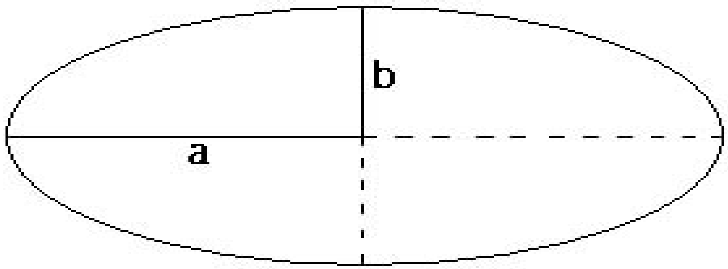
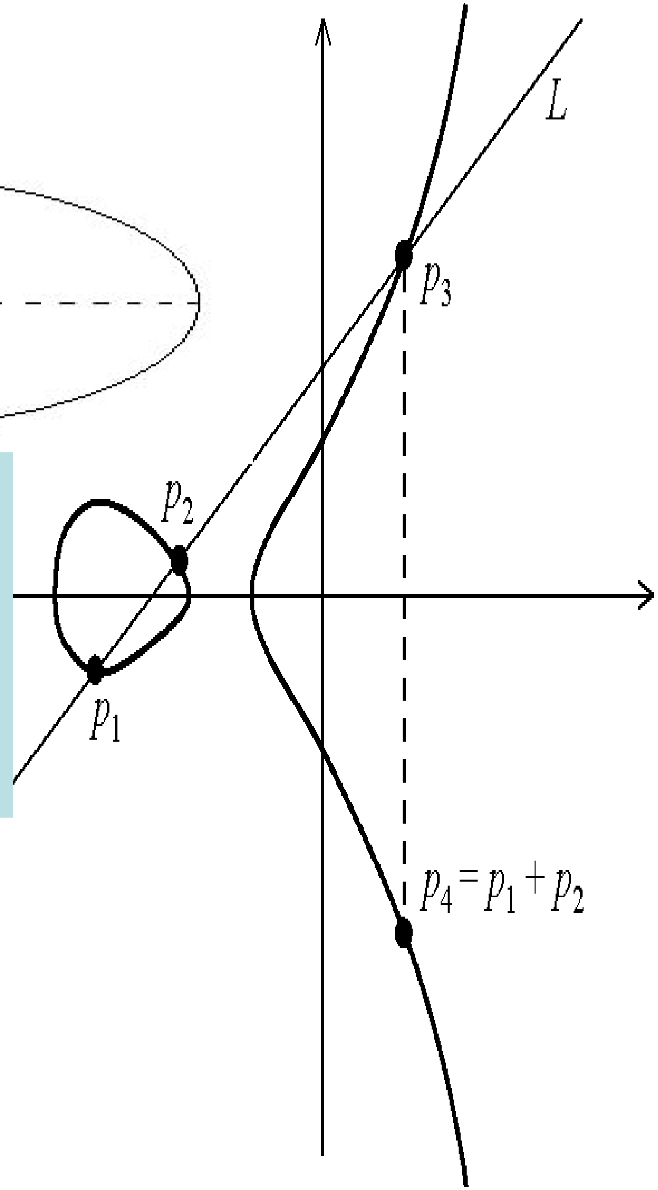
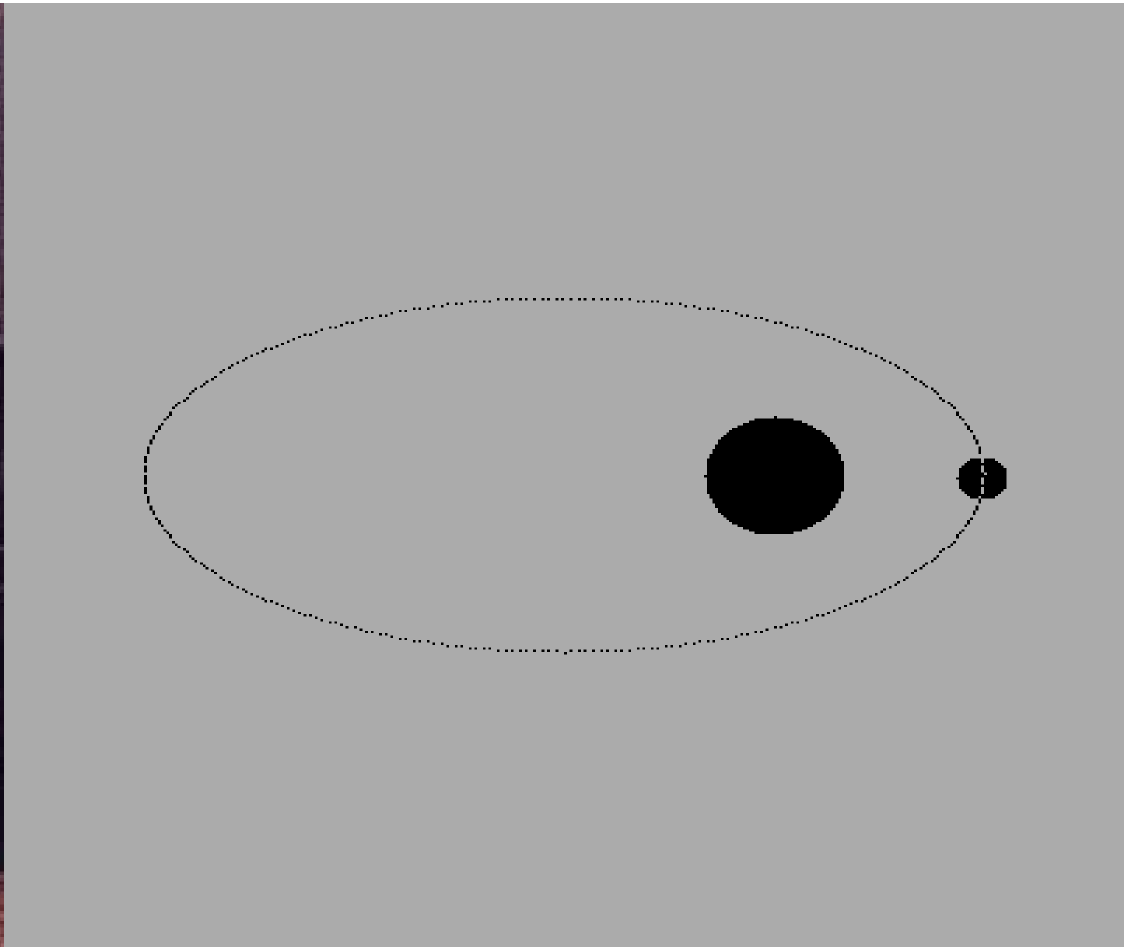


