THE ARAKARUM
From Plimpton 322 and Pythagorus,
to Elliptic Curve Cryptography

NUMBER THEORY, ALGEBRA, GEOMETRY, ANALYSIS
(Elementary, basic, fun)
Friberg (Schoyen): MS 3908 subdivided trapezoid

** Geometric subdivision of a trapezoid: lengths 1:2:3, areas 2:3:2

8.1.2 b. MS 3908. A trapezoid divided into three stripes, and a complete set of associated numerical parameters.
Cutting equal areas from a right-triangular field

Average height by base:

\[ A = \frac{1}{2} (u - t)(su + st) = \frac{1}{2} s \]

\[ u^2 - t^2 = (u - t)(u + t) = 1 \quad \Rightarrow \quad x \cdot \frac{1}{x} = 1 \]

\[ u - t = x \quad u + t = \frac{1}{x} \]

\[ \Rightarrow \quad u = \frac{1}{2} \left( \frac{1}{x} + x \right) = \frac{1 + x^2}{2x}, \quad t = \frac{1}{2} \left( \frac{1}{x} - x \right) = \frac{1 - x^2}{2x} \]

(Algebraic precursor to cosh and sinh)
The ‘arakarum’ – ‘multiplying factor’? – : first glimpse

\[ t = \frac{l_2}{l_1} = \frac{m_2}{m_1}; \quad \text{‘arakarum’}: \quad \chi = \frac{l_1 - l_2}{l_1 + l_2} = \frac{1 - t}{1 + t} = \chi(t) \]

Use: conversion between differences and sums: (and more later!)

\[
\frac{(m_1 + m_2)}{2} \cdot \chi = \frac{m_1}{2} \cdot \frac{(1 + t)}{1} \cdot \frac{(1 - t)}{1 + t} = \frac{m_1}{2} \cdot \frac{(1 - t)}{1} = \frac{(m_1 - m_2)}{2}
\]

[Neugebauer & Sachs]
Define

\[ y = \chi(x) := \frac{1 - x}{1 + x} \]

Then \( \chi \) is an involution (its own inverse function): \( x = \chi(y) = \frac{1 - y}{1 + y} \).

\[-y = \chi\left(\frac{1}{x}\right) = \frac{1 - 1/x}{1 + 1/x} = \frac{x - 1}{x + 1} \]

\[ \frac{1}{y} = \chi(-x) = \frac{1 - (-x)}{1 + (-x)} = \frac{1 + x}{1 - x} \]

\[-\frac{1}{y} = \chi\left(-\frac{1}{x}\right) = \frac{1 - (-\frac{1}{x})}{1 + (-\frac{1}{x})} = \frac{x + 1}{x - 1} \]

Hence \( \chi \) interchanges multiplicative and additive inverse operations.
** Translated about 70 years ago
** List of Pythagorean triples?
(eg (3,4,5), (5,12,13), ... Integers forming sides of a right-angled triangle.)

<table>
<thead>
<tr>
<th>$(d/l)^2$</th>
<th>diagonal $d$</th>
<th>short $s$</th>
<th>row #</th>
<th>long $l$</th>
<th>$(1-x)/(1+x)$</th>
<th>$x = q/p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>missing</td>
<td>missing</td>
<td>missing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.98...</td>
<td>169</td>
<td>119</td>
<td>1</td>
<td>120</td>
<td>0.41</td>
<td>0.417</td>
</tr>
<tr>
<td>1.95...</td>
<td>4825</td>
<td>3367</td>
<td>2</td>
<td>3456</td>
<td>0.41</td>
<td>0.422</td>
</tr>
<tr>
<td>1.92...</td>
<td>6649</td>
<td>4601</td>
<td>3</td>
<td>4800</td>
<td>0.4</td>
<td>0.427</td>
</tr>
<tr>
<td>1.89...</td>
<td>18541</td>
<td>12709</td>
<td>4</td>
<td>13500</td>
<td>0.4</td>
<td>0.432</td>
</tr>
<tr>
<td>1.82...</td>
<td>97</td>
<td>65</td>
<td>5</td>
<td>72</td>
<td>0.39</td>
<td>0.444</td>
</tr>
<tr>
<td>1.79...</td>
<td>481</td>
<td>319</td>
<td>6</td>
<td>360</td>
<td>0.38</td>
<td>0.450</td>
</tr>
<tr>
<td>1.72...</td>
<td>3541</td>
<td>2291</td>
<td>7</td>
<td>2700</td>
<td>0.37</td>
<td>0.463</td>
</tr>
<tr>
<td>1.69...</td>
<td>1249</td>
<td>799</td>
<td>8</td>
<td>960</td>
<td>0.36</td>
<td>0.469</td>
</tr>
<tr>
<td>1.64...</td>
<td>769</td>
<td>481</td>
<td>9</td>
<td>600</td>
<td>0.35</td>
<td>0.480</td>
</tr>
<tr>
<td>1.59...</td>
<td>8161</td>
<td>4961</td>
<td>10</td>
<td>6480</td>
<td>0.34</td>
<td>0.494</td>
</tr>
<tr>
<td>1.56...</td>
<td>75</td>
<td>45</td>
<td>11</td>
<td>30</td>
<td>1</td>
<td>0.500</td>
</tr>
<tr>
<td>1.49...</td>
<td>2929</td>
<td>1679</td>
<td>12</td>
<td>2400</td>
<td>0.32</td>
<td>0.521</td>
</tr>
<tr>
<td>1.45...</td>
<td>289</td>
<td>161</td>
<td>13</td>
<td>240</td>
<td>0.3</td>
<td>0.533</td>
</tr>
<tr>
<td>1.43...</td>
<td>3229</td>
<td>1771</td>
<td>14</td>
<td>2700</td>
<td>0.3</td>
<td>0.540</td>
</tr>
<tr>
<td>1.39...</td>
<td>106</td>
<td>56</td>
<td>15</td>
<td>90</td>
<td>0.29</td>
<td>0.556</td>
</tr>
</tbody>
</table>

