Sobre la mitjana aritmètico-geomètrica.

I. AGM:

$a, b > 0$; $a_0 := a$, $b_0 := b$ i definim $a_{n+1} := \frac{a_n + b_n}{2}$, $b_{n+1} := +\sqrt{a_n b_n}$

suposem $\boxed{b<a}$

Th: $(a_n)_n$, $(b_n)_n$ són adjacents, i.e. $0 \leq b_n \leq b_{n+1} \leq a_{n+1} \leq a_n$

- $a_{n+1} - b_{n+1} = \frac{(\sqrt{a_n} - \sqrt{b_n})^2}{2} = \frac{(a_n - b_n)^2}{2(\sqrt{a_n}+\sqrt{b_n})^2} \leq \frac{(a_n-b_n)^2}{8\, b_0}$

Per tant es té convergència quadràtica.

$M(a,b)$ és la mitjana arit.-geom. de a i b:

$$\exists C_{a_0,b_0} : \ |a_n - M(a,b)| \leq C\,|a_{n-1} - M(a,b)|^2$$

Observem que si fem dos passos a cada iteració, obtindrem convergència quàrtica! (i així tants cops com vulguem).

Borwein: AGM quàrtica: $\alpha_n := \sqrt{a_{2n}}$, $\beta_n := \sqrt{b_{2n}}$, aleshores

$$\alpha_{n+1} = \frac{\alpha_n + \beta_n}{2} \qquad \beta_{n+1} = \frac{(\alpha_n^3 \beta_n + \alpha_n \beta_n^3)^{1/4}}{2}$$

Propietats:

- $M(\lambda a, \lambda b) = \lambda M(a,b) \quad \forall \lambda > 0$
- $M\left(\frac{a+b}{2}, \sqrt{ab}\right) = M(a,b)$

Es comença a estudiar a partir de Lagrange (1784) i Gauss (1791).

Podem considerar $a, b \in \mathbb{C}$, però aleshores hem d'escollir amb més cura l'$\sqrt{\ }$.

Def: La "bona elecció" de l'arrel quadrada és aquella tal que:

$$|a_{n+1} - b_{n+1}| \leq |a_{n+1} + b_{n+1}| \quad \text{i tal que} \quad \mathrm{Im}\left(\frac{b_{n+1}}{a_{n+1}}\right) > 0$$

Per veure que està ben definida, observem que, si $\mathrm{Im}\left(\frac{b_{n+1}}{a_{n+1}}\right) = 0$, aleshores es té:

$$0 \leq \|a_{n+1} - b_{n+1}\| = (a_{n+1} - b_{n+1})(\overline{a_{n+1}} - \overline{b_{n+1}}) = a_{n+1}\overline{b_{n+1}} + \overline{a_{n+1}}\, b_{n+1} \Rightarrow \mathrm{Re}\left(\frac{b_{n+1}}{a_{n+1}}\right) \geq 0$$

Th (Gauss): $a,b\in\mathbb{C}$, $a_0=a$, $b_0=b$, aleshores les successions $(a_n)_n$, $(b_n)_n$ convergeixen i $\lim a_n = \lim b_n = M$, i $M\neq 0 \iff$ s'ha fet ~~elecció~~ incorrecta només un nombre finit de vegades.

Lema: Si b_{n+1} es fa amb elecció correcta,

i) $|a_{n+1}-b_{n+1}| < \dfrac{|a_n-b_n|}{2}$

ii) $\left|\mathrm{Arg}\left(\dfrac{b_{n+1}}{a_{n+1}}\right)\right| \leq \dfrac{1}{2}\left|\mathrm{Arg}\left(\dfrac{b_n}{a_n}\right)\right|$

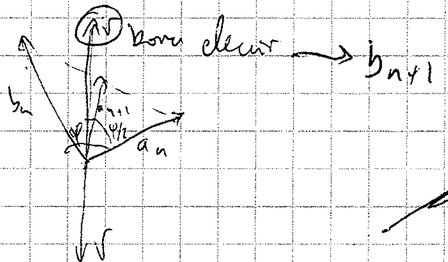
Pf

(i) $a_{n+1}^2 - b_{n+1}^2 = \left(\dfrac{a_n+b_n}{2}\right)^2 - a_nb_n = \dfrac{(a_n-b_n)^2}{4}$

$\parallel$

$(a_{n+1}-b_{n+1})(a_{n+1}+b_{n+1})$ i si $|a_{n+1}-b_{n+1}| \leq |a_{n+1}+b_{n+1}|$ ja està.

(ii) Notem que si $|a_{n+1}-b_{n+1}| \leq |a_{n+1}+b_{n+1}|$, aleshores $\mathrm{Arg}(a_{n+1},b_{n+1}) \leq \pi/2$



Dem del Theorem:

a) Suposem que hem fet ∞ vegades la mala elecció i considerem les succ. $(a_n),(b_n)$

$M_n := \sup(|a_n|,|b_n|)$ $\quad (M_n \to 0 ?)$

$|a_{n+1}-b_{n+1}| \geq |a_{n+1}+b_{n+1}| \Rightarrow |a_{n+2}| = \left|\dfrac{a_{n+1}+b_{n+1}}{2}\right| \leq \dfrac{1}{4}|a_n-b_n| \leq \dfrac{M_n}{2}$ (males eleccions)

pq $|a_{n+1}+b_{n+1}| \leq \frac{1}{2}|a_n-b_n|$

$|b_{n+1}| \leq M_{n+1} \leq M_n$

$|a_{n+3}| \leq \dfrac{3}{4}M_n$; $|b_{n+3}| \leq \dfrac{\sqrt{2}}{2}M_n \Rightarrow M_{n+3} \leq \dfrac{3}{4}M_n \Rightarrow M_n \to 0$

b) Suposem que $\forall n$ s'ha escollit correctament (descartant uns quants termes al començament).

