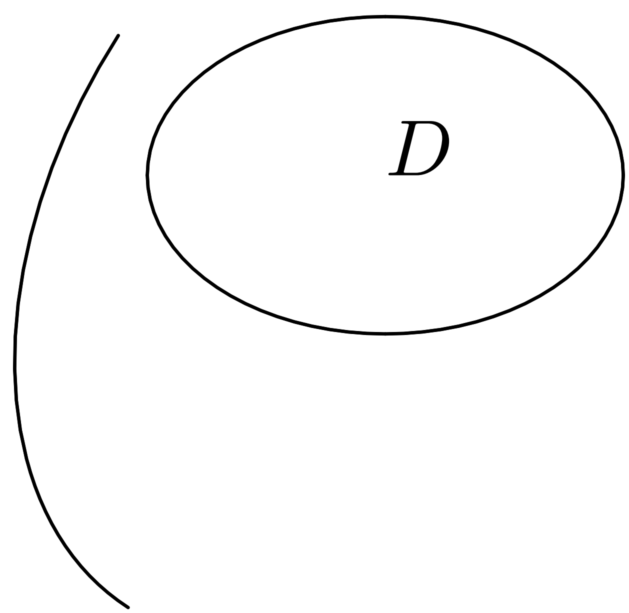
Por fim, volta a Poncelet

Mencionemos um modelo geométrico alternativo para CCE, no qual a cúbica é substituída por um par de cônicas:



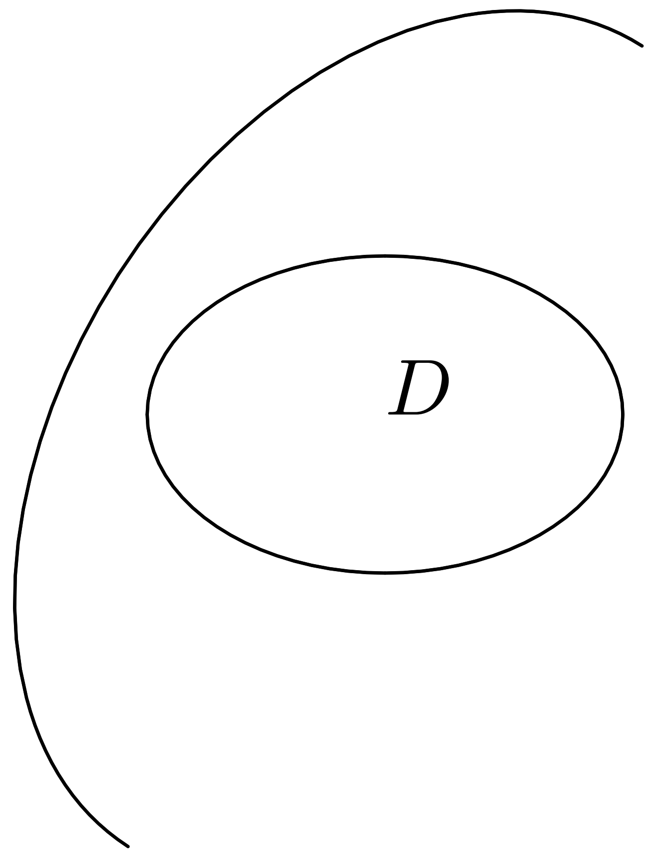
Por fim, volta a Poncelet

Mencionemos um modelo geométrico alternativo para CCE, no qual a cúbica é substituída por um par de cônicas:



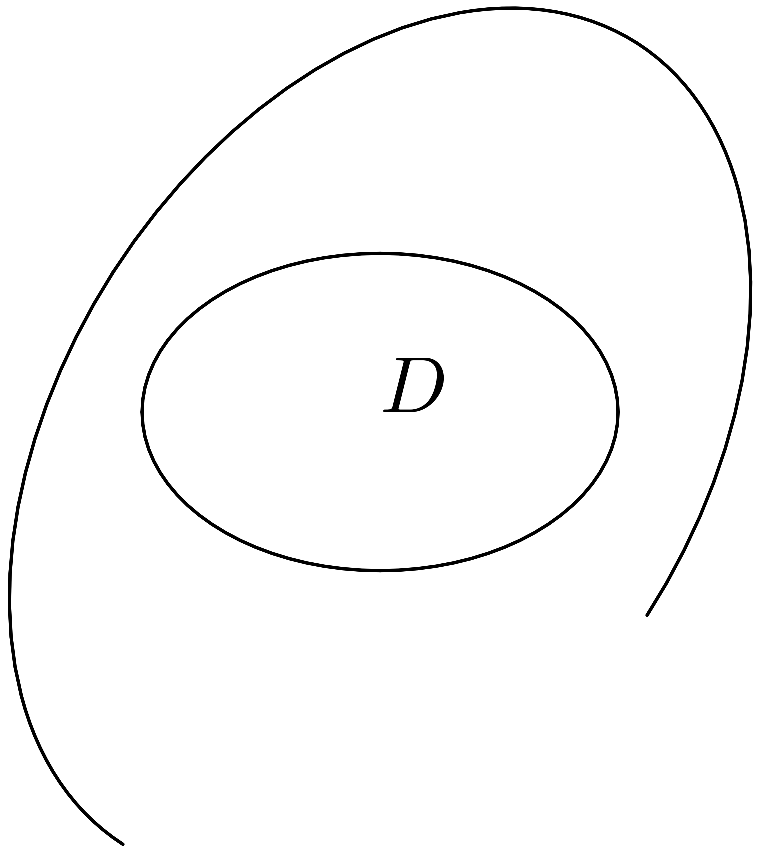
Por fim, volta a Poncelet

Mencionemos um modelo geométrico alternativo para CCE, no qual a cúbica é substituída por um par de cônicas:



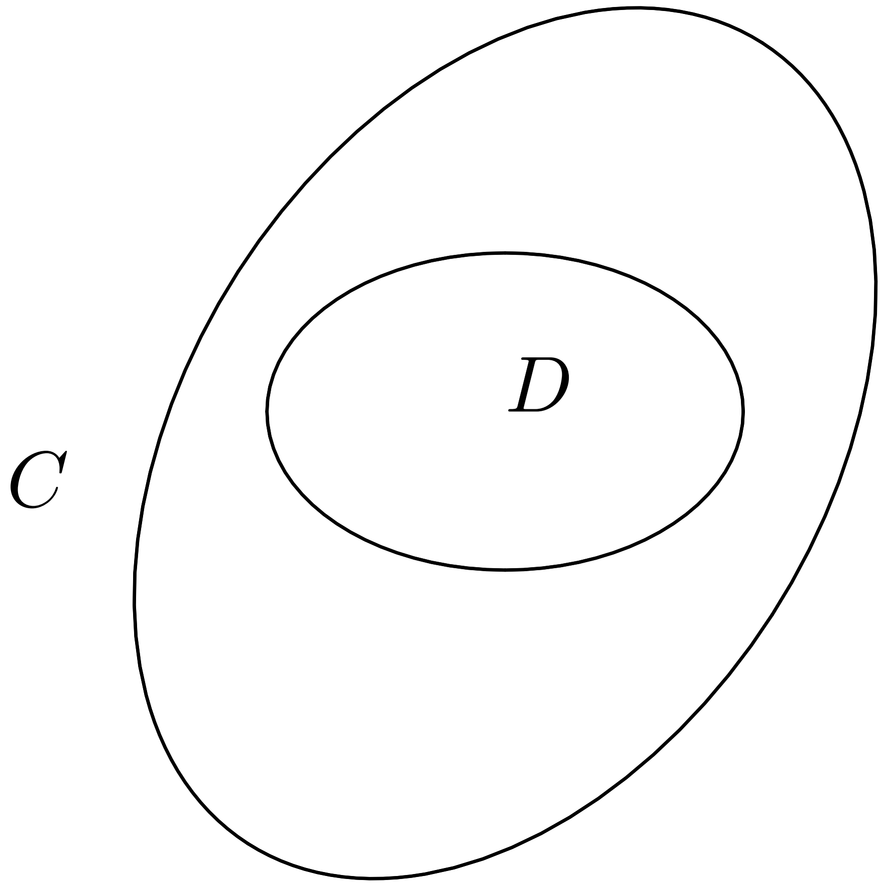
Por fim, volta a Poncelet

Mencionemos um modelo geométrico alternativo para CCE, no qual a cúbica é substituída por um par de cônicas:



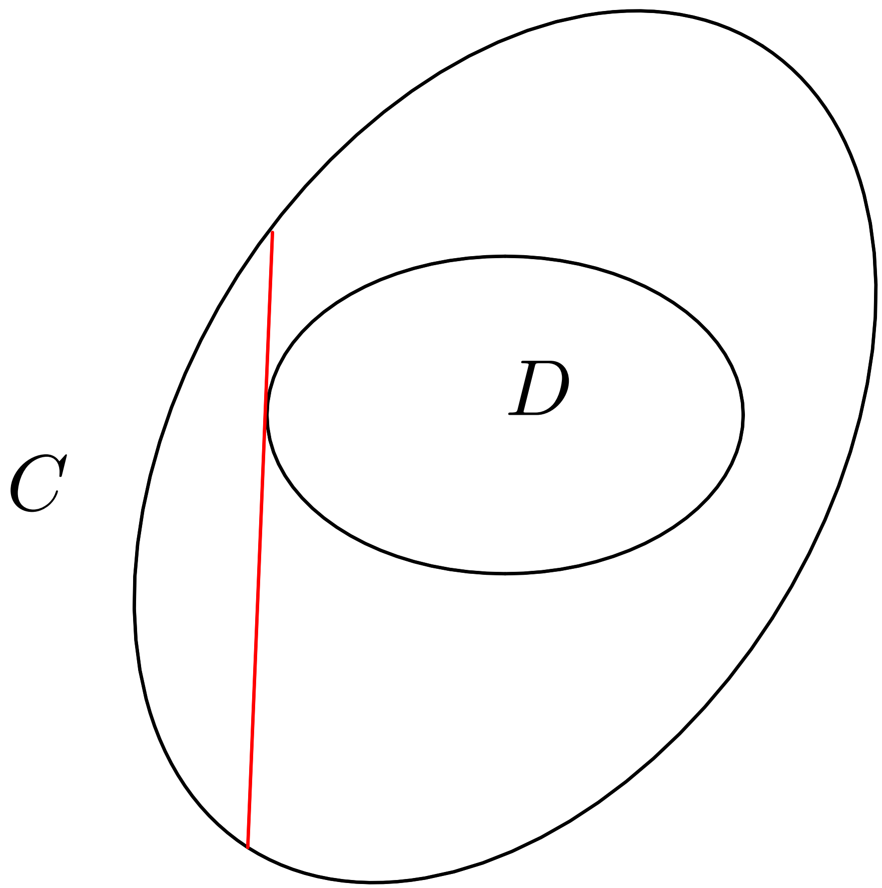
Por fim, volta a Poncelet

Mencionemos um modelo geométrico alternativo para CCE, no qual a cúbica é substituída por um par de cônicas:



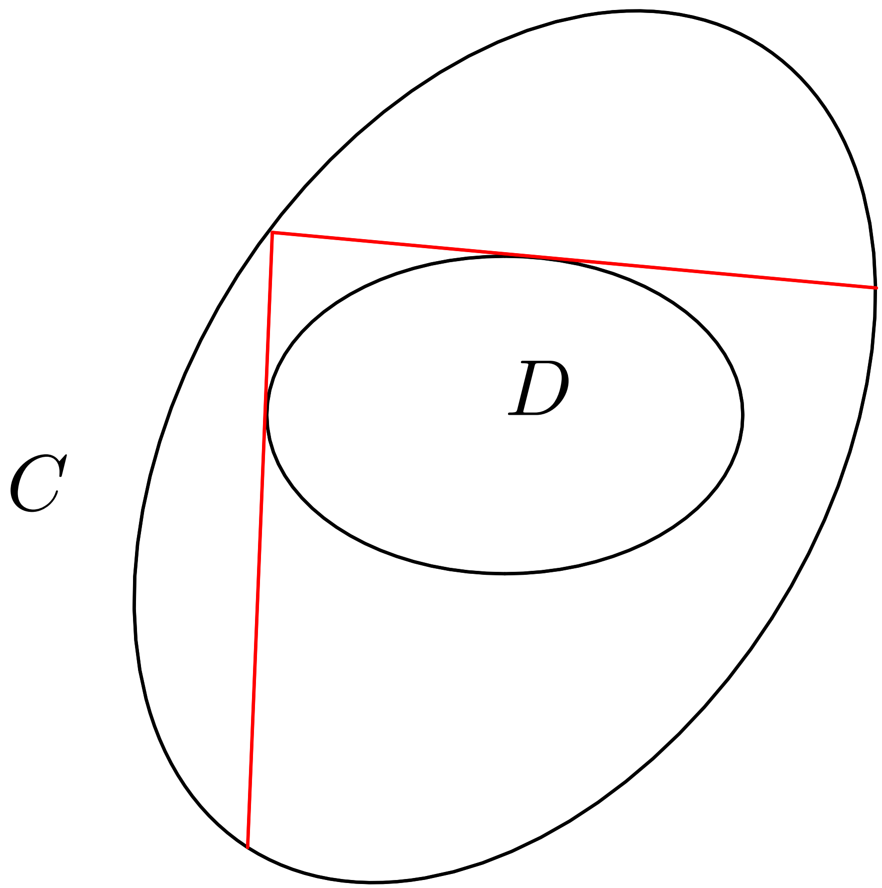
Por fim, volta a Poncelet

Mencionemos um modelo geométrico alternativo para CCE, no qual a cúbica é substituída por um par de cônicas:



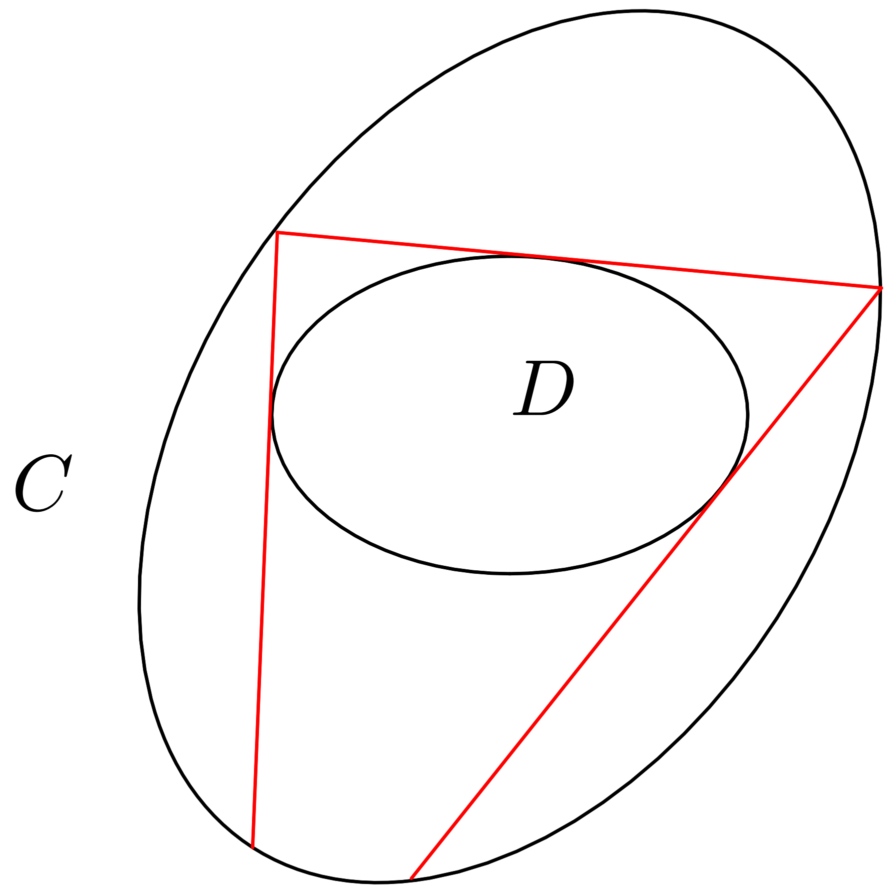
Por fim, volta a Poncelet

Mencionemos um modelo geométrico alternativo para CCE, no qual a cúbica é substituída por um par de cônicas:



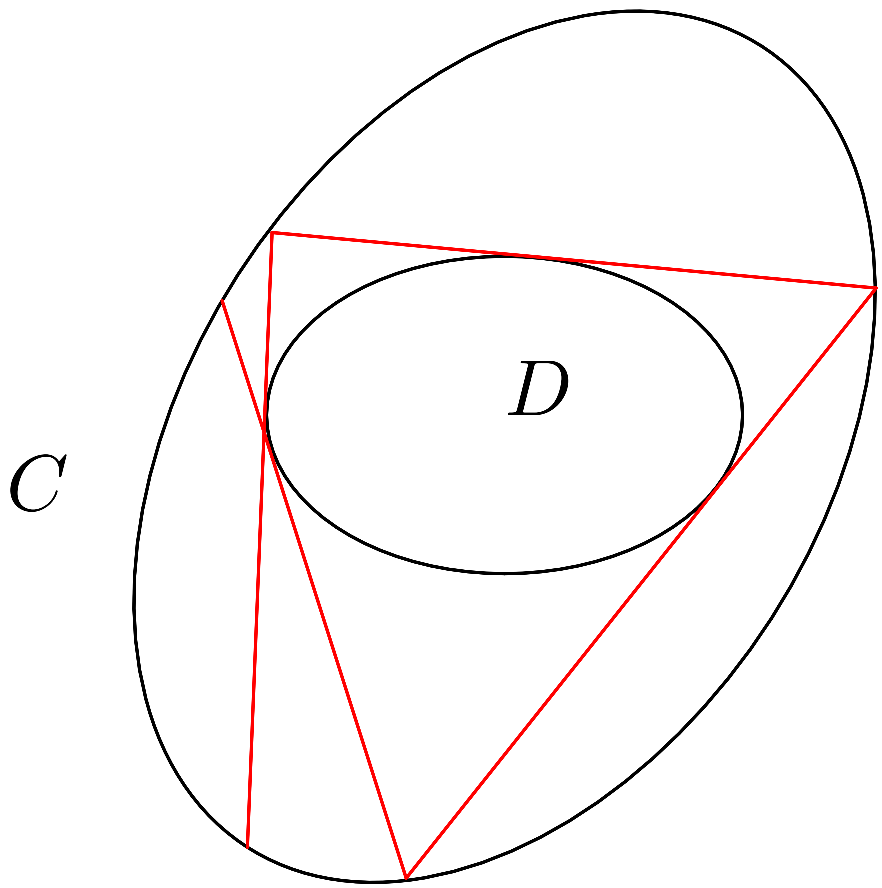
Por fim, volta a Poncelet

Mencionemos um modelo geométrico alternativo para CCE, no qual a cúbica é substituída por um par de cônicas:



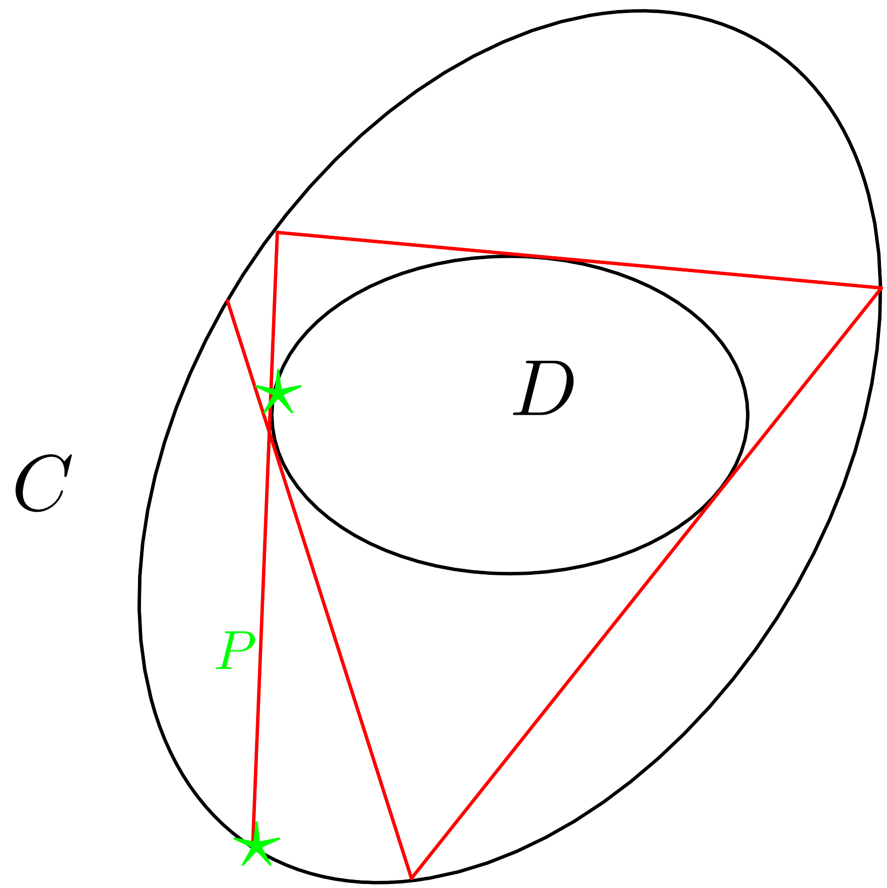
Por fim, volta a Poncelet

Mencionemos um modelo geométrico alternativo para CCE, no qual a cúbica é substituída por um par de cônicas:



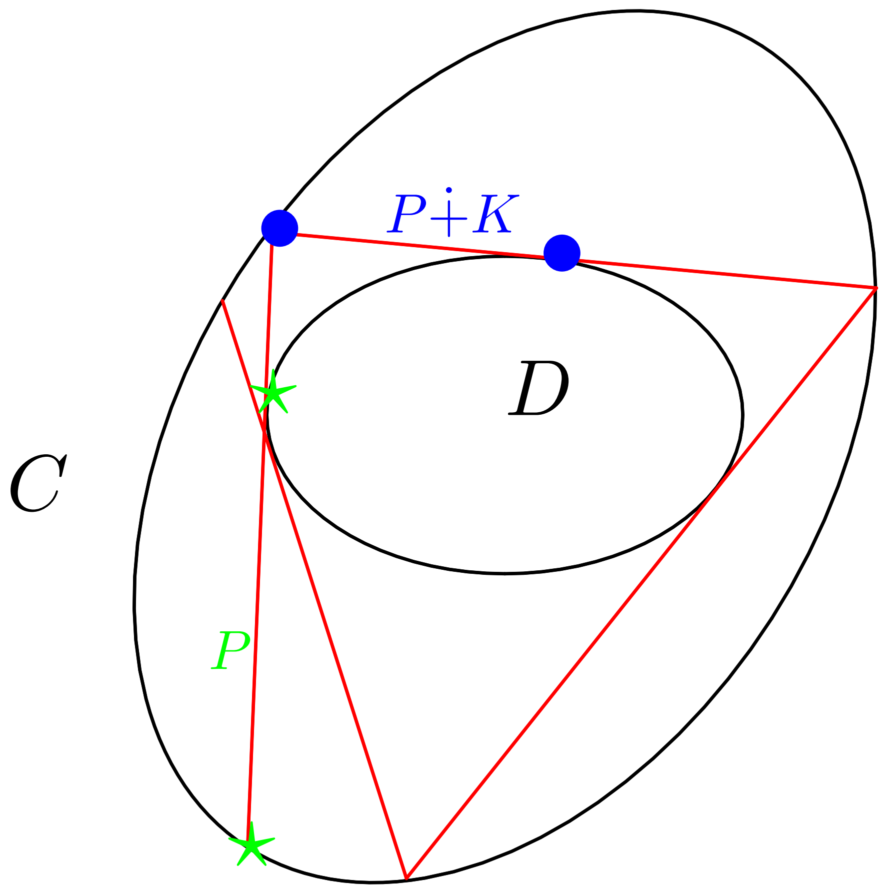
Por fim, volta a Poncelet

Mencionemos um modelo geométrico alternativo para CCE, no qual a cúbica é substituída por um par de cônicas:



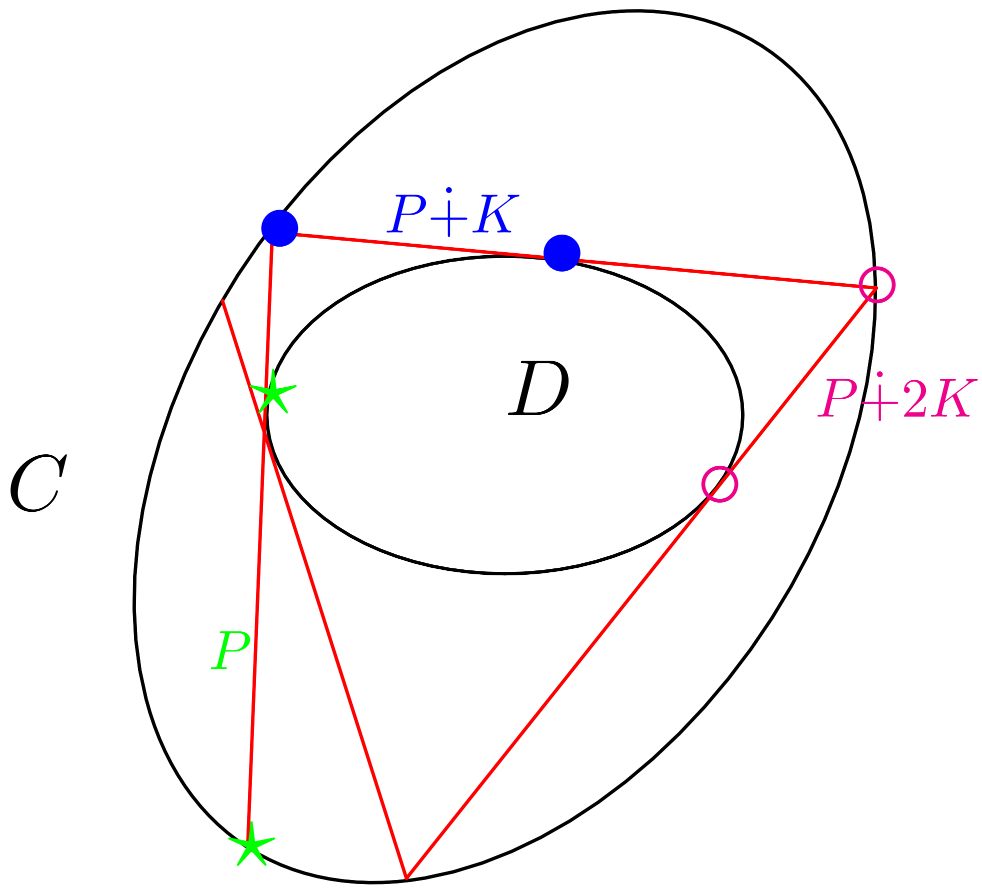
Por fim, volta a Poncelet

Mencionemos um modelo geométrico alternativo para CCE, no qual a cúbica é substituída por um par de cônicas:



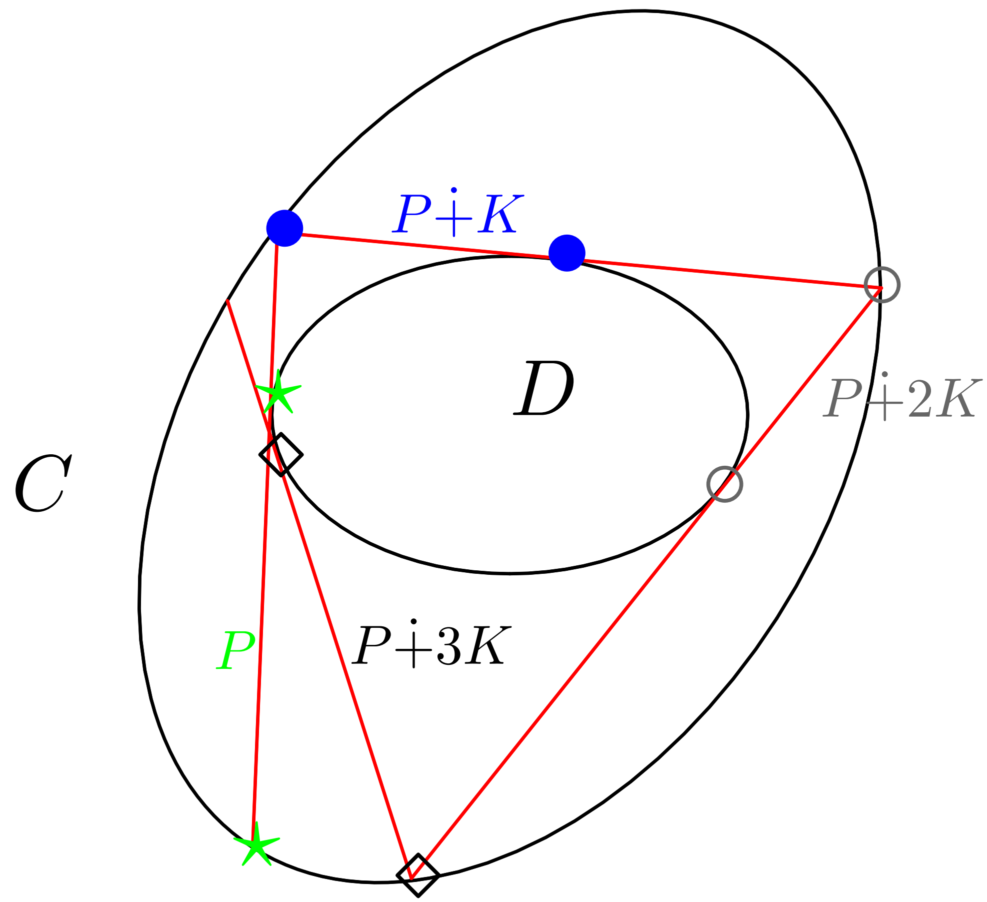
Por fim, volta a Poncelet

Mencionemos um modelo geométrico alternativo para CCE, no qual a cúbica é substituída por um par de cônicas:



Por fim, volta a Poncelet

Mencionemos um modelo geométrico alternativo para CCE, no qual a cúbica é substituída por um par de cônicas:



Na construção de Poncelet, o papel da cúbica

Na construção de Poncelet, o papel da cúbica é trocado pela coleção $\mathcal{E}$, Na construção de Poncelet, o papel da cúbica é trocado pela coleção $\mathcal{E}$, formada pelos pares (c, d) :

Na construção de Poncelet, o papel da cúbica é trocado pela coleção $\mathcal{E}$, formada pelos pares

$$(c, d) : \ \star\star, \ \bullet\bullet, \ \circ\circ, \ldots$$

Na construção de Poncelet, o papel da cúbica é trocado pela coleção $\mathcal{E}$, formada pelos pares

$$(c, d) : \ \star\star, \ \bullet\bullet, \ \circ\circ, \ldots$$

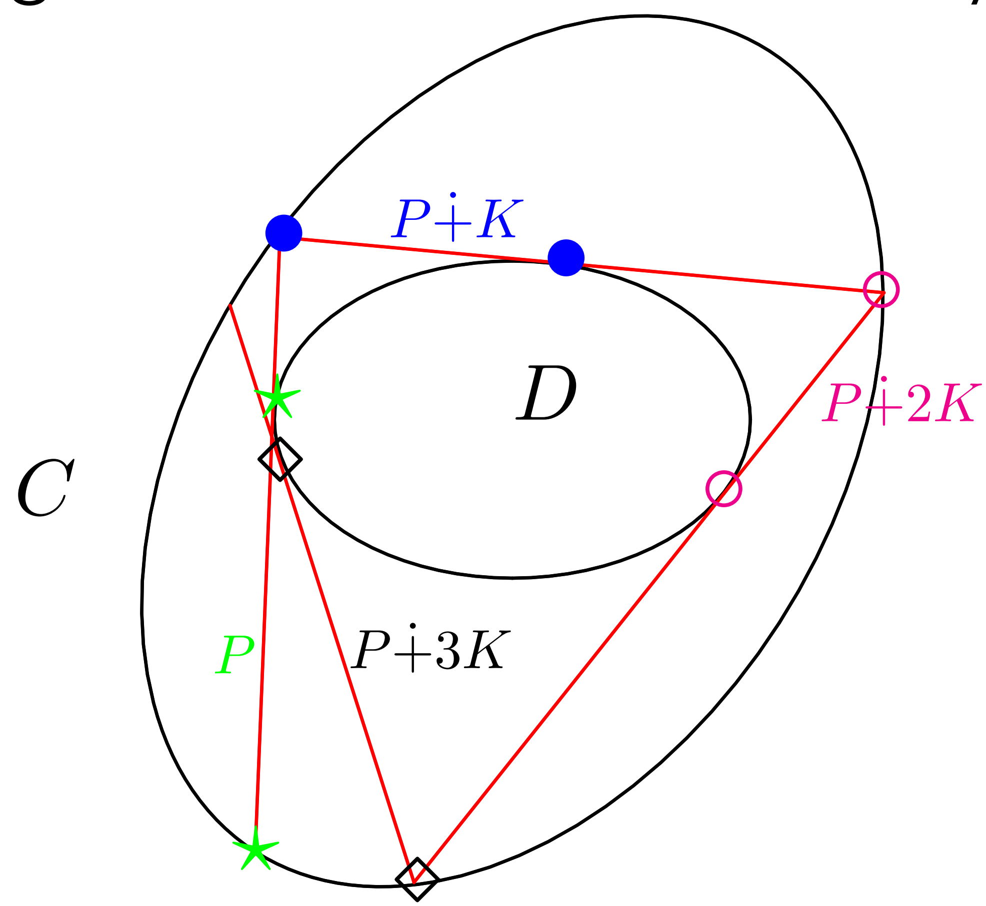
onde c percorre a cônica "externa" C,

Na construção de Poncelet, o papel da cúbica é trocado pela coleção $\mathcal{E}$, formada pelos pares