** Arguments concerning mathematical knowledge of the Old Babylonians
‘Pythagorean triples’ and Plimpton 322

Greeks: \( a^2 + b^2 = c^2 \) (integer-solution preoccupation: 1000 years later)

Old Babylonians?

\[
a^2 + b^2 = c^2 \quad \implies \quad a^2 = c^2 - b^2
\]

(distribute/rescale) \( \implies 1 = u^2 - t^2 = (u - t)(u + t) = x.x^{-1} \)

Choose \( x \) any regular number, look up reciprocal \( x^{-1} \) in a table

(\( x, x^{-1} \): The ‘igi’ and the ‘igi-bi’)

Plug in, rescale:

\[
u = \frac{1}{2} \left( \frac{1}{x} + x \right) = \frac{1 + x^2}{2x}, \quad t = \frac{1}{2} \left( \frac{1}{x} - x \right) = \frac{1 - x^2}{2x}.
\]

** Old Babylonian parametrization by \( x \): Pythagorean triangle (up to rational rescaling) if and only if \( x \) rational
Modern proof: squaring Gaussian integers parametrizes Pythagorean triples

Squaring $z = p + iq$ gives Pythagorean triples, via rational points on the circle.

Generalized Thales Theorem asserts that the line through $-1 \in \mathbb{C}$ parallel to $PA$ intersects the line $PT$ as a rational point on the circle. All Pythagorean triangles can be rationally rescaled to this form:
The Cayley transform

Slope: \( h = \frac{q}{p} \); point: \( P = \left( \frac{p^2 - q^2}{p^2 + q^2}, \frac{2pq}{p^2 + q^2} \right) \)

\[
P = \frac{1 - h^2}{1 + h^2} + i \frac{2h}{1 + h^2} = \frac{(1 + ih)^2}{(1 + ih)(1 - ih)}
\]

\( h \rightarrow P = \frac{1 + ih}{1 - ih} \) Cayley transform \( h \in \mathbb{IR} \)

\( u = h + ik \rightarrow w = \frac{1 + iu}{1 - iu} \) Cayley transform

Fractional-linear transform (invertible): Riemann sphere to itself

Upper-half-plane \( \rightarrow \) interior-of-unit-disc \( (k > 0) \).

\[
u \rightarrow w = \frac{1 + iu}{1 - iu} = x + iy; \quad w \rightarrow u = i \frac{1 - w}{1 + w} = h + ik
\]
Modular diagram in upper-half-space and unit disc

Rational numbers on the real line (as boundary of the upper-half-plane) and as rational points on the circle under the Cayley transform.
The arakarum and Cayley map

\[ P = \left( \frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right) \]

\[ P, Q, R, S \text{ by reflection, corresponding to } \{ t, 1/t, -1/t, -t \} \]

\[
\frac{1 - \frac{(1-t)^2}{(1+t)^2}}{1 + \frac{(1-t)^2}{(1+t)^2}} = \frac{2t}{1 + t^2}, \quad \frac{2\frac{(1-t)}{(1+t)}}{1 + \frac{(1-t)^2}{(1+t)^2}} = \frac{1 - t^2}{1 + t^2}.
\]
The ‘arakarum’: second appearance