Podem suposar també que $|\mathrm{Angle}(a_0,b_0)| < \pi$

$|a_n-b_n| \leq \dfrac{|a_{n-1}-b_{n-1}|}{2} \Rightarrow a_n-b_n \to 0$

Veurem que (a_n) és de Cauchy, i aleshores a_n convergirà (i b_n també haurà de convergir)

$|a_{n+1}-a_n| = \left|\dfrac{a_n+b_n}{2}-a_n\right| = \left|\dfrac{a_n-b_n}{2}\right| \leq \dfrac{1}{2^{n+1}}|a_0-b_0|$ i aleshores $|a_{n+k}-a_n| \leq \frac{1}{2^n}|a_0-b_0|$

Per tant podem anomenar $M = \lim a_n = \lim b_n$.

Suposem $M=0$. Aleshores $a_{n+k} \xrightarrow[k]{} 0$, i per tant

$$|a_n| \leq \frac{1}{2^n}|a_0 - b_0|,$$ ~~que contradiu que hagues~~

Escrivim $m_n = \inf(|a_n|, |b_n|)$. Volem veure que $m_n \neq 0$.

$|b_{n+1}| \geq m_n$

$$|a_{n+1}|^2 = \left|\frac{a_n+b_n}{2}\right|^2 = \frac{1}{4}\left(|a_n|^2 + |b_n|^2 + 2|a_n||b_n|\cos \underset{\pi/2}{\theta_n}\right) \geq \frac{1}{4}\cdot 2 m_n^2 \cos^2\frac{\theta_n}{2}$$

Per tant $|a_{n+1}| \geq m_n \cos\frac{\theta_n}{2}$, i així $\Rightarrow a_{n+1} \geq m_n \cos\frac{\theta_n}{2} \geq m_0 \prod_{n\geq 1}\cos\frac{\theta_n}{2}$

[Sabem que $\prod_{n\geq 1}\cos\frac{\theta}{2^n} = \frac{\sin\theta}{\theta}$, ja que $\left(\sin\theta = 2\sin\frac{\theta}{2}\cos\frac{\theta}{2} = 2^2\sin\frac{\theta}{4}\cos\frac{\theta}{4}\cos\frac{\theta}{2}\ldots = 2^n \sin\frac{\theta}{2^n}\prod_{k\leq n}\cos\left(\frac{\theta}{2^k}\right) \Rightarrow \frac{\sin\theta}{\theta}\right)$ ok.]

Per $\theta = \frac{\pi}{2}$, obtenim $\boxed{\frac{2}{\pi} = \frac{\sqrt{2}}{2}\cdot\frac{\sqrt{2+\sqrt{2}}}{2}\cdot\frac{\sqrt{2+\sqrt{2+\sqrt{2}}}}{2}\cdots}$ (1593, Viete).

//

Considerem ara el conjunt $L = \left\{\frac{1}{M(a,b)} \text{ possibles}\right\}$ (per $a, b \in \mathbb{C}$ fixats).

__Teorema:__

$\lambda :=$ el límit "més senzill", sempre fent la bona elecció.

$\mu :=$ el límit "més senzill" dels $M(a+b, a-b)$.

Aleshores $L = \frac{1}{\lambda} + 4\left[\mathbb{Z}\frac{1}{\lambda} + \mathbb{Z}\frac{i}{\mu}\right]$.

II. 2-isogènies de corbes el·líptiques.

1) Recordem que
$$\underset{\substack{y^2=f(x)\\ \omega_E = \frac{dx}{y}}}{E} \xrightarrow{\varphi} \underset{\substack{Y=F(X)\\ \omega_{E'} = \frac{dX}{Y}}}{E'} \qquad \varphi(x,y) = (X(x), y\,u(x))$$
on $u(x) = \frac{1}{\lambda}X'(x)$

$(\varphi^*(\omega_{E'}) = \lambda\omega_E)$.

2) Sigui E amb un punt d'ordre 2, que suposarem que és $\underset{P_0}{(0,0)}$. Per tant,

$$y^2 = x(x^2+ax+b)$$

a) La translació per P_0; $P \mapsto P_0 + P$ té equació: $(x,y) \mapsto \left(\frac{b}{x}, \frac{-b}{x^2}y\right)$

b) La multiplicació per 2, ve donada per $(x,y) \mapsto \left(\frac{(x^2-b)^2}{4y^2}, y\frac{X'(x)}{2}\right)$

$$E \xrightarrow{\varphi} F = E/\langle(0,0)\rangle$$

$y^2 = x(x^2+ax+b)$ $\qquad$ $y^2 = x(x^2-2aX+a^2-4b)$ $\qquad$ $\varphi:(x,y)\longmapsto\left(\cancel{x}-\dfrac{x^2+ax+b}{x},\ \dfrac{X'(x)}{2y}\right)$

$(\varphi^*(\omega_F) = 2\omega_E)$

Remarques: Si $E(\mathbb{R})$ és connexa (i.e. E té un sol punt ~~real~~ d'ordre 2), i.e. $a^2-4b<0$

alehores $F(\mathbb{R})$ té tres punts d'ordre 2.

(i.e. $a^2-(a^2-4b)=4b$ és $\square$, i.e. b és un quadrat).

El que diu la remarca és que si $a^2-4b<0$, alehores $b>0$ (i.e. $\square$).

Donats (a,b), $E_{a,b} := y^2 = x(x+a^2)(x+b^2)$

Si considerem ara $a_1 := \frac{a+b}{2}$, $b_1 := \sqrt{ab}$ (i.e. $b_1^2 = ab$). $E_{a_1,b_1}: y_1^2 = x_1(x_1+a_1^2)(x_1+b_1^2)$

$$E_{a,b} \xrightarrow{f_1} E_{a_1,b_1}$$

$$(x,y) \longmapsto \left(\frac{(x-ab)^2}{4x},\ \frac{X'(x)}{2}y\right) \qquad \begin{cases} f_1^*(\omega_{E_1}) = 2\omega_E \\ g_1^*(\omega_E) = \omega_{E_1}\end{cases}$$

$$\left(\frac{x(x+b_1^2)}{x+a_1^2}, X(x)y\right) \xleftarrow{\ g_1\ } (x_1, y_1)$$