ELLIPSES
AND
ELLIPTIC CURVES

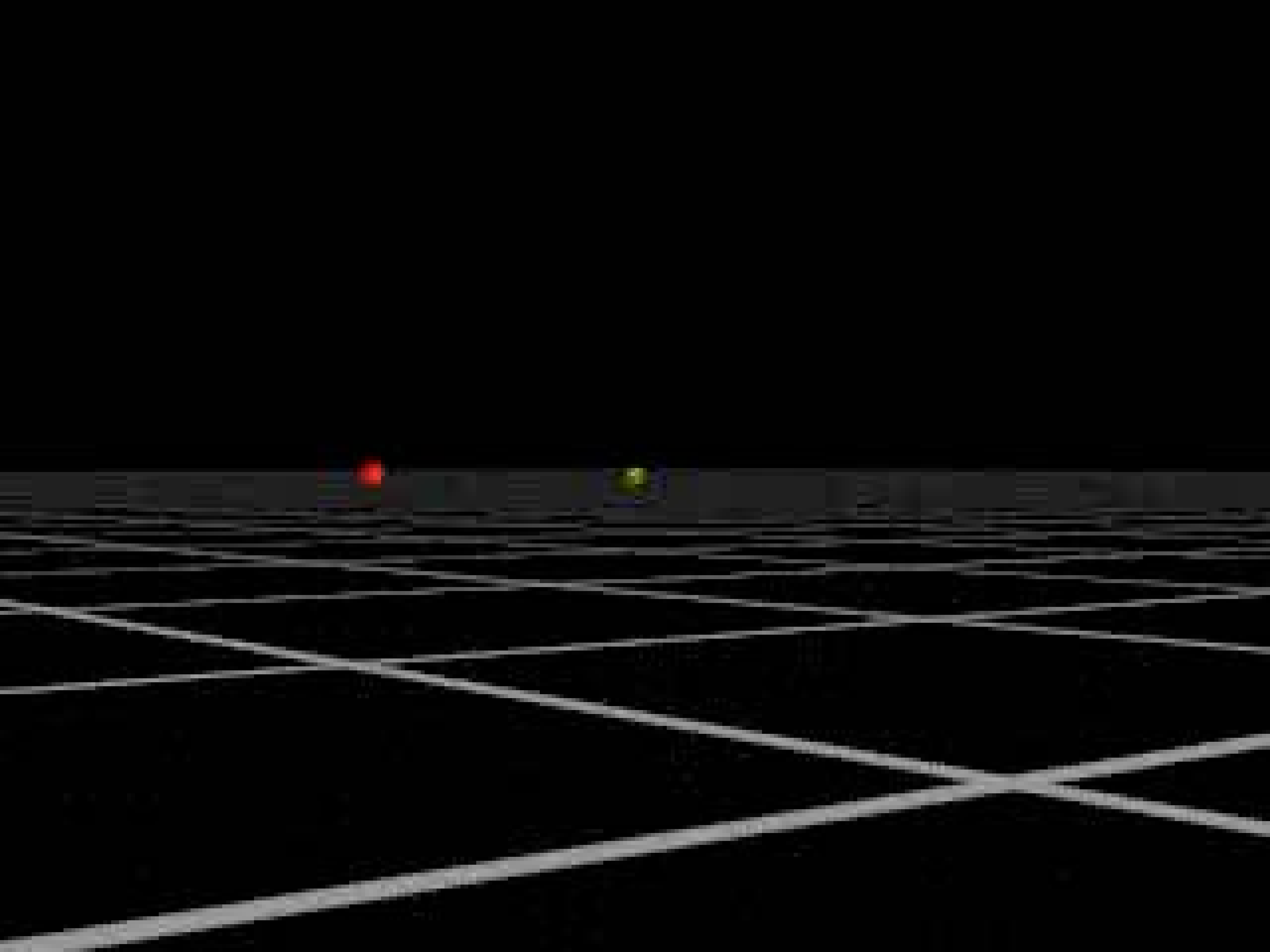
M. Ram Murty
Queen's University



Planetary orbits are elliptical

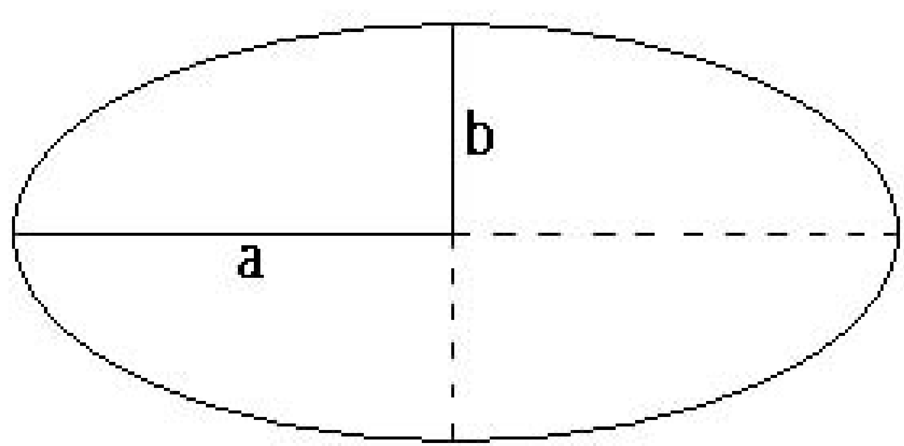