$$(c,d): \;\star\star,\; \bullet\bullet,\; \circ\circ, \ldots$$

onde c percorre a cônica "externa" C, e d denota o ponto de contato de uma tangente à cônica interna D traçada por c.

Na construção de Poncelet, o papel da cúbica é trocado pela coleção $\mathcal{E}$, formada pelos pares (c, d) : $\star\star$, $\bullet\bullet$, $\circ\circ, \ldots$ onde c percorre a cônica "externa" C, e d denota o ponto de contato de uma tangente à cônica interna D traçada por c.



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

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

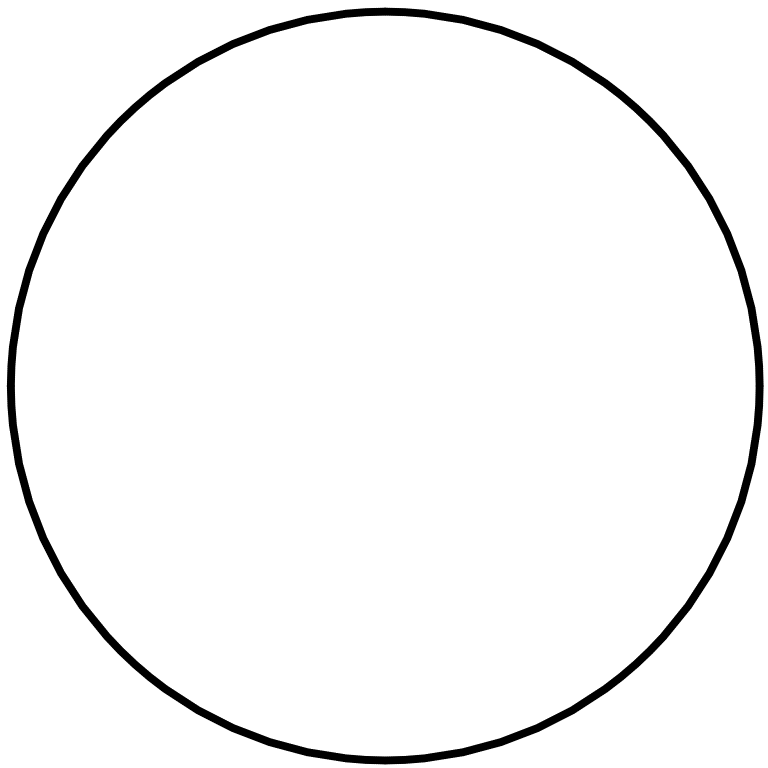
Mas se fechar em n etapas a partir de algum $c \in C$,

Para C, D cônicas "gerais", a poligonal não fecha.
Mas se fechar em n etapas a partir de algum $c \in C$, o mesmo ocorrerá para qualquer outro ponto de C!

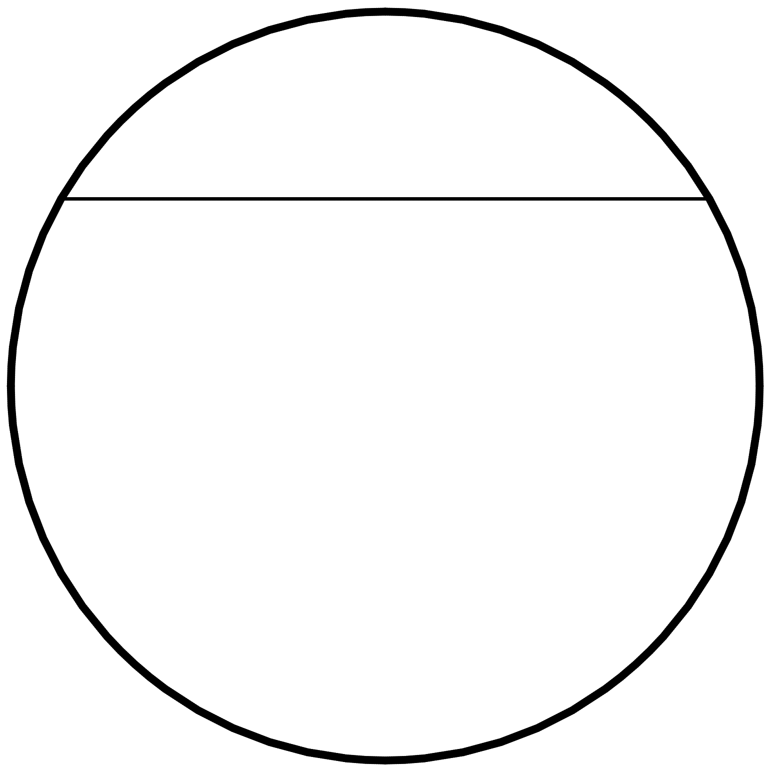
Para C, D cônicas “gerais”, a poligonal não fecha.

Mas se fechar em n etapas a partir de algum $c \in C$, o mesmo ocorrerá para qualquer outro ponto de C!

Reveja a figura do quadrilátero:



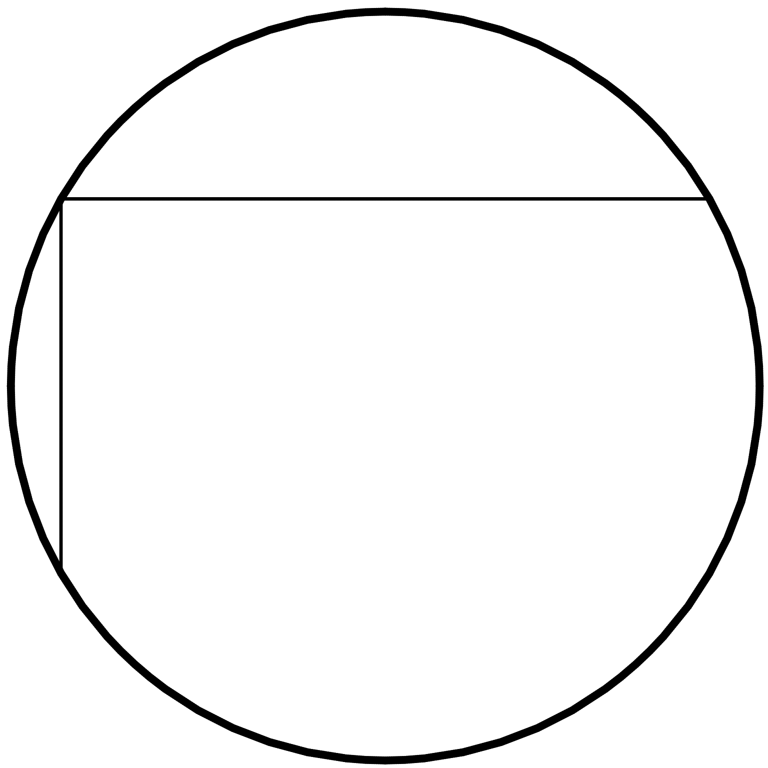
Para C, D cônicas "gerais", a poligonal não fecha.
Mas se fechar em n etapas a partir de algum $c \in C$, o mesmo ocorrerá para qualquer outro ponto de C!
Reveja a figura do quadrilátero:



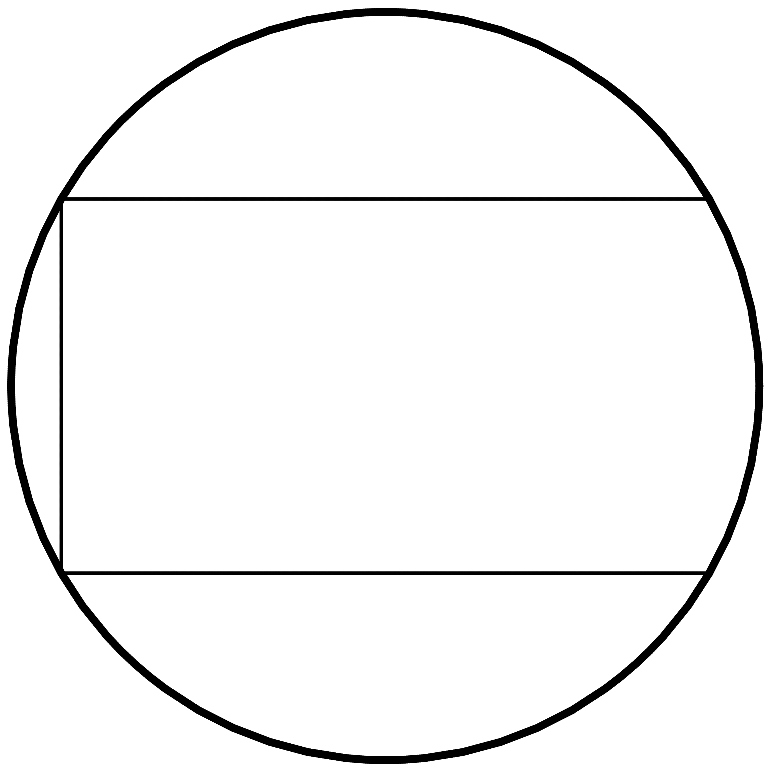
Para C, D cônicas "gerais", a poligonal não fecha.

Mas se fechar em n etapas a partir de algum $c \in C$, o mesmo ocorrerá para qualquer outro ponto de C!