$\operatorname{Ker} g_1 = \langle(-a_1^2, 0)\rangle$

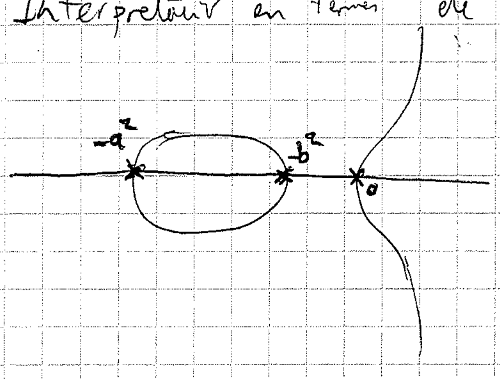
Remarques:

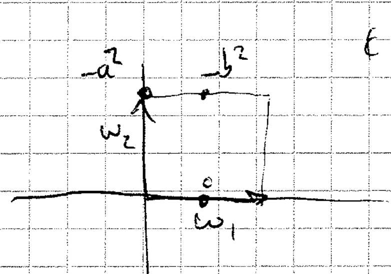
1) Per $x=ab$, $y^2 = ab(ab+a^2)(ab+b^2) = (ab(a+b))^2$. Per tant, tenim un altre punt racional: $P=(ab,\ ab(a+b))$ és d'ordre 4, i $2P=(0,0)$.

2) $j(E_{a,b}) = 256\dfrac{(a^4-a^2b^2+b^4)^3}{a^4b^4(a^2-b^2)^2}$

Si escrivim $t := b/a$, $j = 256\dfrac{(1+t^2+t^4)^3}{t^4(t^2-1)^2}$

3) Interpretació en termes de reticles:





Aleshores E_{a_1,b_1} té, com a retícle de períodes, $\langle \omega_1, 2\omega_2 \rangle$

$$f : E_{a,b} \longrightarrow E_{a_1,b_1}$$
$$z \longmapsto 2z$$
$$z \longleftarrow z$$

III Integrals el·líptiques.

$$I(a,b) := \int_0^{\pi/2} \frac{d\theta}{\sqrt{a^2\cos^2\theta + b^2\sin^2\theta}} \qquad a,b \in \mathbb{R}.\ (b \leq a) \quad (\text{integral de } 1^a \text{ espècie})$$

$$J(a,b) := \int_0^{\pi/2} \sqrt{a^2\cos^2\theta + b^2\sin^2\theta}\, d\theta \qquad a,b \in \mathbb{R} \quad (b \leq a) \quad (\text{integral de } 2^a \text{ espècie}).$$

Si $\boxed{t = b\,\mathrm{tg}\,\theta}$, $I(a,b) = \int_0^\infty \frac{dt}{\sqrt{(t^2+a^2)(t^2+b^2)}}$

Si $\boxed{t = \cos\theta}$, $\int_0^1 \frac{dt}{\sqrt{1-t^4}} = I(\sqrt{2}, 1)$

Si $\boxed{t = \sin\theta}$, $I(a,b) = \int_0^1 \frac{dt}{\sqrt{(1-t^2)(a^2-c^2t^2)}}$ on $c = \sqrt{a^2-b^2}$

Def: $0 < k < 1$; $k' = \sqrt{1-k^2}$

$$K(k) := I(1,k') = \int_0^{\pi/2} \frac{d\theta}{\sqrt{1-k^2\sin^2\theta}} = \int_0^1 \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}$$

$$E(k) = J(1,k') = \int_0^{\pi/2} \sqrt{1-k^2\sin^2\theta}\, d\theta = \int_0^1 \sqrt{\frac{1-k^2t^2}{1-t^2}}\, dt$$

$$K'(k) := K(k') \ ; \ E'(k) := E(k')$$

Observem que $I(a,b) = \frac{1}{a} K\left(\sqrt{1-\left(\frac{b}{a}\right)^2}\right) = \frac{1}{a} K'\left(\frac{b}{a}\right)$

$$x = -a^2 + \overbrace{(a^2-b^2)}^{c^2}\sin^2\theta \ ; \ dx = 2c^2\sin\theta\cos\theta\, d\theta = 2c^2\sqrt{-\frac{(x+a^2)(x+b^2)}{c^4}} = 2\sqrt{-(x+a^2)(x+b^2)}$$

$$I(a,b) = \int_0^{\pi/2} \frac{d\theta}{\sqrt{a^2\cos^2\theta + b^2\sin^2\theta}}$$

$$a^2\cos^2\theta + b^2\sin^2\theta = -a^2\frac{x+b^2}{c^2} + b^2\frac{x+a^2}{c^2} = \frac{(b^2-a^2)x}{c^2} = -x$$

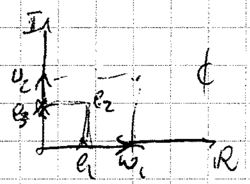
Per tant, fent el canvi, $I(a,b) = \frac{1}{2}\int_{-a^2}^{-b^2} \frac{dx}{\sqrt{x(x+a^2)(x+b^2)}} = \frac{1}{2}\int_{-a^2}^{-b^2} \frac{dx}{y}$

$$J(a,b) = \int_0^{\pi/2} \sqrt{}\, d\theta = \frac{1}{2}\int_{-a^2}^{-b^2} x\,\frac{dx}{y} \qquad \text{on } y^2 = x(x+a^2)(x+b^2)$$

Per tant $2I(a,b) = \int_{-a}^{-b^2} \omega$; $2J = \int x\,\omega$

Com que una translació des de $(-a^2,0)$ no canvia els diferencials

$$2I(a,b) = \int_0^{\infty} \frac{dx}{y}$$



Sigui $E \simeq \mathbb{C}/\Gamma$, $\Gamma = \langle \omega_1, \omega_2 \rangle$

$$X = \wp(z) = \frac{1}{z^2} + \sum_{\gamma\in\Gamma'} \frac{1}{(z-\gamma)^2}, \quad Y = \wp'(z)$$

$$\omega = dz = \frac{dX}{2Y} \longrightarrow Y^2 = 4X^3 - g_2 X - g_3 = 4(X-e_1)(X-e_2)(X-e_3)$$

$$\omega_1 = 2\int_0^{\omega_1/2} dz = 2\int_0^{e_1} \frac{dX}{\sqrt{4X^3 - g_2X - g_3}}$$

$I(a,b) = \omega_1$, període real de $E(a,b)$.