Four real points related by additive and multiplicative inverse:

\begin{align*}
    x & \rightarrow \left( \frac{1 - x^2}{1 + x^2}, \frac{2x}{1 + x^2} \right) \\
    \frac{1}{x} & \rightarrow \left( -\frac{1 - x^2}{1 + x^2}, \frac{2x}{1 + x^2} \right) \\
    -x & \rightarrow \left( \frac{1 - x^2}{1 + x^2}, -\frac{2x}{1 + x^2} \right) \\
    -\frac{1}{x} & \rightarrow \left( -\frac{1 - x^2}{1 + x^2}, -\frac{2x}{1 + x^2} \right)
\end{align*}

corresponding to reflection in the vertical and horizontal axes
Transform of points on axes and unit circle

Iterate Cayley transform:

\[
t \rightarrow \frac{1 + it}{1 - it} \rightarrow i\frac{1 - t}{1 + t} \rightarrow t
\]

real axis \hspace{1cm} \text{circle} \hspace{1cm} \text{imaginary axis} \hspace{1cm} \text{real axis}

\[
\frac{1 - s}{1 + s} \rightarrow i\frac{1 - is}{1 + is} \rightarrow is \rightarrow \frac{1 - s}{1 + s}
\]
Cayley transform and the octahedron/cube

Cayley transform: order-3 rotation of an octahedron around an axis through opposite triangle faces.

Rotated octahedron

Projection to $\mathbb{C}$

Star of Ishtar, Daughter of Sin
The arakarum and Star(s) of Ishtar
The images of the six vertices of the regular octahedron

$$\infty, \ 0, \ 1, \ -1, \ i, \ -i$$

and

the images of the four vertices from the ‘arakarum’

$$a, \ -a, \ \frac{1}{a}, \ -\frac{1}{a}$$

create the ‘Star of Ishtar’
Important Babylonian ‘trinity’: Sin, Shamash and Ishtar

**Shamash**: God of the sun, justice, ...

**Sin**: God of the Moon. Father of ...

**Ishtar**: (Astarte, Venus, ...) Goddess of the morning/evening star .... ‘Mother Earth’ .... Gilgamesh ....

(IRA-VAC-31-29-11-13) Star of Ishtar, Daughter of Sin
Arakarum substitution, iteration (Fagnano?)
Arakarum substitution, iteration (Fagnano?)
Arakarum substitution, iteration (Fagnano?)
Arakarum substitution, iteration (Fagnano?)
Arakarum substitution, iteration (Fagnano?)
Arakarum substitution, iteration (Fagnano?)
Arakarum substitution, iteration (Fagnano?)
Arakarum substitution, iteration (Fagnano?)
Arakarum substitution, iteration (Fagnano?)

The following diagram indicates some of the consequences of generating new points by this construction.
Transcendental functions: trigonometric functions

arc length: curve $x^2 + y^2 = \left(\frac{1-t^2}{1+t^2}\right)^2 + \left(\frac{2t}{1+t^2}\right)^2 = 1$

$$ds^2 = \left(\frac{-2t(1+t^2)-(1-t^2)(2t)}{(1+t^2)^2}\right)^2 dt^2 + \left(\frac{2(1+t^2)-(2t)(2t)}{(1+t^2)^2}\right)^2 dt^2 = 4\frac{dt^2}{(1+t^2)^2}$$

integral (to function): arc-length $f(u) = 2\int_0^u \frac{1}{1 + t^2} dt = 2\arctan(u)$

derivative/integrand: $df(u) = 2\frac{1}{1 + u^2} du$

ARC/ANGLE DOUBLING :
$$\int_0^{2a/(1-a^2)} \frac{1}{1 + t^2} dt = 2 \int_0^a \frac{1}{1 + t^2} dt$$
‘Polynomial’ substitution to double arc length

P: \[
\left( \frac{2s}{1 + s^2}, \frac{(1 - s^2)}{1 + s^2} \right)
\]

Q: vertical tangent \( t = \tan 2x \)

\[
t = \frac{2s}{1 - s^2}
\]

\[
dt = \frac{2(1 - s^2) - 2s(-2s)}{(1 - s^2)^2} \, ds
\]

\[
1 + t^2 = \frac{(1 - s^2)^2 + 4s^2}{(1 - s^2)^2}
\]
Transcendental functions: ‘tangent addition’

\[
F(x) = \int_0^x \frac{du}{1 + u^2} \implies dF = \frac{dx}{1 + x^2}
\]