Reveja a figura do quadrilátero:



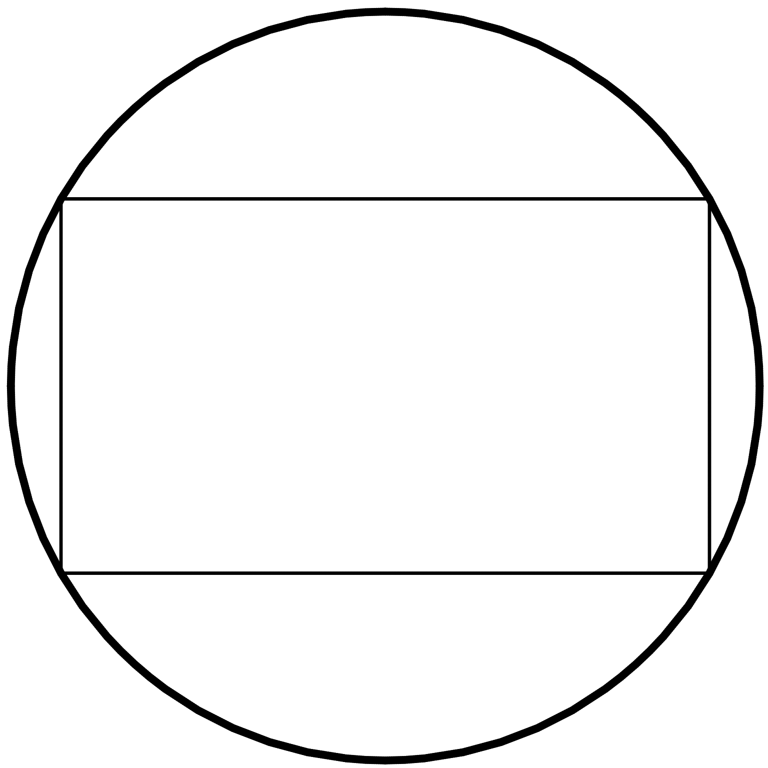
Para C, D cônicas "gerais", a poligonal não fecha.
Mas se fechar em n *etapas a partir de algum* $c \in C$*,*
o mesmo ocorrerá para qualquer outro ponto de C*!*
Reveja a figura do quadrilátero:



Para C, D cônicas “gerais”, a poligonal não fecha.

Mas se fechar em n etapas a partir de algum $c \in C$, o mesmo ocorrerá para qualquer outro ponto de C!

Reveja a figura do quadrilátero:

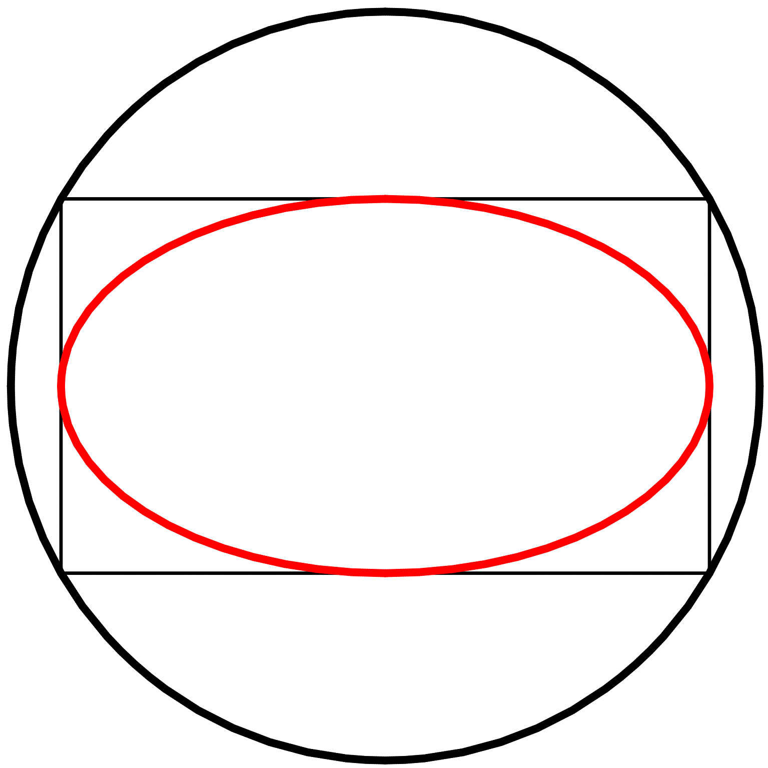


Para C, D cônicas “gerais”, a poligonal não fecha.

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

o mesmo ocorrerá para qualquer outro ponto de C*!*

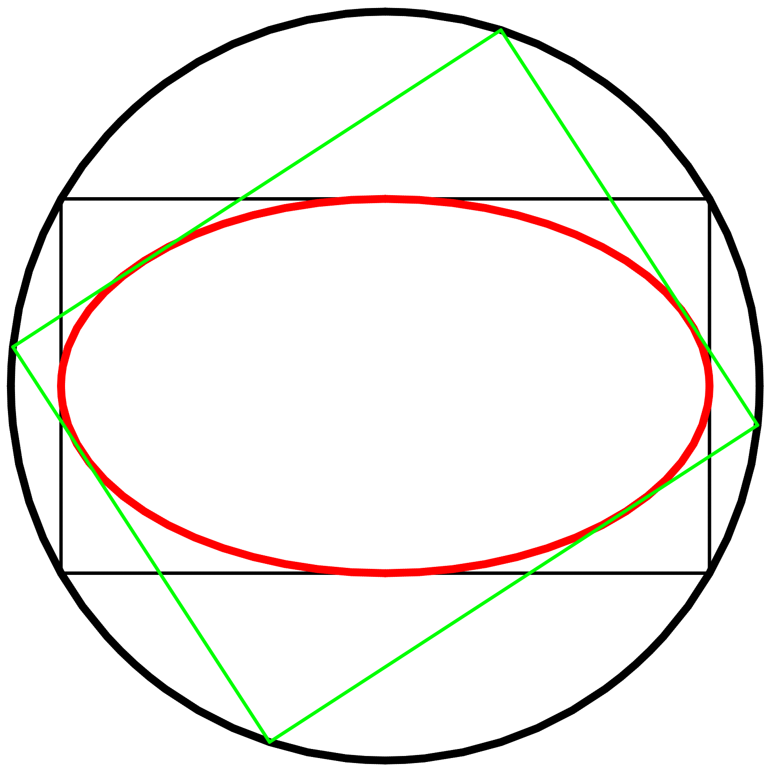
Reveja a figura do quadrilátero:



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

Mas se fechar em n etapas a partir de algum $c \in C$, o mesmo ocorrerá para qualquer outro ponto de C!

Reveja a figura do quadrilátero:



De fato, abstratamente, $\mathcal{E}$ é uma curva elíptica.

De fato, abstratamente, $\mathcal{E}$ é uma curva elíptica.
Mas agora, ao invés de curva (cúbica) plana,

De fato, abstratamente, $\mathcal{E}$ é uma curva elíptica.
Mas agora, ao invés de curva (cúbica) plana,
ela está situada na superfície $C \times D$.

De fato, abstratamente, $\mathcal{E}$ é uma curva elíptica. Mas agora, ao invés de curva (cúbica) plana, ela está situada na superfície $C \times D$.

O movimento do “jogo de bilhar” corresponde novamente à adição na lei de grupo.

De fato, abstratamente, $\mathcal{E}$ é uma curva elíptica.
Mas agora, ao invés de curva (cúbica) plana,
ela está situada na superfície $C \times D$.

O movimento do "jogo de bilhar" corresponde
novamente à adição na lei de grupo.
A vantagem é que, na versão do bilhar de Poncelet,

De fato, abstratamente, $\mathcal{E}$ é uma curva elíptica.
Mas agora, ao invés de curva (cúbica) plana,
ela está situada na superfície $C \times D$.

O movimento do "jogo de bilhar" corresponde
novamente à adição na lei de grupo.
A vantagem é que, na versão do bilhar de Poncelet,
o ponto K usado para embaralhar é imediatamente
calculável a partir da configuração C, D.