Com que $x(x+a^2)(x+b^2) = y^2$, $\quad c = \sqrt{a^2-b^2}$

$$x' = x + a^2 \rightsquigarrow y^2 = x'(x'-a^2)(x'+b^2-a^2) = x'(x'-a^2)(x'-c^2)$$

$$y^2 = X(X+a^2)(X+c^2) \qquad (\text{fent } X = -x').$$

Per tant $\omega_2 = i\, I\left(a, \sqrt{a^2-b^2}\right)$.

$$K(k) = \int_0^{\pi/2} \frac{d\theta}{\sqrt{1-k^2\sin^2\theta}} \qquad \left(K(0) = \frac{\pi}{2}\right)$$

$9!! = 1\cdot 3\cdot 5\cdot 7\cdot 9$

Es pot desenvolupar com $K(k) = \dfrac{\pi}{2} \displaystyle\sum_{i=0}^{+\infty} \left(\frac{(2i-1)!!}{2^i\, i!}\right)^2 k^{2i}$

També, per $E(k)$:

$$E(k) = \frac{\pi}{2}\left(1 - \sum_{i=1}^{\infty} \left(\frac{(2i-1)!!}{2^i\, i!}\right)^2 \frac{k^{2i}}{2i-1}\right)$$

Es defineix la funció hipergeomètrica (Gauss, 1812): $F(a,b,c,z) := 1 + \dfrac{ab}{1\cdot c} z + \dfrac{a(a+1)b(b+1)}{1\cdot 2\cdot c(c+1)} z^2 + \dots$

i aleshores:

$$K(k) = \frac{\pi}{2} F\left(\frac12, \frac12, 1, k^2\right), \quad E(k) = \frac{\pi}{2} F\left(-\frac12, \frac12, 1, k^2\right).$$

Aleshores $F(a,b,c,z)$ és solució de:

$$z(1-z)y'' + \left(c-(a+b+1)z\right)y' - aby = 0$$

També, $K(k)$ és solució de

$$(k^3-k)y'' + (3k^2-1)y' + ky = 0$$

També $K'(k)$ $\left(=K(k')\right)$ és solució de la mateixa equació integral.

Es sap que
$$K'(k) = \frac{2}{\pi}K(k)\log\frac{4}{k} - 2\left[\left(\frac{1}{2}\right)^2\frac{1}{1\cdot 2}k^2 + \left(\frac{1\cdot 3}{2\cdot 4}\right)^2\left(\frac{1}{1\cdot 2}+\frac{1}{3\cdot 4}\right)k^4 + \cdots\right]$$

$$\left|K'(k) - \log\frac{4}{k}\right| \le 10\left|k^2\log k\right|$$

També es pot veure (molt fàcil) que:

$$\dot{E}(k) = \frac{dE}{dk} = \frac{E-K}{k} \quad ; \quad \dot{K}(k) = \frac{dK}{dk} = \frac{E-k'^2K}{k\,k'^2}$$

Relació de Legendre:

$$\varphi(k) = K'E + KE' - KK' = \frac{\pi}{2}.$$

$\varphi'(k) = \cdots = 0 \Rightarrow \varphi$ és constant en $(0,1)$. I per $k\to 0$ es pot fer el límit.

(Legendre ho havia demostrat per $k=\frac{\sqrt{3}-1}{8}, \ldots$).

- D'on ve l'estudi de les integrals el·líptiques?

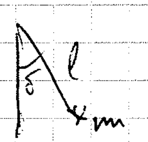
- L'el·lipse $\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$.

fent $x = a\cos\theta$, $y = b\sin\theta$

Volem calcular el perímetre de l'el·lipse: $\int_0^{\pi/2}\sqrt{(x')^2+(y')^2}\,dx = 4J(a,b)$

- La corba $y=\sin x$

$$L = 4J(\sqrt{2},1).$$



$$\frac{1}{2}mv^2 = \Delta E_p.$$

$$\frac{1}{2}m(\ell\dot{\theta})^2 = m\ell(\cos\theta - \cos\gamma) = 2mg\ell\left(\sin^2\frac{\delta}{2} - \sin^2\frac{\theta}{2}\right)$$

Per tant
$$t = \int_0^{\Phi} dt = 2\sqrt{\frac{\ell}{g}}\int_0^{\Phi}\frac{d\theta}{\sqrt{\sin^2\frac{\delta}{2}-\sin^2\frac{\theta}{2}}}$$

s'anomenen integrals incompletes.

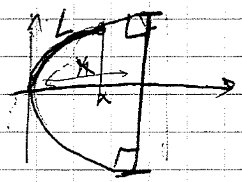
temps per anar de 0 (repòs) fins a un angle determinat

$$T = 4\int_0^{\delta} dt = 2\sqrt{\ell/g}\int_0^{\delta}\frac{d\theta}{\sqrt{\ }}$$

Si fem el canvi $\sin\varphi = \dfrac{\sin \theta/2}{\sin \delta/2}$, aleshores

$$T = 4\sqrt{\ell/g}\int_0^{\pi/2}\frac{d\varphi}{\sqrt{1-\sin^2\frac{\delta}{2}\sin^2\varphi}} = 4\sqrt{\ell/g}\; I\left(1,\cos\frac{\delta}{2}\right)$$

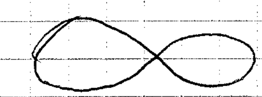
- Corba elàstica: Jacob Bernoulli (1961)



$$y = \int_0^x \frac{t^2\,dt}{\sqrt{1-t^4}} \qquad L = \int_0^x \frac{dt}{\sqrt{1-t^4}}$$

El 1694, ell mateix va descriure la <u>lemniscata</u>, que és una corba algebraica amb la mateixa llargada que la primera (rectificació).