Consider:
\[
dF(x_1) + dF(x_2) = \frac{dx_1}{1 + x_1^2} + \frac{dx_2}{1 + x_2^2}
\]

\[
\frac{(1 + x_1^2)(1 + x_2^2)}{(1 - x_1 x_2)^2} \left\{ \frac{dx_1}{1 + x_1^2} + \frac{dx_2}{1 + x_2^2} \right\}
\]

\[
= \frac{1}{(1 - x_1 x_2)^2} \left\{ (1 - x_1 x_2 + x_1 x_2 + x_2^2)dx_1 + (1 - x_1 x_2 + x_1 x_2 + x_1^2)dx_2 \right\}
\]

\[
= \frac{(dx_1 + dx_2)(1 - x_1 x_2)}{(1 - x_1 x_2)^2} + \frac{(x_1 + x_2)(x_2 dx_1 + x_1 dx_2)}{(1 - x_1 x_2)^2} = d\left( \frac{(x_1 + x_2)}{(1 - x_1 x_2)} \right)
\]

\[
(1 + x_1^2)^{-1}dx_1 + (1 + x_2^2)^{-1}dx_2 = (1 + \frac{(x_1 + x_2)^2}{(1 - x_1 x_2)^2})^{-1}d\left( \frac{(x_1 + x_2)}{(1 - x_1 x_2)} \right)
\]

Conclude:
\[
\tan(a_1 + a_2) = \frac{(\tan a_1 + \tan a_2)}{(1 - \tan a_1 \tan a_2)}
\]
Integral Substitution: ‘tangent addition’

\[ u_2 = \frac{(u_3 - x_1)}{(1 + x_1 u_3)}, \quad u_3 = \frac{(x_1 + u_2)}{(1 - x_1 u_2)}, \quad \frac{du_3}{1 + u_3^2} = \frac{du_2}{1 + u_2^2} \]

\[ x_3 = \frac{(x_1 + x_2)}{(1 - x_1 x_2)} \]

\[ \int_{-x_1}^{x_2} \frac{du_2}{1 + u_2^2} = \int_{0}^{x_3} \frac{du_3}{1 + u_3^2} = \int_{-x_1}^{0} \frac{du_2}{1 + u_2^2} + \int_{0}^{x_2} \frac{du_2}{1 + u_2^2} \]

\[ \int_{0}^{x_3} \frac{du_3}{1 + u_3^2} = \int_{0}^{x_1} \frac{du_1}{1 + u_1^2} + \int_{0}^{x_2} \frac{du_2}{1 + u_2^2}, \quad u_1 = -u_2 \]

\[ \arctan x_3 = \arctan x_1 + \arctan x_2, \quad a_3 = a_1 + a_2, \quad \text{where} \]

\[ a_1 = \arctan x_1, \quad a_2 = \arctan x_2, \quad a_3 = \arctan x_3 \]

\[ a_1 + a_2 = \arctan \left( \frac{\tan a_1 + \tan a_2}{1 - \tan a_1 \tan a_2} \right), \quad \tan(a_1 + a_2) = \frac{(\tan a_1 + \tan a_2)}{(1 - \tan a_1 \tan a_2)} \]
BERNOULLI’S LEMNISCATE

[‘Bagel-dunking in Babylon’]

Three kinds of ‘horizontal slice’

Proclus (412-485 AD) attributes to some Perseus. (‘Morse theory’)

origins of the hippopede (‘horse-fetter’)
Jakob Bernouilli (according to Struik) considered the lemniscate:
\[ x^2 + y^2 = a \sqrt{x^2 - y^2} \implies r^2 = ar \sqrt{\cos 2\theta}, \quad r^2 = a^2 \cos 2\theta \]

Fagnano (later Gauss): integral
\[
\int_0^w \frac{1}{\sqrt{1 - u^4}} \, du
\]
for arc length of the lemniscate:
\[ r^2 = \cos 2\theta \]

ASIDE: \( t = \tan \theta \)
\[ r^2 = 2 \cos \theta^2 - 1 = \frac{2}{\sec^2 \theta} - 1 = \frac{2}{1 + \tan^2 \theta} - 1 = \frac{1 - \tan^2 \theta}{1 + \tan^2 \theta} \]
\[ r^2 = \frac{1 - t^2}{1 + t^2} \iff t^2 = \frac{1 - r^2}{1 + r^2}. \]
\[(x^2 + y^2)^2 - 2xy = 0 \implies r^2 = \sin 2\theta = x^2 + y^2,\]

\[r \, dr = \cos 2\theta \, d\theta, \quad d\theta = \frac{r \, dr}{\sqrt{1 - \sin^2 2\theta}} = \frac{r \, dr}{\sqrt{1 - r^4}}\]

\[dx = \cos \theta \, dr - r \sin \theta \, d\theta, \quad dy = \sin \theta \, dr + r \cos \theta \, d\theta\]

\[dx^2 + dy^2 = (\cos^2 \theta + \sin^2 \theta)dr^2 + r^2(\sin^2 \theta + \cos^2 \theta)d\theta^2 = dr^2 + r^2d\theta^2\]

\[ds^2 = dr^2 + r^2d\theta^2 = \left[\frac{\cos^2 2\theta}{\sin 2\theta} + \sin 2\theta\right]d\theta^2 = \left[\frac{d\theta}{r}\right]^2\]

\[s = \int_0^r \frac{1}{\sqrt{1 - r^4}}dr\]
Parameters: circle and lemniscate

QUARTER-CIRCLE

\[(x, y) = \frac{1}{1 + t^2} (1 - t^2, 2t)\]

\[l(t) = 2 \int_0^t \frac{1}{1 + u^2} \, du\]