cinco pontos ainda é de graça

cinco pontos ainda é de graça

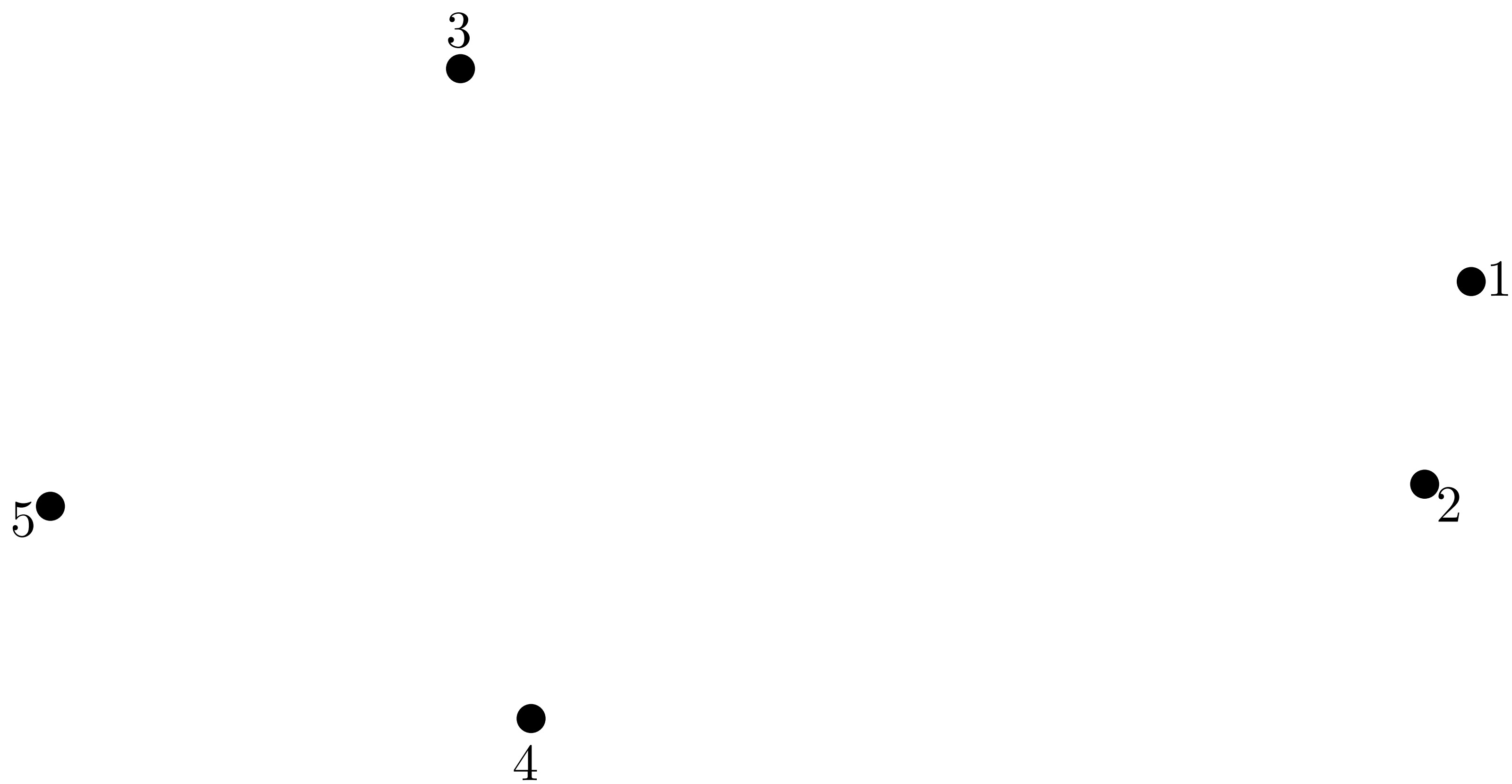
●1

cinco pontos ainda é de graça

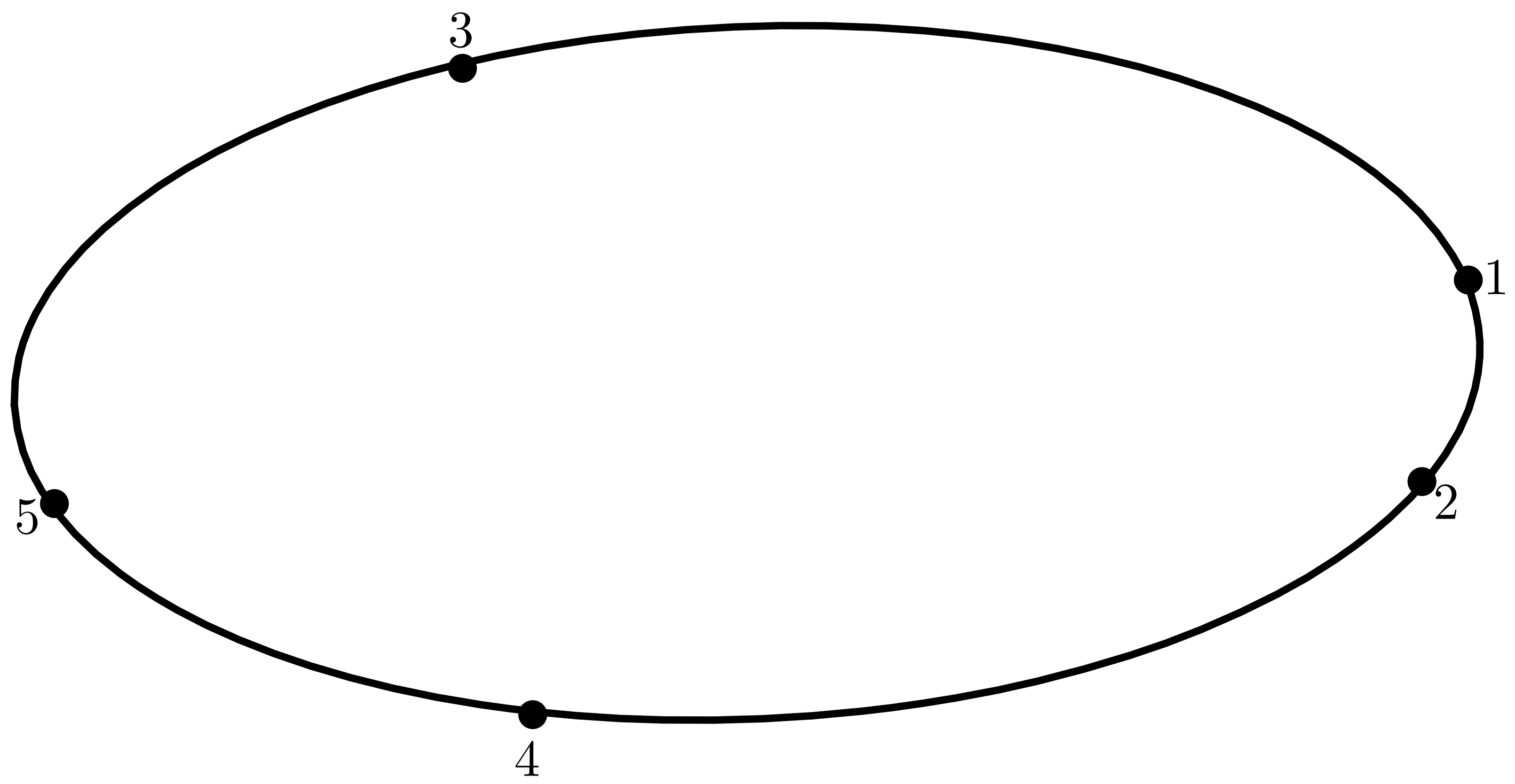
cinco pontos ainda é de graça

cinco pontos ainda é de graça

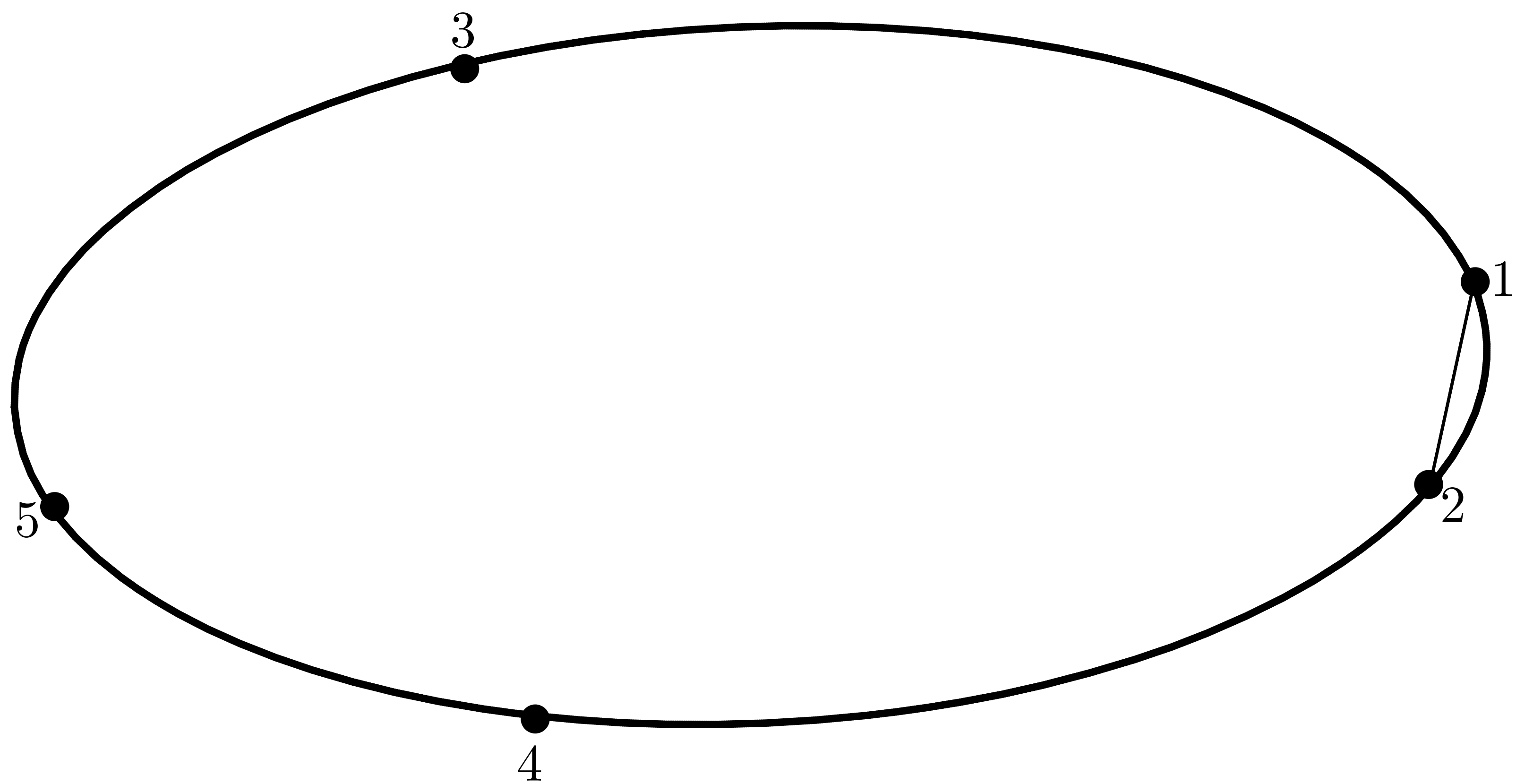
cinco pontos ainda é de graça



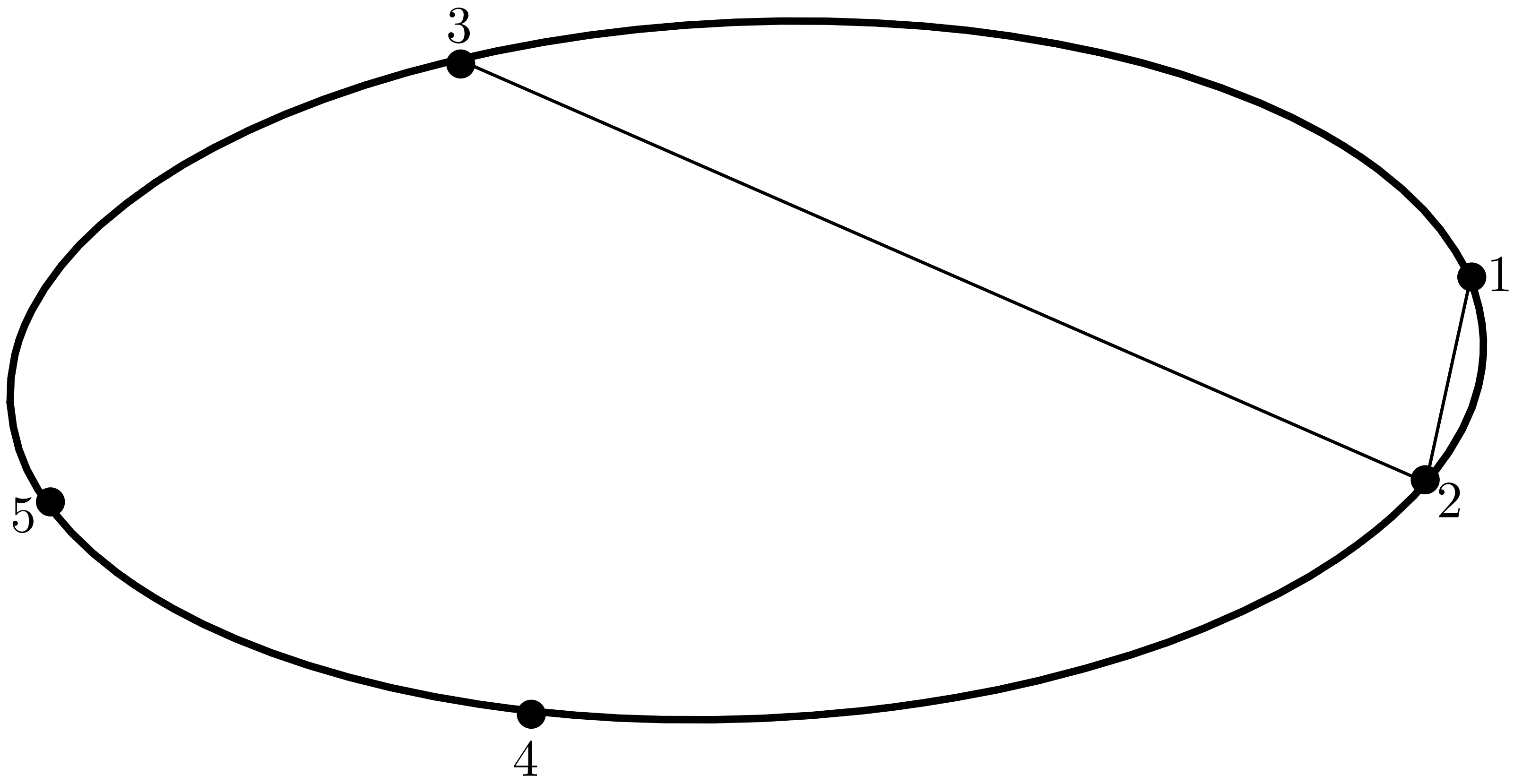
cinco pontos ainda é de graça



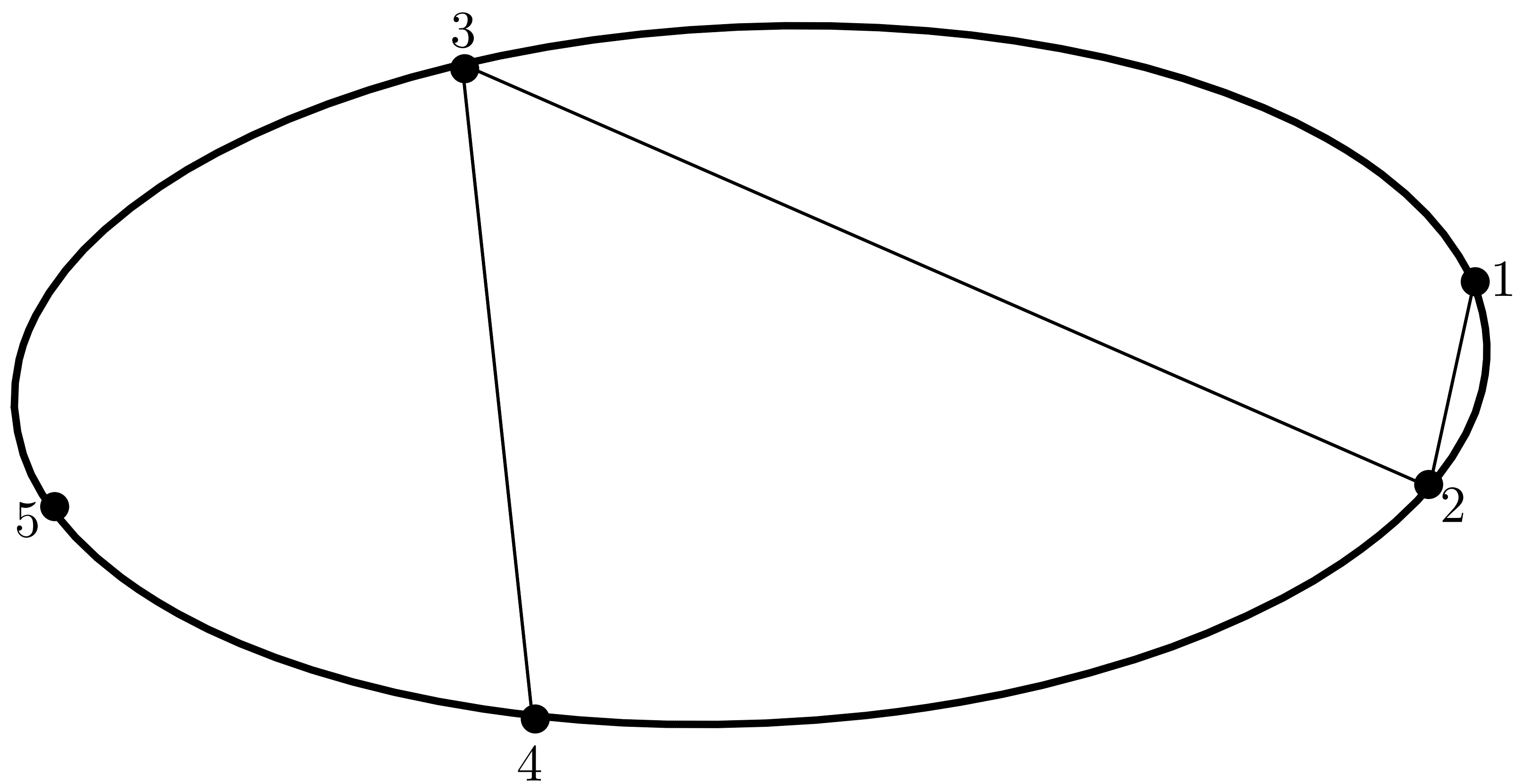
cinco pontos ainda é de graça



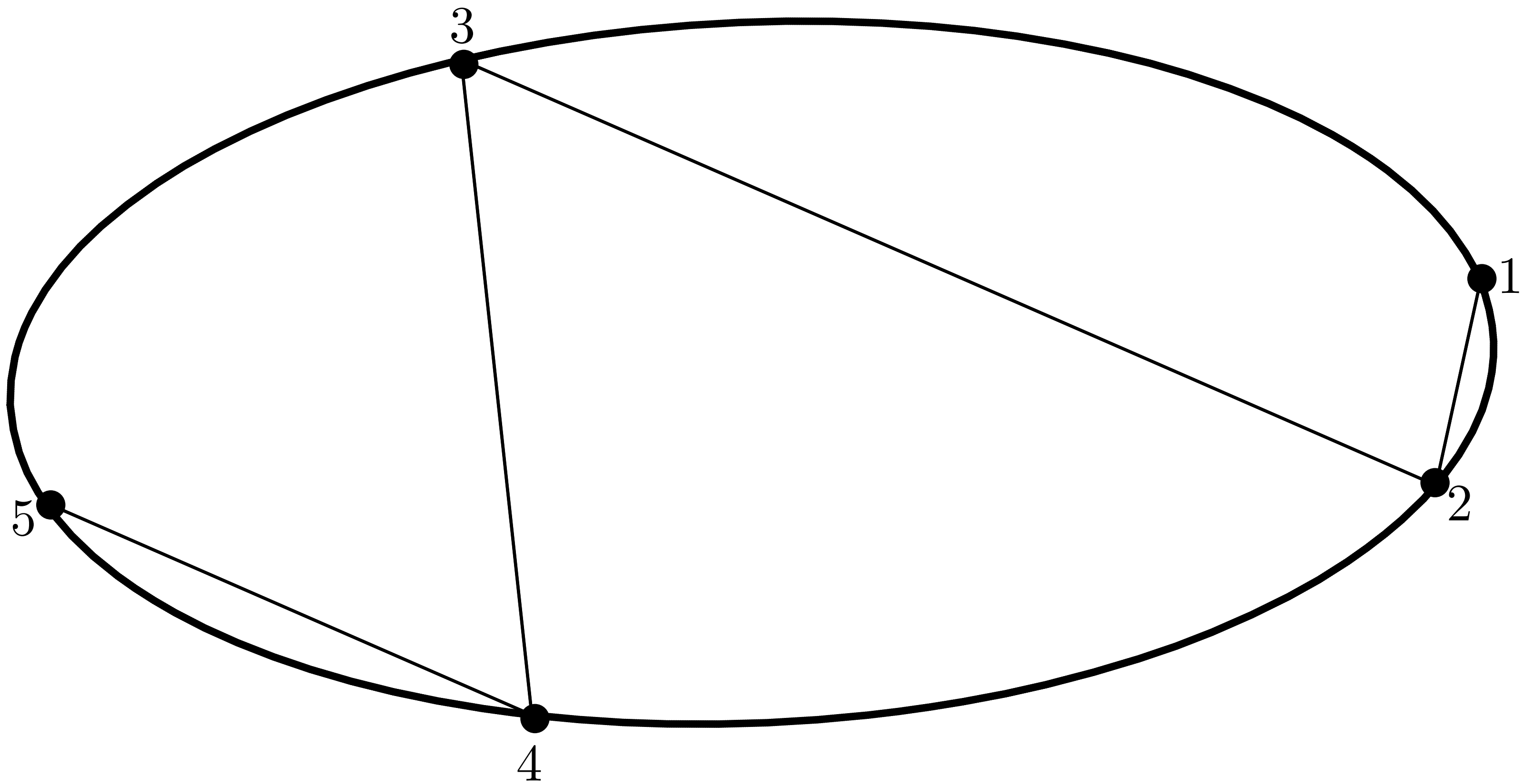
cinco pontos ainda é de graça



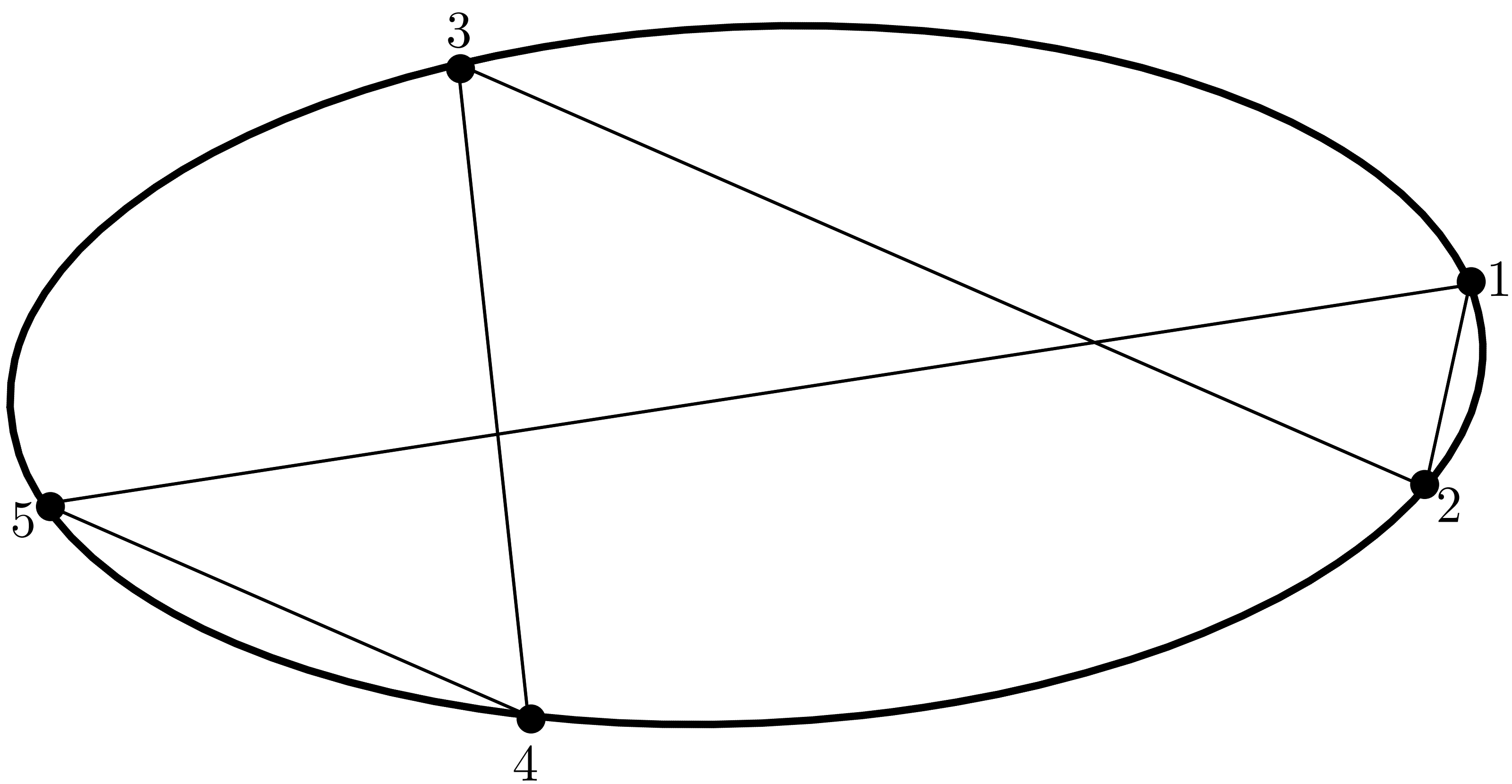
cinco pontos ainda é de graça



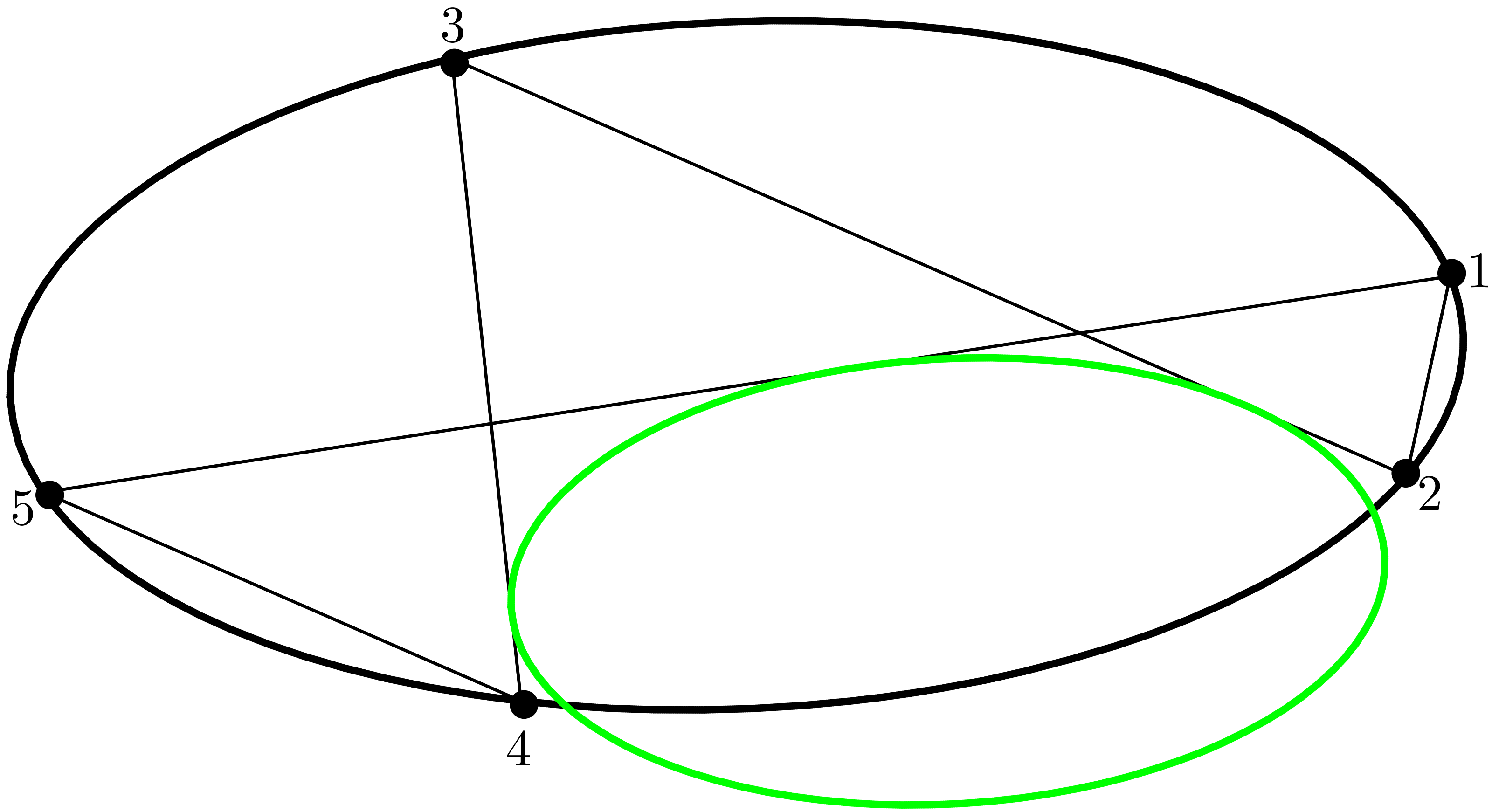
cinco pontos ainda é de graça