$r = \sqrt{\cos 2\theta}$ (polars) Complex $(x^2+y^2)^2 = x^2-y^2$



Es ~~va~~ introduir les funcions sinus lemniscat i cosinus lemniscat

$$\left.\begin{aligned} sl\left(\int_0^x \frac{dt}{\sqrt{1-t^4}}\right) &= x \\ cl\left(\int_x^1 \frac{dt}{\sqrt{1-t^4}}\right) &= x \end{aligned}\right\} \quad cl(\alpha) = sl\left(\frac{\varpi}{2}-\alpha\right) \quad \text{on } \varpi := 2\int_0^1 \frac{dt}{\sqrt{1-t^4}}$$

- $sl^2 + cl^2 + sl^2\,cl^2 = 1$
- $sl(x+x') = \dfrac{sl(x)\,cl(x') + sl(x')\,cl(x)}{1 - sl(x)\,cl(x')\,sl(x')\,cl(x)}$

$$\boxed{\int_0^1 \frac{t^2\,dt}{\sqrt{1-t^4}}\int_0^1 \frac{dt}{\sqrt{1-t^4}} = \frac{\pi}{4}}$$ <u>Euler</u>

Si considerem $\displaystyle\int_0^a \frac{dx}{\sqrt{g(x)}} + \int_0^b \frac{dx}{\sqrt{g(x)}} = \int_0^c \frac{dx}{\sqrt{g(x)}}$ amb $g(x) = (1-x^2)(1-k^2x^2)$

Aleshores $c = \dfrac{b\sqrt{g(a)} + a\sqrt{g(b)}}{\sqrt{1-k^2a^2b^2}}$

Funcions Θ

Sigui τ, $\mathrm{Im}(\tau) > 0$.

$$\Theta(z,\tau) := \sum_{n\in\mathbb{Z}} e^{\pi i n^2 \tau + 2\pi i n z} \qquad q := e^{\pi i \tau},$$

Llavors definim
$$P = \Theta(0,\tau) = \sum_n q^{n^2} = 1 + 2q + \cdots$$
$$Q = \Theta(\tfrac{1}{2},\tau) = \sum_n (-1)^n q^{n^2}$$
$$R = \sum q^{(n+\frac{1}{2})^2} = q^{-\frac{1}{4}}\,\Theta\left(\frac{\tau}{2},\tau\right)$$

És fàcil $P^2(q^2) = \dfrac{P^2(q)+Q^2(q)}{2}$ i $Q^2(q^2) = \sqrt{P(q)Q(q)}$.

P.ex per veure la primera igualtat,
$$\frac{1}{2}\sum_{n,m} q^{n^2+m^2}\left(1+(-1)^{m+n}\right) = \sum_{a,b} q^{2(a^2+b^2)} \quad \text{(elemental).}$$

Suposem ara $|q|<1$. Fixem-lo $q = q_0$.

$a_0 = P^2(q)$ i $a_n = P^2(q^{2^n})$
$b_0 = Q^2(q)$ $\quad b_n = P^2(q^{2^n})$ obtenim, per les fórmules anteriors, que són la successió AGM.

A més, $a_n, b_n \longrightarrow 1$ i $a_n - b_n \sim O(q^{2^n})$

$$M(P^2(q), Q^2(q)) = 1$$

Recordem que havíem definit $c_n^2 = a_n^2 - b_n^2$. Llavors
$$P^4(q) = Q^4(q) + R^4(q), \text{ i per tant } c_n = R^2(q^{2^n})$$

És complex

$$I(a,b) = \frac{\pi}{2M(a,b)} \text{ i això} \Rightarrow \text{que } K(k) = \frac{\pi}{2M(1,k')} \quad \text{(1a espècie)}$$

$$E(k) = \frac{\pi}{2M(1,k')}\left(1 - \sum_{k=0}^{\infty} 2^{n-1} c_n^2\right) \quad \text{(segona espècie)}$$

Demostració geomètrica (1818, Gauss). Un canvi de variables que porta $I(a_n,b_n) \longrightarrow I(a_{n+1},b_{n+1})$.

$E_0 = E(a_0,b_0) \qquad y^2 = x(x+a_0^2)(x+b_0^2) \qquad \omega_i = \frac{dx_i}{y_i}$ complex?

$\uparrow\varphi_1 \qquad \downarrow\psi_1$

$E_1 = \qquad y_1^2 = x_1(x_1+a_1^2)(x_1+b_1^2) \qquad \varphi_i^*(\omega_{i-1}) = \omega_i$

$\vdots$

$E_n \qquad \uparrow\varphi_n \qquad \downarrow\psi_n$

$$\int_0^{+\infty}\omega_i = \int_0^{+\infty}\omega_{i-1} = \dots = \int_0^{+\infty}\omega_0 = I(a_0,b_0)$$

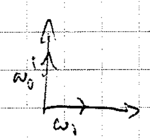
$\downarrow$

$$E_\infty = y^2 = x(x+M^2(a,b))^2 \rightsquigarrow \int_0^\infty \frac{dx}{\sqrt{x}\,(x+M^2)} = \int_0^{+\infty}\frac{2u\,du}{u(u^2+M^2)} =$$

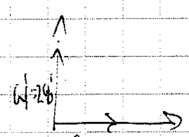
$$= \frac{1}{M}\int_0^\infty \frac{2\,du}{u^2+1} = \frac{\pi}{M}$$

Per tant podem calcular la integral a partir de M.