-----------------------------

QUARTER-LEMNISCATE

\[(x, y) = \frac{t}{1 + t^4} (1 + t^2, 1 - t^2)\]

\[l(t) = \sqrt{2} \int_0^t \frac{1}{\sqrt{1 + u^4}} \, du\]

(The integrand arising from this parametrization was first discussed briefly by Carlson, with the comment that ‘the geometry was not apparent’.)
**Inverse:**

\[ x \rightarrow \frac{1}{x} \]

**Hyperbolae:**

\[ xy = 1 \]

Rotate \(2\pi/8): \]

\[ (x - y)(x + y) = x^2 - y^2 = 1 \]

Translate, scale gives Arakarum, symmetric rational function:

\[ y = \frac{1 - x}{1 + x} = -1 + \frac{2}{1 + x} \]

\[ (y + 1) = 2 \frac{1}{(1 + x)} \]

**Lemniscates:** Geometric inversion of hyperbola in circle:
From reciprocals to inversion: parametrized hyperbola

\[
\frac{(v + 1/v)^2}{4} - \frac{(v - 1/v)^2}{4} = 1
\]

\[
cosh^2 u - \sinh^2 u = 1
\]
The lemniscate as inversion of a hyperbola

\[ P \text{ is constructed starting with } YL; \ OP \text{ bisects } \angle VOR. \ TP \text{ determines } UV \text{ – hence also } A = L', YL', \text{ which determines a further point } P', \text{ etc.} \]
Bernoulli’s lemniscate: inverted hyperbola

\[ Q : \left( \frac{a^2 + 1}{2a}, \frac{a^2 - 1}{2a} \right), \quad |OQ|^2 = \frac{a^4 + 1}{2a^2} = R^2 \]

\[ P : \quad s\left( \frac{a^2 + 1}{2a}, \frac{a^2 - 1}{2a} \right), \quad |OP|^2 = s^2\left( \frac{a^4 + 1}{2a^2} \right) = R^{-2} \]

\[ \Rightarrow \quad s^2 = \frac{2a^2}{a^4 + 1} \cdot \frac{2a^2}{a^4 + 1}, \quad P = a\left( \frac{a^2 + 1}{a^4 + 1}, \frac{a^2 - 1}{a^4 + 1} \right) \]

\[ ZP : \quad \text{slope:} \quad \frac{1 + \frac{a^3 - a}{a^4 + 1}}{\frac{a^3 + a}{a^4 + 1}} = \frac{a^4 + 1 + a^3 - a}{a^3 + a} \]
Elliptic integrals, functions, curves from the lemniscate

Jacobi: credits origins to

1718 Fagnano’s work on lemniscate arc length integrals
1751 given to Euler for review: birth of ELLIPTIC INTEGRALS

Source of Fagnano’s insights: unclear for 300 years

G.N. Watson . . . ‘will most likely never be known’ . . . maybe complex numbers?
C. Siegel: . . . ‘maybe by analogy with trigonometric substitutions?’
Fagnano first substitution

\[ r^2 = 2a^2 \cos 2\theta, \quad x = a\sqrt{t + t^2}, \quad y = a\sqrt{t - t^2}, \quad a = \frac{1}{\sqrt{2}}, \quad t = \cos 2\theta \]

arc length:

\[ l = \frac{a}{\sqrt{2}} \int \frac{dt}{\sqrt{t(1 - t^2)}} = \frac{1}{2} \int \frac{dt}{\sqrt{t(1 - t^2)}} \]