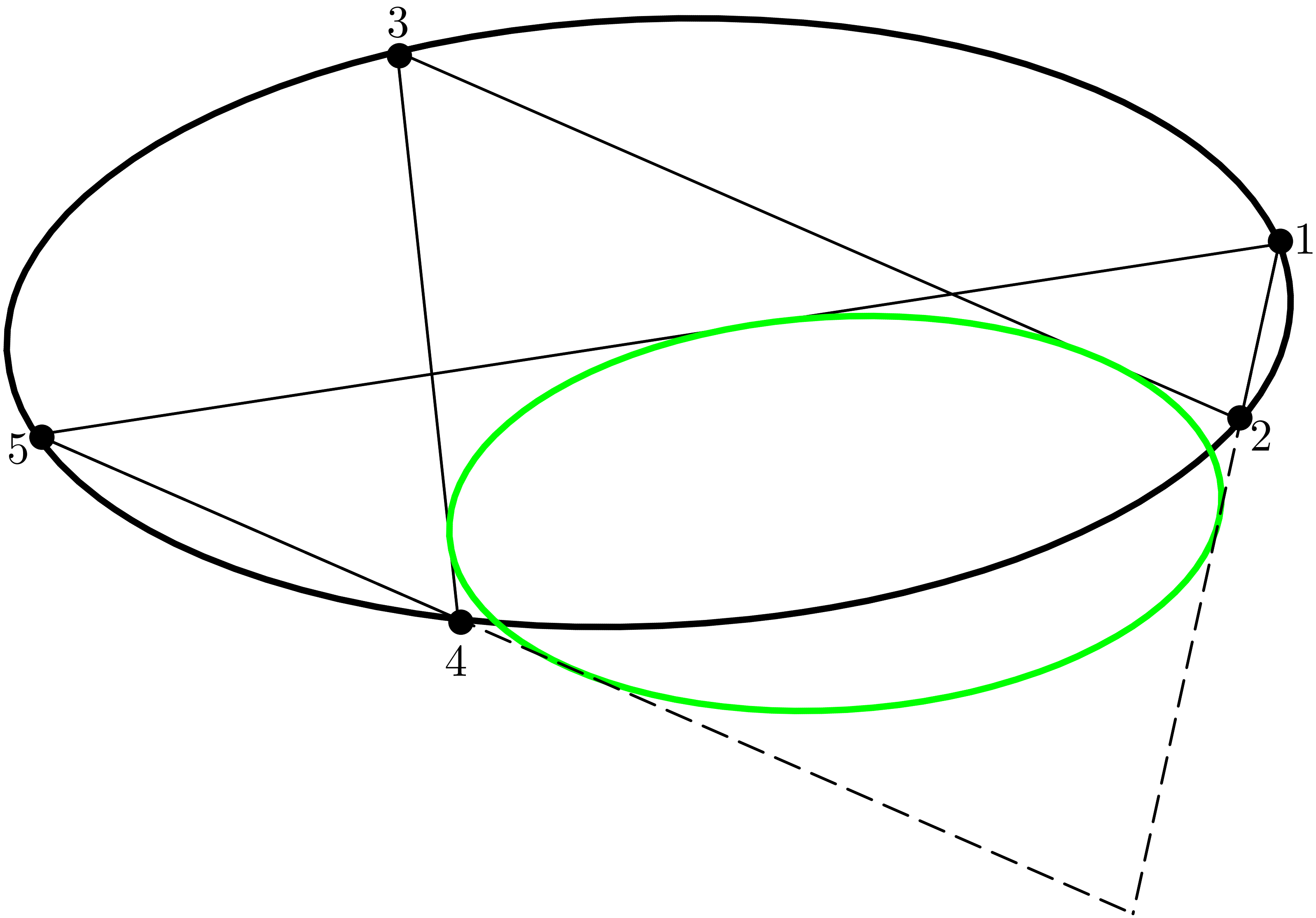
cinco pontos ainda é de graça



cinco pontos ainda é de graça



cinco pontos ainda é de graça



Em particular, tomando coordenadas sobre um corpo finito,

Em particular, tomando coordenadas sobre um corpo finito, sempre fecha.

Em particular, tomando coordenadas sobre um corpo finito, sempre fecha.

Fica a pergunta de como proceder para

Em particular, tomando coordenadas sobre um corpo finito, sempre fecha.

Fica a pergunta de
como proceder para
produzir eficientemente

Em particular, tomando coordenadas sobre um corpo finito, sempre fecha.

Fica a pergunta de
como proceder para
produzir eficientemente
pares de cônicas C_n, D_n
definidas sobre um corpo finito

Em particular, tomando coordenadas sobre um corpo finito, sempre fecha.

Fica a pergunta de

como proceder para

produzir eficientemente

pares de cônicas C_n, D_n

definidas sobre um corpo finito

e munidas de

n*–ágono inscrito/circunscrito*

com $n >> 0 \ldots$

referências

I. Blake, G. Seroussi & Nigel Smart, *Elliptic Curves in Cryptography*, Cambridge University Press (1999) (todos da HP);

N. Koblitz, *a Course in Number Theory and Cryptography*, Springer-Verlag, 1987.

S. Collier Coutinho, *Números inteiros e criptografia RSA*, (segunda edição) Série de Computação e Matemática (IMPA), Rio de Janeiro; Sociedade Brasileira de Matemática, Rio de Janeiro, 2000.