• Reticles:



corresponents a $E(a_0,b_0)$



$E_1 = E(a_1,b_1)$

En general, $E_n \cong \dfrac{\mathbb{C}}{\langle \omega_0, 2^n\omega_0' \rangle}$

• En termes de funcions Θ:

$\omega_1 = \int_0^\infty \frac{dx}{y} = \frac{\pi}{M(a,b)}$ Volem $a = \alpha P^2(q)$, $b = \alpha Q^2(q)$ amb $\alpha = M(a,b)$

$q = e^{i\pi\tau}$

$\omega_2 = \frac{\pi}{M(a,c)} \qquad c = \sqrt{a^2-b^2}. \qquad \boxed{\frac{\omega_2}{\omega_1} = \tau} \stackrel{?}{=} \frac{M(a,b)}{M(a,c)}$

Gauss, més tard (1818) tornà a la AGM per culpa d'un problema d'astronomia. Volia calcular el desenvolupament en sèrie Fourier de

$$\frac{1}{\sqrt{1+\mu\cos^2 t}} = A_0 + A_1\cos t + A_2\cos 2t + \dots$$

i resulta que $A_0 = \frac{2}{\pi}\int_0^{\pi/2}\frac{dt}{\sqrt{1+\mu\cos^2 t}} = \frac{1}{M(1+\mu,1)}$

Va provar que $M\left(1+\frac{2t}{1+t^2}, 1-\frac{2t}{1+t^2}\right) = \frac{M(1+t^2,1-t^2)}{1+t^2}$

Es pot provar que $2J(a_{n+1},b_{n+1}) = J(a_n,b_n) - a_n b_n I(a_n,b_n)$

i això és equivalent al lema:

Lema: $\displaystyle\int_{-a^2}^{-b^2}\frac{x\,dx}{y} = -a^2b^2\int_{-a^2}^{-b^2}\frac{1}{x}\frac{dx}{y}$ (on $y^2 = x(x+a^2)(x+b^2)$).

Dem: Es fa un canvi de variables $P \longmapsto P+(0,0)$, $x \longmapsto \frac{a^2b^2}{x}$

Donada una corba el·líptica, i donat $P=(x,y)$ sobre la corba, volem saber quan val $\frac{z}{\omega_1}$ (ω_1 és el vector del reticle).

$\frac{z}{\omega_1} = 0,\ \overset{y>0}{1}\ \underset{y<0}{0}\ \dots$ a cada iteració un bit. ← mètode de Zagier.

· Càlcul de π. (Mètode de Gauss, (Brent, Salamin)).

$k = \frac{\sqrt2}{2} = k'$.

Per la fórmula de Legendre, $2KE - K^2 = \frac{\pi}{2}$.

$$K = \frac{\pi}{2M(1,\frac{\sqrt2}{2})} \quad \text{i} \quad E = K\Big(1 - \sum_{i\geq 1} 2^{i-1}c_i^2\Big)$$

$$\frac{\pi^2}{4M^2}\Big(2 - \sum_{i\geq1} 2^i c_i^2\Big) = \frac{\pi}{2} \Rightarrow \pi = \frac{2M^2(1,\frac{\sqrt2}{2})}{1-\sum_{i\geq 1}^{\infty} 2^i c_i^2}$$

Altures:

$E/\mathbb{Q}$. Fix h_v, $h: E(K) \longrightarrow \mathbb{R}$. $h(P) = \sum h_v(P)$.

La part més delicada de calcular és $h_\infty(P) = \lambda_\infty(P)$.

funcions el·líptiques

constants (i conegudes)

Si identifiquem $\begin{array}{l} E \longleftrightarrow \mathbb{C}/\Lambda \\ P \longmapsto z \end{array}$, $\lambda_\infty(P) = -\log\left|e^{-\frac{1}{2}z\eta(z)}\sigma(z)\Delta^{1/12}(z)\right|$

λ_∞ és una funció tal que: $\lambda_\infty : E(\mathbb{C}) \to \mathbb{R}$

i) $|\lambda_\infty(z) - \log z|$ és afitat.

ii) $\lambda_\infty(z+z') + \lambda_\infty(z-z') = 2\lambda_\infty(\overset{z}{P}) + 2\lambda_\infty(\overset{z'}{Q}) + \log|x(\overset{z}{P}) - x(\overset{z'}{Q})| - \frac{1}{2}\log|\Delta|$

A més, λ_∞ queda únicament determinada per aquestes dues propietats.

$$\begin{array}{ll} E_0: & y^2 = x(x+a_0^2)(x+b_0^2) \\ f_1 \downarrow \uparrow g_1 & \\ E_1: & y^2 = x(x+a_1^2)(x+b_1^2) \\ f_n \downarrow \uparrow g_n & \\ E_n: & y^2 = x(x+a_n^2)(x+b_n^2) \\ f_n \downarrow \uparrow g_n & \\ E_\infty: & y^2 = x(x+M)^2 \end{array}$$

$f_n^*(\omega_n) = 2\omega_{n-1}$

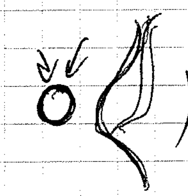
$g_n^*(\omega_{n-1}) = \omega_n$

(recordatori)

Considerem $\mu(P) := \lambda(P) + \frac{1}{12}\log|\Delta|$

Si $P_0 = g_1(P_1)$, aleshores:

$$\boxed{\mu_0(P_0) = 2\mu_1(P_1) - \frac{1}{2}\log|x_1(P_1) + a_1^2|}$$

Partim de $P_0 \in E_0^c(\mathbb{R})$ (la component connexa de E_0 )

Utilitzant les isogènies f_n, arribem a $P_\infty \in E_\infty$.

$$x_{n+1} = \frac{1}{2}\left(x_n - a_n b_n + \sqrt{(x_n+a_n^2)(x_n+b_n^2)}\right)$$

Com que $n \to \infty \Rightarrow P_n = P_{n+1}$,

$$\mu_\infty(P_\infty) = \frac{1}{2}\log|x_\infty(P_\infty) + M^2|$$

$$\mu(P) = \frac{1}{2}\log\lim \frac{(x_n+a_n^2)^{2^{n-1}}}{\prod_{k=1}^{n-1}(x_k+a_k^2)^{2^{k-1}}}$$

- Aplicació de l'AGM al càlcul de capacitats d'una unió d'intervals.

Sigui $K \neq \emptyset$ un compacte de $\mathbb{C}$.

$\exists!\ g_K : \mathbb{C} \longrightarrow \mathbb{R}$ contínua tal que:

i) $g_{|K} \equiv 0$

ii) $g(z) - \log|z|$ és afitada per $z \to \infty$.

iii) $g_{|\mathbb{C}\setminus K}$ és harmònica.