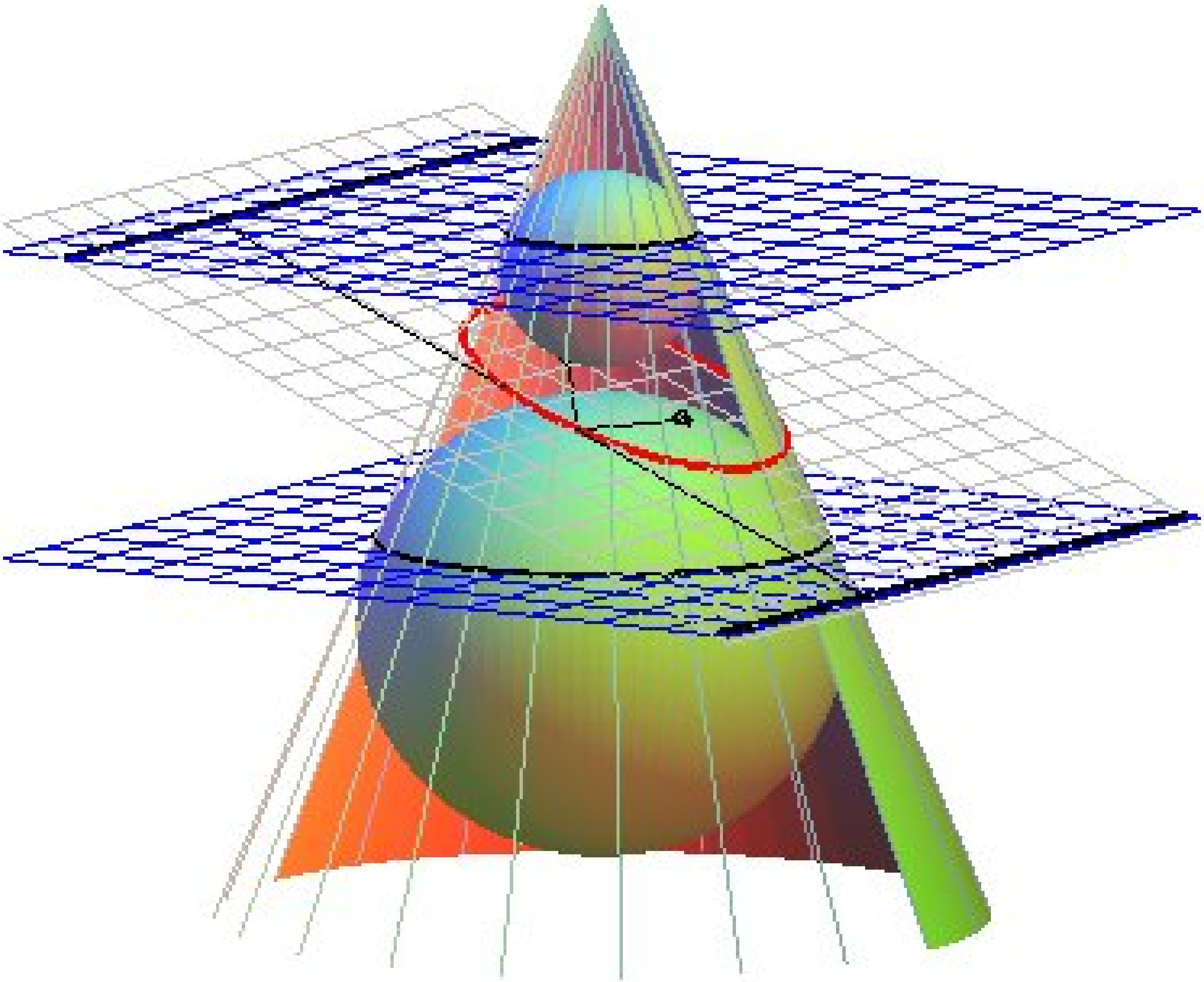
Johannes Kepler



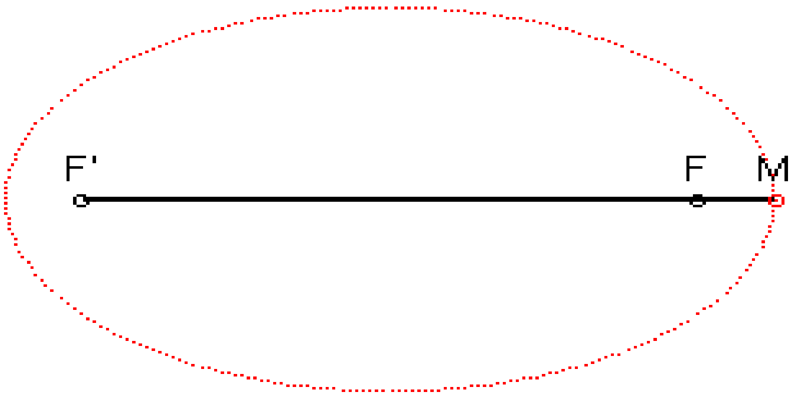
What is an ellipse?

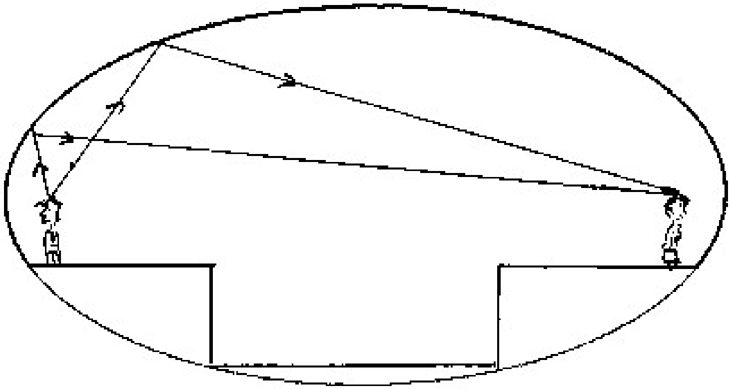
$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$