Fagnano:

\[ (t + 1)(z + 1) = 2. \]

\[ \Rightarrow \quad \frac{dt}{\sqrt{t(1 - t^2)}} + \frac{dz}{\sqrt{z(1 - z^2)}} = 0 \]

\[ \frac{1}{2} \int_0^z \frac{dt}{\sqrt{t(1 - t^2)}} = \frac{1}{2} \int_0^1 \frac{dt}{\sqrt{t(1 - t^2)}} \]

transformation under which the integrand is invariant. BUT NOTE!:

\[ t + 1 = \frac{2}{z + 1} \quad \Leftrightarrow \quad t = \frac{2}{1 + z} - \frac{1 + z}{1 + z} \quad \Rightarrow \quad t = \frac{1 - z}{1 + z} \]
Fagnano first substitution: origins of substitution

\[ r^2 = 2a^2 \cos 2\theta, \]

\[ r^2 = t, \quad t = \cos 2\theta, \quad a = \frac{1}{\sqrt{2}} \]

\[ x = r \cos \theta = \sqrt{t} \sqrt{\frac{1}{2}(1 + \cos 2\theta)}, \quad y = r \sin \theta = \sqrt{t} \sqrt{\frac{1}{2}(1 - \cos 2\theta)} \]

\[ x = \sqrt{\frac{t + t^2}{2}}, \quad y = \sqrt{\frac{t - t^2}{2}} \]

arc length:
\[ l = \frac{a}{\sqrt{2}} \int \frac{dt}{\sqrt{t(1 - t^2)}} = \frac{1}{2} \int \frac{dt}{\sqrt{t(1 - t^2)}} \]
Fagnano 1718, doubling formula; Euler elliptic integrals,

\[ t^2 = \frac{2v^2}{1 + v^4} \quad \Rightarrow \quad \sqrt{1 - t^4} = \frac{1 - v^4}{1 + v^4} \]

\[ \frac{dt}{\sqrt{1 - t^4}} = \sqrt{2} \frac{dv}{\sqrt{1 + v^4}} \]

\[ v^2 = \frac{2w^2}{1 - w^4} \quad \Rightarrow \quad \frac{dv}{\sqrt{1 + v^4}} = \sqrt{2} \frac{dw}{\sqrt{1 - w^4}} \]

\[ t^2 = \frac{4w^2(1 + w^4)}{(1 - w^4)^2} \quad \Rightarrow \quad \frac{1}{\sqrt{1 + t^4}} dt = 2 \frac{1}{\sqrt{1 + w^4}} dw \]

Similarly

\[ \int_0^{2x} \frac{\sqrt{1 - x^4}/(1 + x^4)}{\sqrt{1 - t^4}} \, dt = 2 \int_0^x \frac{dt}{\sqrt{1 - t^4}} \]

What is a natural origin for these substitutions?
Assertion 1: \[ x^2 z^2 = 1 - \sqrt{1 - z^4}, \quad x^2 = \frac{1 - \sqrt{1 - z^4}}{z^2} \]

\[ \Rightarrow 1 - z^4 = (1 - x^2 z^2)^2 = 1 - 2x^2 z^2 + x^4 z^4 \Rightarrow 2x^2 = z^2 (1 + x^4) \]

\[ \Rightarrow z^2 = \frac{2x^2}{1 + x^4} \]

Solves

\[ \frac{dz}{\sqrt{1 - z^4}} = \sqrt{2} \frac{dx}{\sqrt{1 + x^4}} \]
Arakarum, cross ratio, multiplicative hyperbolic distances

\[
\frac{4s(1+ss)}{1+6ss+sسس} \quad \frac{4s(1+ss)}{(1-ss)(1-ss)}
\]

\[
\frac{2s}{1+ss} \quad \frac{2S}{1-SS}
\]

\[
\frac{(1-S)(1-S)}{(1+S)(1+S)} \quad \frac{1-S}{1+S}
\]

\[
\frac{ss}{1-سسسس} \quad \frac{2ss}{1-سسسس}
\]

\[
\frac{(1-ss)}{1+ss} \quad \frac{(1-ss)(1-ss)}{(1+6ss+sسس)}
\]
Geometric origins of the substitutions

Compare this diagram with that for doubling the arc of the circle.

\[ ee = p \]

\[ \frac{4p(1+pp)}{(1+6pp+pppp)} \]

\[ bb = \frac{2aa}{(1-aaaaa)} \]
\[ = \frac{4p(1+pp)}{(1-pp)(1-pp)} \]

\[ aa = \frac{2p}{(1+pp)} \]

\[ \frac{(1-pp)(1-pp)}{(1+6pp+pppp)} \]
Historical forms for elliptic curve equations

- Intersections of two quadrics in $\mathbb{CP}^3$
- **Short Weierstrass** form: $y^2 = x^3 + ax + b$
- **Montgomery** form: $By^2 = x^3 + Ax^2 + x$.
- **Extended Jacobi** form: $v^2 = 1 - 2\rho u^2 + du^4$
- **Legendre** form: $y^2 = x(x - 1)(x - \lambda)$

  **Rationality of points of order 2.**

- **Hessian** form: $u^3 + v^3 + w^3 = 3\mu uvw$.