La funció g_K s'anomena potencial d'equilibri de K.

Propietats:

- $g_K(\mathbb{C}) \subseteq \mathbb{R}^+$
- $\exists\, U \ni 0$ i $h : U \longrightarrow \mathbb{R}$ harmònica en U, tal que $g(z) - \log|z| = h\left(\frac{1}{z}\right)$
- $\lim (g_K(z) - \log|z|) = h(0)$ (existeix) i s'anomena $r(K)$

  S'anomena la constant de Robin de K.

Df: La capacitat de K és $e^{-r(K)}$ i s'escriu $c(K)$

Df: $\delta_n(K) := \sup_{z_1,\dots,z_n \in K} \left\{ \prod_{1 \leq i < j \leq n} |z_i - z_j| \right\}^{\frac{2}{n(n-1)}}$ és el diàmetre d'ordre n.

$\delta_\infty(K) := \lim_{n\to\infty} \delta_n(K)$ és el diàmetre transfinit de K.

Th: $\delta_\infty(K) = c(K)$.

Exemple 1: $K = B(0,r)$. $g_K(z) = \begin{cases} 0 & z \in K \\ \log \frac{|z|}{r} & \end{cases}$

$r(K) = -\log r$

$\boxed{c(K) = r}$

Exemple 2: $K = [a,b] \subset \mathbb{R}$. $g_K(z) = \log\left|\frac{1}{2}\left(z - \frac{a+b}{2} + \sqrt{(z-a)(z-b)}\right)\right| - \log\frac{b-a}{4}$

on si $z = \rho e^{i\theta}$, $-\pi < \theta < \pi$, $\sqrt{z} = \sqrt{\rho}\, e^{i\frac{\theta}{2}}$

$r(K) = -\log\frac{b-a}{4}$, $\boxed{c(K) = \frac{b-a}{4}}$

Si el K és unió finita d'intervals, en general no hi ha una fórmula tancada per la funció g_K, per tant haurem d'utilitzar el diàmetre transfinit.

L'AGM es pot utilitzar per generalitzar aquests conceptes.

Sigui X una superfície compacta de Riemann, K un compacte no buit de X, D un divisor de X, $\underbrace{Supp(D)}_{|D|} \cap K = \phi$

$\exists !\, g_{K,D} : X \setminus |D| \longrightarrow \mathbb{R}$ contínua, nul·la sobre K, harmònica en $X - K \setminus |D|$ i tal que $\forall$ U obert connex, $U \cap K = \phi$, $\forall$ s funció en U de divisor D, $g_{K,D} - \log |s|^{-1}$ es prolonga a una funció harmònica en U.

(el cas anterior era $X = \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$, i $D = (\infty)$).

g_K representa (si $D = (P)$) el potencial elèctric obtingut al situar una càrrega elèctrica unitària en P, on K és conductor i $X - K$ és dielèctric.

$g_{K,D}$ és la funció de Green sobre l'obert $X - K$ associada a D.

Thm: (Bost, Mestre): Si $y^2 = (x-a)(x-b)(x-c)(x-d)$, i P és un punt real d'abscissa α, sigui C la capacitat de la unió de 2 intervals d'extrems $(0, (\alpha-a)(\alpha-b), (\alpha-c)(\alpha-a), (\alpha-b)(\alpha-c))$, i h_∞ l'altura de P. Aleshores:

$$h_\infty = \frac{1}{4} \log (4C).$$

Recíprocament:

Sigui $I = [\alpha, \beta] \cup [\gamma, \delta]$, sigui C: $y^2 = (x-\alpha)(x-\beta)(x-\gamma)(x-\delta)$

∞_+, ∞_- les dues places a ∞.

Capacitat $(I) = h_\infty(\infty_-)$ (escollint ∞_+ com a 0 de la corba).

$\underline{Th}$: $I = \bigcup_{1\leq i\leq g+1} [a_i, b_i]$ i $C: y^2 = \prod_{i=1}^{g+1} (x-a_i)(x-b_i)$

Aleshores $Cap(I) = h_\infty(\infty_-)$ si es pren ∞_+ com a origen de $Jac(C)$.

Suposem $C_0 : y^2 = f(x)$ $\deg f = 6$

Considerem $Jac(C_0)$.

$\int_{P_i}^{P_j} s(x)\frac{dx}{y}$ amb $\deg s \leq 1$. Busquem un algoritme quadràtic per calcular aquesta integral.

Un article de Richelot (~~1830~~) dona un mètode.

Humbert va donar un mètode geomètric per solucionar-ho (~1896)

$A_0 = J(C_0)$ C_0

$A_1 = J(C_1)$. C_1

$A_n = \mathbb{C}^g / \Lambda_n = [-\Omega_0, 2^n \Omega_0]$ C_n

Recordem la generalització de l'AGM:

$G = \left(\mathbb{Z}/2\mathbb{Z}\right)^g$: a tot $(a_\tau)_{\tau\in G} \rightsquigarrow (A_\tau)_{\tau\in G}$, on:

$$A_\tau = \frac{1}{2^g}\sum_{\sigma\in G}\sqrt{a_\sigma a_{\sigma+\tau}}$$ Convergeix quadràticament, també

Per $g=1$, coincideix amb l'AGM.

Per $g=2$, fórmules de Borchardt. $\left\{\begin{array}{l} A = \frac{a+b+c+d}{4} \\ B = \dots \\ C \\ D = \frac{\sqrt{ad}+\sqrt{bc}}{2}\end{array}\right\} \longrightarrow M(a,b,c,d)$ Mitjana de Borchardt de 4 nombres.

- Relació amb les funcions theta, periodes de corbes algebraiques, ...

1) Cas $g=2$.