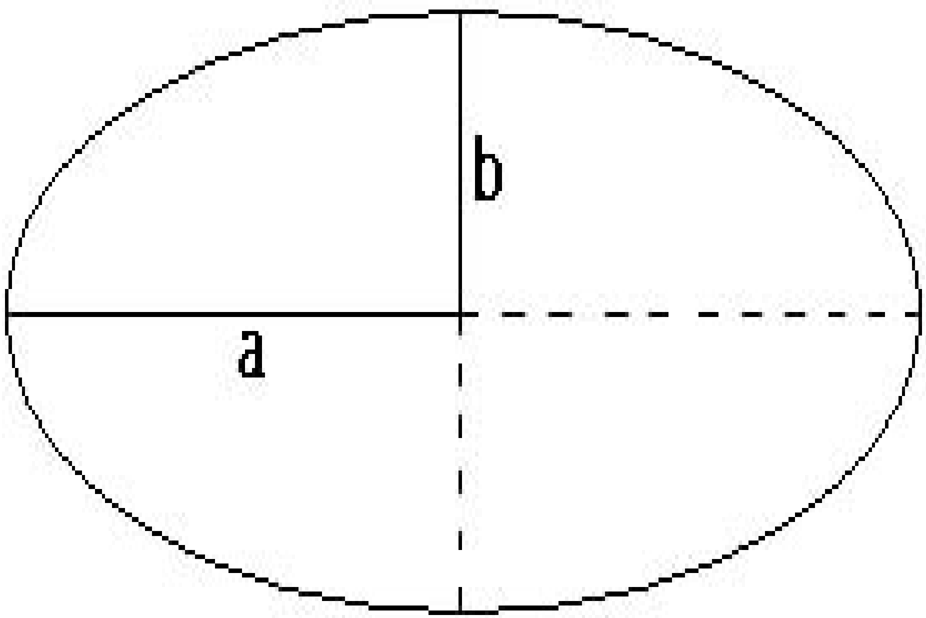


An ellipse has two foci





From: gomath.com/geometry/ellipse.php



Area and Perimeter of Ellipse

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

$$\text{Perimeter} = 2\pi\sqrt{\frac{a^2 + b^2}{2}}$$

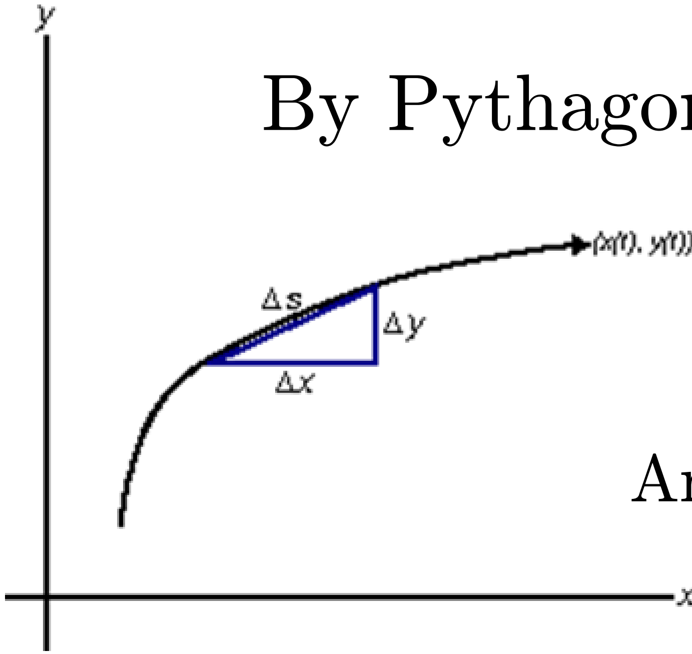
$$\text{Area} = \pi ab$$

Metric mishap causes loss of Mars orbiter (Sept. 30, 1999)

(NASA)

How to calculate arc length

Let $f:[0,1]\to\mathbb{R}^2$ be given by $t\mapsto(x(t),y(t))$.



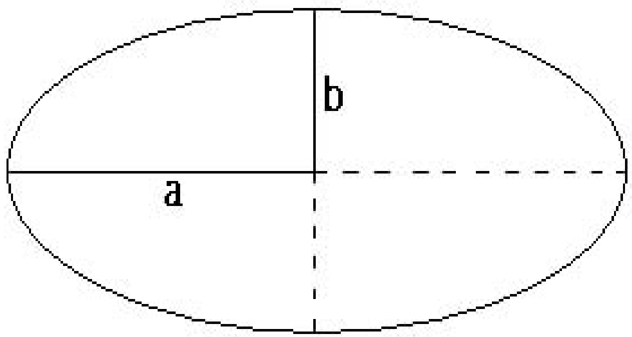
By Pythagoras, $\Delta s=\sqrt{(\Delta x)^2+(\Delta y)^2}$

$$ds=\sqrt{\left(\frac{dx}{dt}\right)^2+\left(\frac{dy}{dt}\right)^2}dt$$

$$\text{Arc length}=\int_0^1\sqrt{\left(\frac{dx}{dt}\right)^2+\left(\frac{dy}{dt}\right)^2}dt$$

Circumference of an ellipse

We can parametrize the points of an ellipse in the first quadrant by $f : [0, \pi/2] \to (a \sin t, b \cos t)$.



Circumference =
$$4 \int_0^{\pi/2} \sqrt{a^2 \cos^2 t + b^2 \sin^2 t}\, dt.$$

Observe that if $a = b$, we get $2\pi a$.

We can simplify this as follows.
Let $\cos^2\theta = 1 - \sin^2\theta$.
The integral becomes
$4a\int_0^{\pi/2}\sqrt{1-\lambda\sin^2\theta}\,d\theta$
Where $\lambda = 1-\mathrm{b}^2/a^2$.

We can expand the square root using the binomial theorem:
$4a\int_0^{\pi/2}\sum_{n=0}^{\infty}\binom{1/2}{n}(-1)^n\lambda^n\sin^{2n}\theta\,d\theta$.