  **Curves with points of order 3.** (Projective coordinates)

- **Edwards** form (2007): $x^2 + y^2 = c^2 + c^2x^2y^2$

  **Quartic plane projective curve with rational singularity:** Up to $k$-rational birational equivalence, Edwards elliptic curves are those having a $k$-rational point of order 4.
Edwards curves


\[ x^2 + y^2 = c^2 + c^2 x^2 y^2 \]

where \( c \) is an arbitrary parameter. Other equivalent forms:

\[ x^2 + y^2 = 1 + e x^2 y^2 \]
\[ x^2 + y^2 = c^2(1 + d x^2 y^2) \]

For

\[ x^2 + y^2 = c^2(1 + d^2 x^2 y^2) \]
\[ \frac{x^2}{c^2} + \frac{y^2}{c^2} = 1 + d^2 c^4 \frac{x^2}{c^2} \frac{y^2}{c^2} \]
\[ u^2 + v^2 = 1 + (dc^2)^2 u^2 v^2 = 1 + e^2 u^2 v^2, \quad e = dc^2 \]
Edwards curves: Addition Law very simple!

Distinct points:

\[(x_1, y_1) + (x_2, y_2) = \left( \frac{x_1 y_1 + x_2 y_2}{x_1 x_2 + y_1 y_2}, \frac{x_1 y_1 - x_2 y_2}{x_1 y_2 - x_2 y_1} \right)\]

Doubling a point:

\[(u_1, v_1) + (u_1, v_1) = \left( \frac{2u_1 v_1}{1 + c^4 u_1^2 v_1^2}, \frac{u_1^2 - v_1^2}{1 - c^4 u_1^2 v_1^2} \right)\]

The general group law is given by

\[(u_1, v_1) + (u_2, v_2) = \left( \frac{u_1 v_2 + v_1 u_2}{1 + c^4 u_1 u_2 v_1 v_2}, \frac{u_1 u_2 - v_1 v_2}{1 - c^4 u_1 u_2 v_1 v_2} \right)\]

(simplifies for distinct points)
Hyperbolic geometry: Beltrami/Poincaré model

Geodesics as arcs of circles meeting unit circle orthogonally
Hyperbolic geometry: Beltrami/Klein model

Geodesics as arcs of chords
Hyperbolic geometry: Beltrami/Poincaré/Klein models

Radial correspondence between points of two models
Disc models for hyperbolic geometry: Poincaré and Klein

Isometric arcs for each model, simultaneously
Arakarum gives multiplicative hyperbolic distance

$k = \frac{2p}{pp+1}$

$1/a$

$(aa-1)/2a$

$(aa+1)/2a$

$(1-p)/(1+p)$

Hyperbola
Hyperbolic geometry: Hartshorne’s ‘multiplicative length’

Poincaré model: For $P' = (0, p)$, the segment $OP'$, based at the origin, has multiplicative length $\mu_P$ given by

$$\mu_P^{-1}(OP') := \left\{ \frac{0 - (-i)}{ip - (-i)} \right\} \left\{ \frac{ip - i}{0 - i} \right\} = \frac{1 - p}{1 + p}$$

which is the Euclidean length $OP^*$. The middle is the cross-ratio of complex numbers $(0, ip; -i, i)$. The additive length is $d_h(OP) := \log \mu_P$.

Klein model: For $K' = (0, 2p/(1 + p^2))$, the segment $OK'$, based at the origin, has multiplicative length given by the Euclidean length $OK^*$

$$\mu_K^{-1}(OK') := \frac{|| (0, 0) - (0, -1)|| (0, 2p/(1 + p^2)) - (0, 1)|| (0, 0) - (0, 1)|}{|| (0, 2p/(1 + p^2)) - (0, -1)|| (0, 0) - (0, 1)||} = \frac{(1 - p)^2}{(1 + p)^2}$$

Additive lengths: take the logarithm, with a factor half for Klein’s model to compensate for the square.
Arakarum, cross ratio, multiplicative hyperbolic distances
Hyperbolic Pythagorean right-triangles as Edwards curves

Additive metric: side lengths $\alpha, \beta, \gamma$ (hypotenuse):

\[
\cosh \alpha \cdot \cosh \beta = \cosh \gamma \quad \text{hyperbolic right-triangle}
\]

Multiplicative metric: side lengths $u, v, w$ (hypotenuse):

\[
\frac{2u}{1 + u^2} \cdot \frac{2v}{1 + v^2} = \frac{2w}{1 + w^2}
\]