Sigui $C_{/\mathbb{R}}: Y^2 = f(X) = (X-a_1)(X-a_1')\cdots(X-a_3)(X-a_3')$ $a_i \in \mathbb{R}$

Escrivim $a_0 := \sqrt{|(a_1-a_2)(a_1-a_3)(a_1'-a_2')(a_1'-a_3')|}$

$b_0 := \sqrt{\dots}$

$c_0 := \sqrt{\dots}$

$d_0 := \sqrt{\dots}$

permutant les diferents possibilitats. (fixant a_1, a_1', obtenim $\{a_2, a_2'\}, \{a_3, a_3'\}$ i són 4 permutacions.

Thm (Borchardt): $M(a_0, b_0, c_0, d_0) = \dfrac{4\pi^2}{|\det \Omega_1|}$, on

Ω_1: es pren una base de formes diferencials, $\{\frac{dx}{y}, \frac{xdx}{y}\}$ de $\Omega^1(C)$,

i es pren $\gamma_1, \gamma_1', \gamma_2, \gamma_2'$ x periodes (Mumford, Tata Lect. on Θ-functions chap 3 (6.II)).

Aleshores

$$\underbrace{\left(\int_{\gamma_i}\omega_j \; \int_{\gamma_j'}\omega_i\right)}_{2g} \Big\} g$$

Per $g=1$, $\omega_1 = 2\int_{e_1}^{e_2}\frac{dx}{y}$.

Això permet de calcular quadràticament $|\det \Omega_1|$.

2) Per g qualsevol,

C corba hiperel·líptica, de gènere g: $Y^2 = (X-a_1)(X-a_1')\cdots(X-a_{g+1})(X-a_{g+1}')$

Fixant $\{a_1, a_1'\}$, obtenim 2^g permutacions diferents, que estan associades a un element de $\left(\mathbb{Z}/2\mathbb{Z}\right)^g$.

Per tant, sigui $a_\tau = \sqrt{(a_1 - \tau(a_1)) \dots (a_1 - \tau(a_{g+1}))}$

Thm: La $M\left((a_\tau)_{\tau \in G}\right) = \dfrac{(2\pi)^g}{|\det \Omega_1|}$ (fórmula de Thomae-Fay).

Considerem ara

$$\begin{aligned} (\Omega_1, \Omega_2) &\longrightarrow (\mathrm{Id} \ \ \overset{\tau}{\overset{\shortparallel}{\Omega_1^{-1}\Omega_2}}) \\ \underset{\mathbb{C}^g}{\vec{z}} &\longmapsto \Omega_1^{-1}\vec{z} \end{aligned}$$

Thm (Riemann): τ és simètrica, $\mathrm{Im}(\tau) >> 0$.

A cada τ, se li associa $\Theta(z, \tau) := \sum_{\vec{n}} e^{\pi i \dots} e^{2\pi i \vec{z}\vec{n}}$

Els punts d'ordre 2, són de $\mathbb{C}^g / [\mathrm{Id}, \tau]$,

P-adics (Henriot-Mestre 1989).

K cos, π uniformitzador, $\mathrm{char}\, K \neq 0$, char res $= p$.

$a_0 = a$, $b_0 = b$: l'AGM convergeix $\Leftrightarrow \dfrac{b_0}{a_0} \equiv 1 \ (8\pi)$.

Si $\frac{b}{a} \equiv 1 \ (4\pi)$, $\exists! \sqrt{\frac{b}{a}} \equiv 1 \ (2\pi)$.

Aleshores $|a_{n+1} - b_{n+1}|_\pi = \dfrac{|a_n - b_n|_\pi^2}{|8 b_0|_\pi}$ convergència quadràtica si $\pi \neq 2$.

Però si $\pi = 2 \to v(a_n - b_n) = 3 \Rightarrow v(a_{n+1} - b_{n+1}) = 3$.

Si treiem aquest cas, tenim doncs un límit $M(a,b)$.

$E: y^2 = x(x - a^2)(x - b^2)$

Si l'AGM convergeix, $\frac{b}{a} \equiv 1 \ (8\pi)$, signifiquen que $v_\pi(j) < 0$. $(\Leftrightarrow)$.

Per tant, la reducció de E és multiplicativa.

Aleshores, llevat de fer una ext. quadràtica $K(\sqrt{-c_6})$, E

és isomorfa a la corba de Tate $E(q)$:

$j = \frac{1}{q} + 744 + \dots \rightsquigarrow q = \varphi\left(\frac{1}{j}\right) \rightsquigarrow |q| < 1 \dots$

I $E(q) \simeq \mathbb{C}^\times / q^{\mathbb{Z}}$

La corba de Tate serà $y^2+xy=x^3+\alpha(q)x+\beta(q)$, i l'isom.
vindrà donat per $\varphi^*\left(\frac{dq}{q}\right)=u\frac{dx}{y}$ on $u^2\in K$.
Mitjançant l'AGM, tindrem un algoritme quadràtic per calcular u i q.
Es pot estendre a una corba general amb invariant j de valoració negativa.

En el cas $\pi=2$, què s'ha de fer?
$E: y^2=x(x-a^2)(x-b^2)$ definida en $\mathbb{Q}_2^d=K$
i suposem $v\left(\frac{b}{a}-1\right)=3$.
E té doncs reducció ordinària.
Si prenem $E/\mathbb{F}_{2^d}: y^2+xy=x^3+a_6$; és fer un lift a K, veurem que sempre és $v\left(\frac{b}{a}-1\right)=3$.
Si $b/a\equiv 1\ (8)$ podem definir $b_1=a\sqrt{\frac{b}{a}}\equiv 1\ (4)$ i $a_1=\frac{a+b}{2}$.
Llavors $\frac{b_1}{a_1}\equiv 1\ (8)$.
Per tant, encara que no convergeixi, almenys està definida.

$$E_0 \rightleftarrows E_1 \rightleftarrows \cdots \rightleftarrows E_n$$

És fa $j(E_n)\longrightarrow j(\text{lift canònic de } E/\mathbb{F}_d)$. Per tant, $\frac{b_n}{a_n}$ sí que convergeix, $\lim_{n\to\infty}\frac{b_n}{a_n}=\mu$.

~~$v\left(\frac{b_n}{a_n}-1\right)=v\left(\frac{b_n}{\right.}\right.$~~