We can use the fact that
$2\int_0^{\pi/2}\sin^{2n}\theta\,d\theta = \pi\frac{(1/2)(1/2)+1)\cdots((1/2)+(n-1))}{n!}$

The final answer

The circumference is given by
$2\pi a F(1/2, -1/2, 1; \lambda)$
where
$F(a, b, c; z) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{n!(c)_n} z^n$
is the hypergeometric series and
$(a)_n = a(a+1)(a+2)\cdots(a+n-1)$.

We now use Landens transformation:
$F(a, b, 2b; \frac{4x}{(1+x)^2}) = (1+x)^{2a} F(a, a-b+1/2, b+1/2; x^2)$.

We put $a = -1/2, b = 1/2$ and $x = (a-b)/(a+b)$.

The answer can now be written as $\pi(a+b)F(-1/2, -1/2, 1; x^2)$.

Approximations

- In 1609, Kepler used the approximation $\pi(a+b)$. The above formula shows the perimeter is always greater than this amount.
- In 1773, Euler gave the approximation $2\pi\sqrt{(a^2+b^2)/2}$.
- In 1914, Ramanujan gave the approximation $\pi(3(a+b) - \sqrt{(a+3b)(3a+b)})$.

What kind of number is this?

For example, if a and b are rational,
is the circumeference irrational?

In case $a = b$ we have a circle
and the circumference $2\pi a$
is irrational.

In fact, π is transcendental.

What does this mean?

This means that π does not satisfy an equation of the type
$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$
with a_i rational numbers.

In 1882, Ferdinand von Lindemann proved that π is transcendental.

1852-1939

This means that you can't square the circle!

- There is an ancient problem of constructing a square with straightedge and compass whose area equals π.
- Theorem: if you can construct a line segment of length α then α is an algebraic number.
- Since π is not algebraic, neither is $\sqrt{\pi}$.

Some other interesting numbers

- The number e is transcendental.
- This was first proved by Charles Hermite (1822-1901) in 1873.

Is $\pi + e$ transcendental?

Answer: unknown.

Is πe transcendental?

Answer: unknown.

Not both can be algebraic!

- Here's a proof.
- If both are algebraic, then

$(x-e)(x-\pi) = x^2 - (e+\pi)x + \pi e$
is a quadratic polynomial with algebraic coefficients.
This implies both e and π are algebraic,
a contradiction to the theorems of
Hermite and Lindemann.

Conjecture:
π and e are algebraically independent.

But what about the case of the ellipse?

Is the integral
$\int_0^{\pi/2} \sqrt{a^2 \cos^2 t + b^2 \sin^2 t} dt$
transcendental
if a and b are rational?

Yes.
This is a theorem of
Theodor Schneider (1911-1988)

Lets look at the integral again.

Putting $u = \sin t$ the integral becomes

$$\int_0^1 \sqrt{\frac{a^2-(a^2-b^2)u^2}{1-u^2}}du.$$

Set $k^2 = 1 - b^2/a^2$:

The integral becomes

$$a\int_0^1 \sqrt{\frac{1-k^2u^2}{1-u^2}}du.$$

Put $t = 1 - k^2u^2$:

$$\frac{1}{2}\int_{1-k^2}^1 \frac{t\,dt}{\sqrt{t(t-1)(t-(1-k^2))}}$$

Elliptic Integrals

Integrals of the form

$$\int \frac{dx}{\sqrt{x^3+a_2x^2+a_3x+a_4}}$$

are called elliptic integrals of the first kind.

Integrals of the form

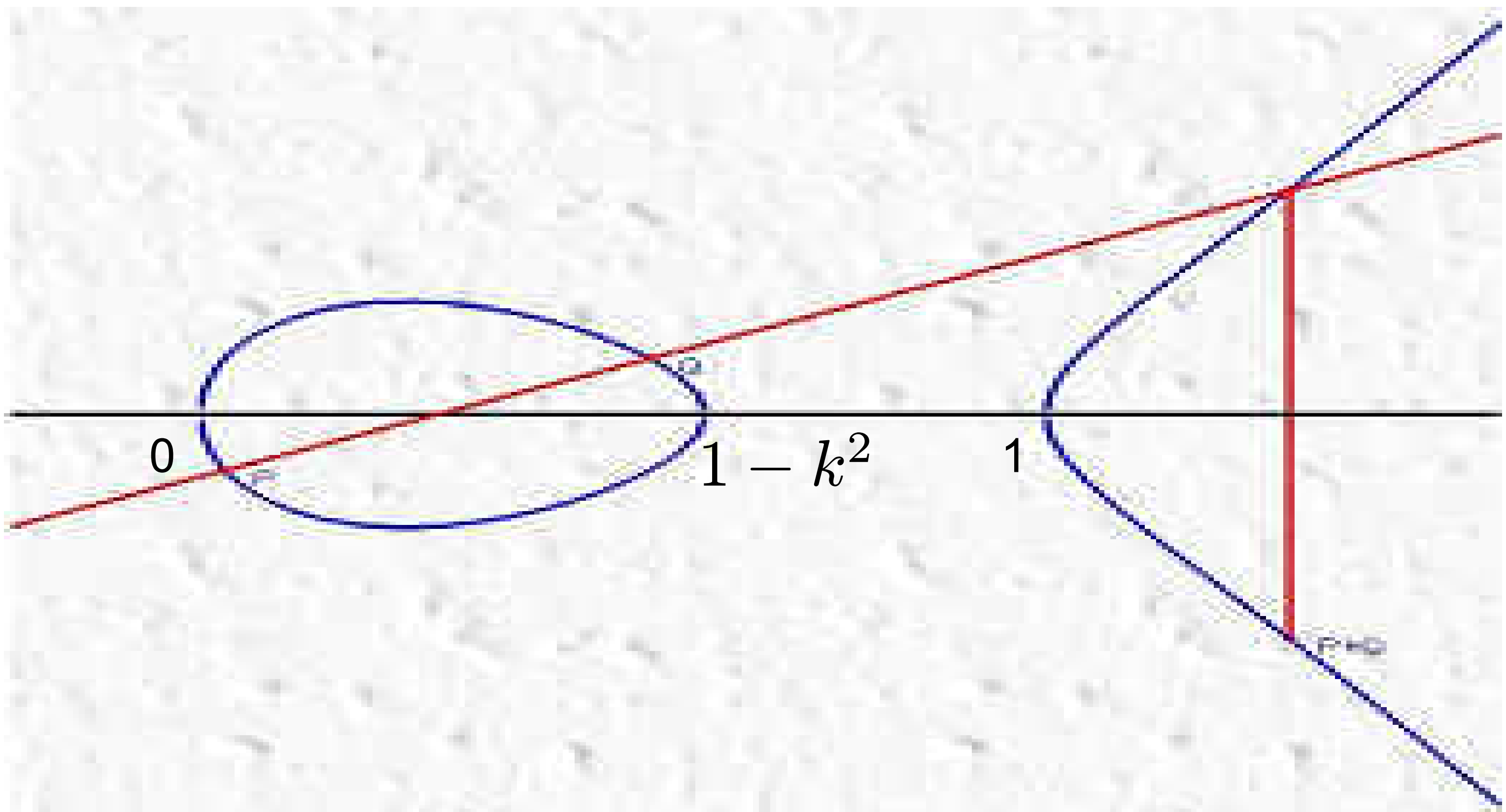
$$\int \frac{x\,dx}{\sqrt{x^3+a_2x^2+a_3x+a_4}}$$