Problem: Find rational solutions

Multiplicative lengths: determined by arakarum of Euclidean segments: set

\[
u = \frac{1 - x}{1 + x}, \quad v = \frac{1 - y}{1 + y}, \quad w = \frac{1 - a}{1 + a}
\]

\[
\frac{1 - x^2}{1 + x^2} \cdot \frac{1 - y^2}{1 + y^2} = \frac{1 - a^2}{1 + a^2}
\]

\[
x^2 + y^2 = a^2 + x^2 y^2 a^2
\]

\[
x^2 + y^2 = a^2(1 + x^2 y^2)
\]

‘Edwards curves with parameter $a$ as hyperbolic triangle hypotenuse’
Edwards curves and octahedral vertices

Setting

\[ z = y(1 - a^2x^2), \quad a \neq 0 \]

transforms

\[ x^2 + y^2 = a^2 + a^2x^2y^2 \]

\[ \rightarrow z^2 = (a^2 - x^2)(1 - a^2x^2) = a^2(x - a)(x + a)(x - \frac{1}{a})(x + \frac{1}{a}) \]

This gives an elliptic curve, a Riemann surface defined as a 2-fold branched cover over the Riemann sphere with 4 branch points at

\[ x = -a, \quad +a, \quad -\frac{1}{a}, \quad \frac{1}{a} \]

if and only if \( a^5 \neq a \), i.e. \( a \neq \infty, 0, -1, 1, i, -i \).
Excluding the images of the six vertices of the regular octahedron \[ \infty, \ 0, \ 1, \ -1, \ i, \ -i \]

‘Edwards’ elliptic curves’ for real \( a \): branch-cover \( S^2 \) over the images

\[ a, \ -a, \ \frac{1}{a}, \ -\frac{1}{a} \]

of the four vertices from the ‘arakarum’

Interpret \( a \) via (‘Euclidean’) length of (‘hyperbolic’) hypotenuse.
Euler, Lenstra, Hartshorne-van Luijk and K3 surfaces

Hendrik Lenstra to Hartshorne (2008): ‘rational solutions to the multiplicative non-Euclidean Pythagorus equation are equivalent to rational solutions to a problem of Euler on rational cuboids: Find $x^2, y^2, z^2$ such that the differences

\[ x^2 - y^2 = t^2, \quad x^2 - z^2 = u^2, \quad y^2 - z^2 = v^2 \]

are all squares.’

Hartshorne-van Luijk 2008: Equations give a projective algebraic variety in $\mathbb{C}P^5$: this is a K3-surface. They show, using results of Euler, that the set of rational points is dense.

(Elliptic curves; K3-surfaces; Calabi-Yau 3-folds; . . . :
Classification of 1-, 2-, 3-complex-dimensional complex Kähler manifolds, trivial canonical class: Calabi-Yau spaces, admit Ricci-flat metrics (Yau))
Marvin Greenberg (2010):

‘Hilbert gets the credit for the main ideas in the foundations of plane hyperbolic geometry without real numbers, but he only sketched much of what needed to be done. The details were worked out by others as described in the introduction to Pambuccian; the best exposition of those details is Hartshorne, where a remarkable new hyperbolic trigonometry without real numbers is presented. Using it, all arguments in other treatises using classical hyperbolic trigonometry can be rephrased so as to avoid their apparent dependence on real numbers.’

‘I conjectured and Hartshorne proved that a segment in a hyperbolic plane is constructible from that initial data if and only if Hartshorne’s multiplicative length of that segment is a constructible number in the field of ends based on that data. That multiplicative length is a key discovery which Hartshorne and Van Luijk have applied to algebraic geometry and number theory.’
Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization.

The use of elliptic curves in cryptography was suggested independently by Neal Koblitz and Victor S. Miller in 1985. Elliptic curve cryptography algorithms entered wide use in 2004 to 2005. The algorithm was approved by NIST in 2006. In 2013, the New York Times revealed that Dual Elliptic Curve Deterministic Random Bit Generation (or Dual–EC–DRBG) had been included as a NIST national standard due to the influence of NSA, which had included a deliberate weakness in the algorithm.
8-pointed ‘Star of Ishtar’, ‘contemporary’ uses on flags

(a) Eureka Flag 1854; (b) Iraqi Flag 1958-1963; (c) Maori flag 1834

(a) 1854 Eureka Stockade, opposition to Victoria gold rush miner’s tax
(b) 1958 – 1963: General Qasim deposed the Western-allied Iraqi monarchy imposed by the British in 1921 – until CIA supported Saddam Hussein’s Ba’ath Party 1963 coup.
(c) Unofficial United Tribes of New Zealand flag, as used by Maori today and as per Busby’s original description of the flag. (cf 8-pointed star for Venus at Te Papa Maori cosmology audio-visual display in Wellington)

**Conclusion:**

STAR OF ISTHAR ASSOCIATED WITH TROUBLE MAKING!