are called elliptic integrals of the second kind.

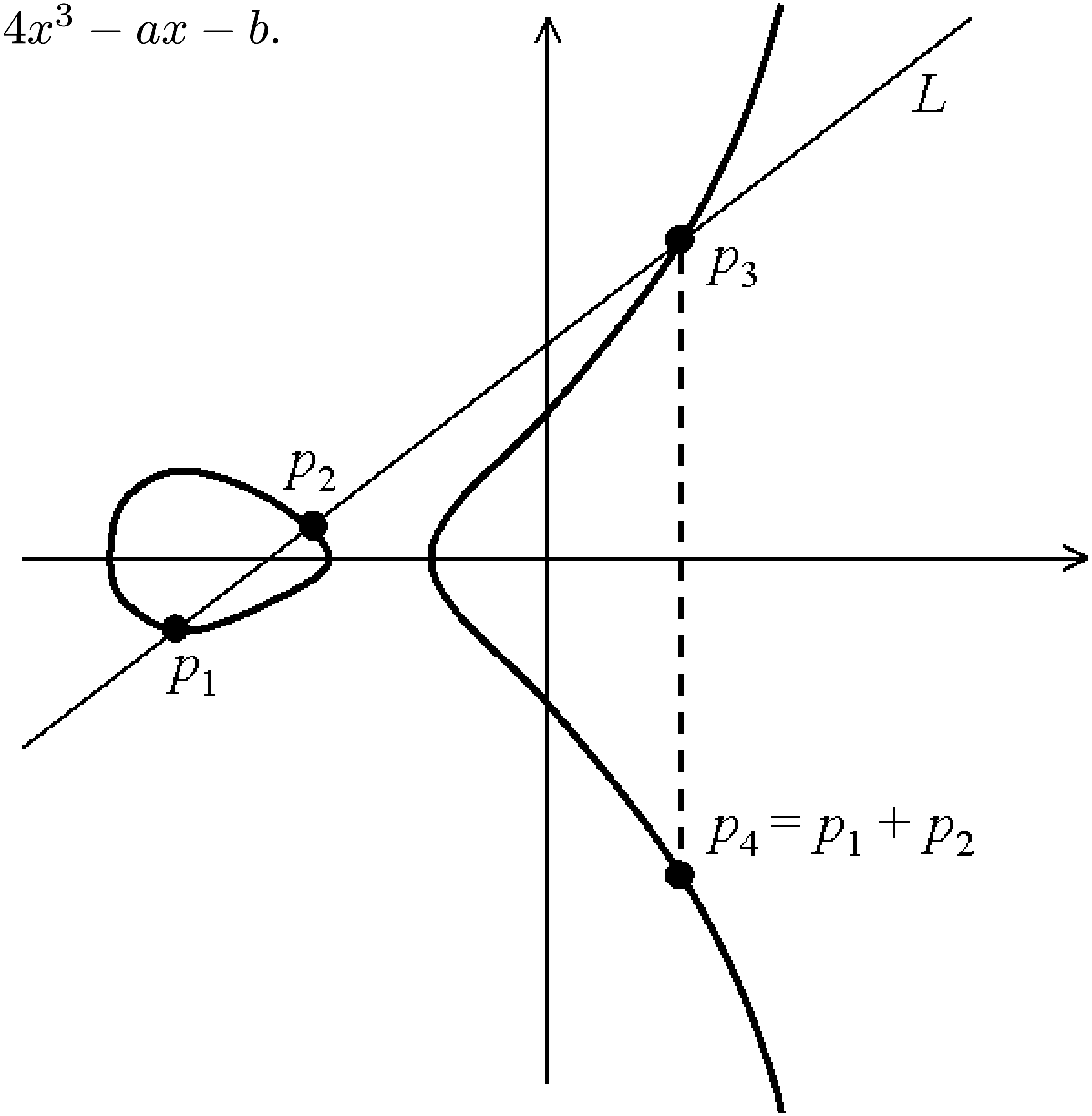
Our integral is of the second kind.

Elliptic Curves

The equation $$y^2 = x(x-1)(x-(1-k^2))$$ is an example of an elliptic curve.



One can write the equation of such a curve as
$y^2 = 4x^3 - ax - b.$



Elliptic Curves over $\mathbb{C}$

Let L be a lattice of rank 2 over $\mathbb{R}$.

This means that $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$

We attach the Weierstrass $\wp$-function to L:

$$\wp(z) = \frac{1}{z^2} + \sum_{0 \neq \omega \in L} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

The $\wp$ function is doubly periodic:

This means

$\wp(z) = \wp(z + \omega_1) = \wp(z + \omega_2)$.

$$e^{2\pi i} = 1$$

The exponential function is periodic since $e^z = e^{z+2\pi i}$.

The periods of the exponential function consist of multiples of $2\pi i$.

That is, the period "lattice" is of the form $\mathbb{Z}(2\pi i)$.

The Weierstrass function

The $\wp$-function satisfies
the following differential equation:

$$(\wp'(z))^2 = \quad 4\wp(z)^3 - g_2\wp(z) - g_3,$$

where

$$g_2 = 60\sum_{0\neq\omega\in L}\omega^{-4}$$

and

$$g_3 = 140\sum_{0\neq\omega\in L}\omega^{-6}.$$

This means that $(\wp(z), \wp'(z))$
is a point on the curve
$y^2 = 4x^3 - g_2x - g_3$.

The Uniformization Theorem

Conversely, every complex point on the curve
$y^2 = 4x^3 - g_2 x - g_3$
is of the form $(\wp(z), \wp'(z))$
for some $z \in \mathbb{C}$.

Given any $g_2, g_3 \in \mathbb{C}$,
there is a $\wp$ function such that
$(\wp'(z))^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$.

Even and Odd Functions

Recall that a function f is even if $f(z) = f(-z)$.
For example, z^2 and $\cos z$ are even functions.

A function is called odd if $f(z) = -f(-z)$.
For example, z and $\sin z$ are odd functions.

$\wp(z)$ is even since $\wp(z) = \frac{1}{z^2} + \sum_{0\neq\omega\in L}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$

$\wp'(z)$ is odd since $\wp'(z) = -\frac{2}{z^3} - 2\sum_{0\neq\omega\in L}\left(\frac{1}{(z-\omega)^3}\right).$

Note that $\wp'(-\omega/2) = -\wp'(\omega/2)$

This means $\wp'(\omega/2) = 0.$

In particular
$\wp'(\omega_1/2) = 0$
$\wp'(\omega_2/2) = 0$ and
$\wp'((\omega_1 + \omega_2)/2) = 0.$

$$[\wp'(z)]^2 = 4[\wp(z)]^3 - g_2\wp(z) - g_3,$$

This means the numbers
$\wp(\omega_1/2), \wp(\omega_2/2), \wp((\omega_1 + \omega_2)/2)$
are roots of the cubic
$4x^3 - g_2 x - g_3 = 0.$

One can show these roots are distinct.

In particular, if g_2, g_3 are algebraic, the roots are algebraic.

Schneider's Theorem

If g_2, g_3 are algebraic and $\wp$ is the associated Weierstrass $\wp$-function, then for α algebraic, $\wp(\alpha)$ is transcendental.

Since $\wp(\omega_1/2)$, $\wp(\omega_2/2)$ are algebraic
It follows that the periods ω_1, ω_2 must be transcendental when g_2, g_3 are algebraic.

This is the elliptic analog of the Hermite-Lindemann theorem
that says if α is a non-zero algebraic number, then e^α is transcendental.

Note that we get π transcendental by setting $\alpha = 2\pi i$

Why should this interest us?

Let $y = \sin x$.
Then
$(\frac{dy}{dx})^2 + y^2 = 1.$

Let $y = \wp(x)$.
Then
$\left(\frac{dy}{dx}\right)^2 = 4y^3 - g_2 y - g_3.$

Thus $\frac{dy}{\sqrt{1-y^2}} = dx.$

Thus $\frac{dy}{\sqrt{4y^3-g_2y-g_3}} = dx.$

Integrating both sides, we get
$\int_0^{\sin b} \frac{dy}{\sqrt{1-y^2}} = b.$

Integrating both sides, we get
$\int_{\wp(\omega_1/2)}^{\wp((\omega_1+\omega_2)/2)} \frac{dy}{\sqrt{4y^3-g_2y-g_3}} = \frac{\omega_2}{2}$

Let's look at our formula for the circumference of an ellipse again.

$\int_{1-k^2}^{1} \frac{tdt}{\sqrt{t(t-1)(t-(1-k^2))}}$

where

$k^2 = 1 - \frac{b^2}{a^2}$.

The cubic in the integrand is not in Weierstrass form.

It can be put in this form.

But let us look at the case $k = 1/\sqrt{2}$.

Putting $t = s + 1/2$, the integral becomes

$\int_0^{1/2} \frac{2s+1}{\sqrt{4s^3-s}} ds$.

The integral
$\int_0^{1/2} \frac{ds}{\sqrt{4s^3-s}}$
is a period of the elliptic curve
$y^2 = 4x^3-x$.

But what about $\int_0^{1/2} \frac{s\,ds}{\sqrt{4s^3-s}}$?

Let us look at the Weierstrass ζ-function:
$\zeta(z) = \frac{1}{z} + \sum_{0\neq\omega\in L} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right)$.

Observe that $\zeta'(z) = -\wp(z)$.

ζ is not periodic!

- It is "quasi-periodic".
- What does this mean?

$$\zeta(z+\omega) = \zeta(z) + \eta(\omega).$$

Put $z = -\omega/2$ to get
$\zeta(\omega/2) = \zeta(-\omega/2) + \eta(\omega)$.
Since ζ is an odd function, we get
$\eta(\omega) = 2\zeta(\omega/2)$.

This is called a quasi-period.

What are these quasi-periods?

Observe that
$\zeta(\omega_1/2) = \zeta(-\omega_1/2 + \omega_1) = \zeta(-\omega_1/2) + \eta(\omega_1)$
But ζ is odd, so $\zeta(-\omega_1/2) = -\zeta(\omega_1/2)$ so that
$2\zeta(\omega_1/2) = \eta(\omega_1)$.

Similarly, $2\zeta(\omega_2/2) = \eta(\omega_2)$

Since η is a linear function on the period lattice, we get
$2\zeta((\omega_1 + \omega_2)/2) = \eta(\omega_1) + \eta(\omega_2)$.

Thus
$d\zeta = -\wp(z)dz.$
Recall that
$d\wp = \sqrt{4\wp(z)^3 - g_2\wp(z) - g_3}dz.$

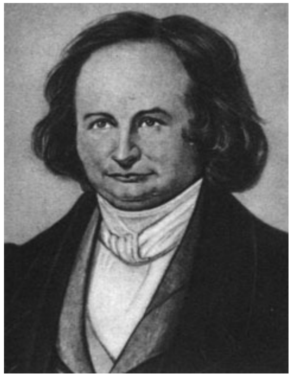
Hence,
$d\zeta = -\frac{\wp(z)d\wp}{\sqrt{4\wp(z)^3-g_2\wp(z)-g_3}}$

We can integrate both sides
from $z = \omega_1/2$
to $z = (\omega_1 + \omega_2)/2$ to get
$\eta_2 = 2\int_{e_1}^{e_2} \frac{xdx}{\sqrt{x^3-g_2x-g_3}}$
where
$e_1 = \wp(\omega_1)$ and
$e_2 = \wp((\omega_1 + \omega_2)/2).$

Hence, our original integral is a sum of a period and a quasi-period.

Are there triply periodic functions?

- In 1835, Jacobi proved that such functions of a single variable do not exist.
- Abel and Jacobi constructed a function of two variables with four periods giving the first example of an abelian variety of dimension 2.



1804-1851

1802 - 1829

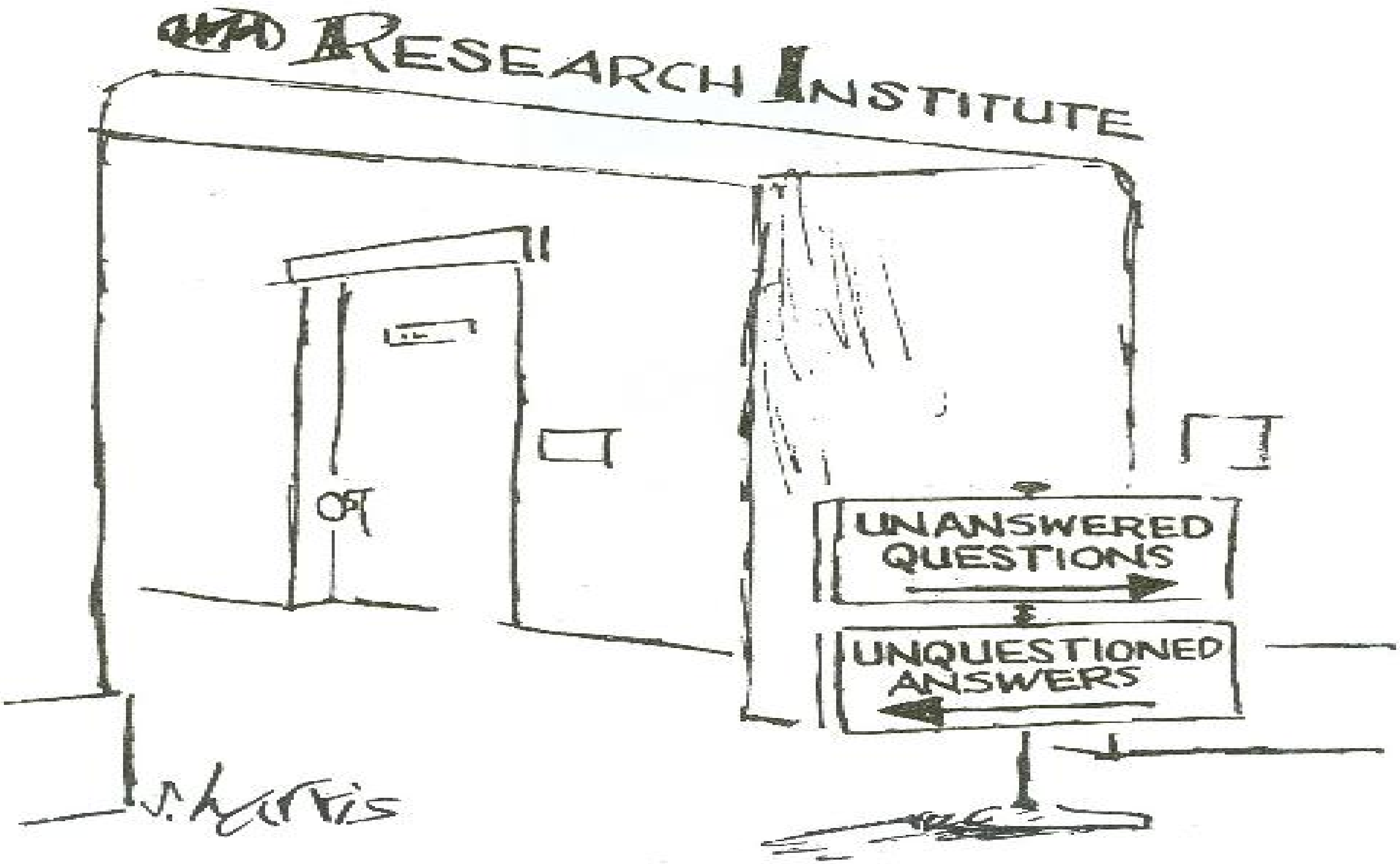
What exactly is a period?

- These are the values of absolutely convergent integrals of algebraic functions with algebraic coefficients defined by domains in R^n given by polynomial inequalities with algebraic coefficients.
- For example π is a period.

$$\pi = \int\int_{x^2+y^2\leq 1} dxdy$$

Some unanswered questions

- Is e a period?
- Probably not.
- Is $1/\pi$ a period?
- Probably not.
- The set of periods $\mathcal{P}$ is countable but no one has yet given an explicit example of a number not in $\mathcal{P}$.


RESEARCH INSTITUTE
UNANSWERED QUESTIONS
UNQUESTIONED ANSWERS
S. Harris

$$\mathbf{N} \subseteq \mathcal{Z} \subseteq \mathcal{Q} \subseteq \mathcal{A} \subseteq \mathcal{P}$$