Sonderdruck aus
Arch. Math., Vol. 52, 507–512 (1989)

0003-889X/89/5205-0507 $ 2.70/0

The arithogeometric mean

By

DANIEL R. GRAYSON*)

In this expository note we derive the arithogeometric mean method of Gauss. We assume the reader knows basic algebraic geometry and the theory of elliptic curves. We arrive at the required quadratic substitution with no guesswork, explain how to compute the periods of an elliptic curve, and how to compute the (inverse) elliptic integrals (elliptic functions). The algorithms described are suitable for machine computation to hundreds of digits of accuracy.

Begin with an elliptic curve E given by the equation $y^2 = x(x+r)(x+s)$. We assume that $(x+r)(x+s)$ has real coefficients, and that neither r nor s is real and nonnegative. Any real elliptic curve can be brought into this form. We let $L \subset \mathbb{C}$ be the lattice of periods of $\omega = \dfrac{dx}{2y}$, and let $\Phi: \mathbb{C}/L \xrightarrow{\approx} E(\mathbb{C})$ be the isomorphism with $\Phi^*\omega = dz$ (z = parameter on $\mathbb{C}$). We write $L = \mathbb{Z}\gamma + \mathbb{Z}\delta$ where $\gamma = 2\int_0^\infty \omega$ is real. We know that $\Phi([0,\gamma])$ is a component of $E(\mathbb{R})$ containing $\Phi(0) = \infty$, so $\Phi(\frac{1}{2}\gamma) = (0,0)$. The other points of order two are $(-r,0)$ and $(-s,0)$, so we may assume $\Phi(\frac{1}{2}\delta) = (-r,0)$ and $\Phi(\frac{1}{2}\delta + \frac{1}{2}\gamma) = (-s,0)$ (by interchanging r and s, if necessary).

Let Λ be the lattice $\mathbb{Z}\gamma + \mathbb{Z}2\delta \subsetneqq \mathbb{C}$. It is invariant under complex conjugation, so it corresponds to a real elliptic curve. We find an equation $v^2 = u(u+R)(u+S)$ and an isomorphism $\Psi: \mathbb{C}/\Lambda \xrightarrow{\approx} F(\mathbb{C})$. The constant c in $\Psi^*\left(\dfrac{du}{2v}\right) = c\,dz$ may be assumed to be 1 by change of variable. We assume that R and S satisfy the same conditions that r and s did, so that $\Psi(0) = \infty$, $\Psi(\frac{1}{2}\gamma) = (0,0)$, $\Psi(\delta) = (-R,0)$, and $\Psi(\delta + \frac{1}{2}\gamma) = (-S,0)$.

The inclusion $\Lambda \subset L$ provides a 2-to-1 map (isogeny) $\varphi: F \longrightarrow E$ which makes the diagram

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \longrightarrow & \mathbb{C}/L \\ {\scriptstyle\Psi}\downarrow & & \downarrow{\scriptstyle\Phi} \\ F(\mathbb{C}) & \xrightarrow[\varphi]{} & E(\mathbb{C}) \end{array}$$

*) Research supported by NSF (MCS 82-02692 and DMS 85-04692).

commute. We see that $\varphi^*\left(\frac{dx}{2y}\right) = \frac{du}{2v}$, $\varphi(0,0) = \varphi(-S,0) = (0,0)$, and $\varphi(\infty) = \varphi(-R,0) = \infty$. The explicit formulas which describe φ comprise the "Landen transformation"; we begin to calculate them now.

Projection on the x-axis gives an isomorphism $x: E/\sim \xrightarrow{\approx} \mathbb{P}^1$, where $\sim$ denotes the equivalence relation $P \sim -P$. Since φ is a group homomorphism, it induces a map $\psi: \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ on the quotients which is 2-to-1, and satisfies $\psi(0) = \psi(-S) = 0$, $\psi(\infty) = \psi(-R) = \infty$.

We write $x = \psi(u) = \frac{p(u)}{q(u)}$ where p and q are polynomials. Regarding u as unknown in the equation $xq(u) - p(u) = 0$, we see that $\max(\deg p, \deg q) = 2$. We must therefore have

$$x = \frac{ku(u+S)}{u+R}$$

where k is some nonzero constant. We deduce

$$ku^2 + (kS - x)u + (-xR) = 0,$$

which is a quadratic equation for u whose discriminant is

$$D(x) = x^2 + 2k(2R - S)x + k^2S^2.$$

Now $D(x) = 0$ iff x is a branch point for ψ. If $x = x(\Phi(z))$, then $\Psi^{-1}(\psi^{-1}(\{x\})) = \{z, -z, z+\delta, -z+\delta\}$ modulo Λ, so x is a branch point iff $z = -z + \delta$ modulo Λ. Thus the branch points are given by taking $z = \frac{1}{2}\delta$ or $\frac{1}{2}\delta + \frac{1}{2}\gamma$, yielding $x = -r$ or $-s$. Equating $D(x)$ with $(x+r)(x+s)$ yields

$$r + s = 2k(2R - S)$$
$$rs = k^2S^2.$$

We compute

$$\begin{aligned} y^2 = x(x+r)(x+s) &= \\ &= \frac{ku(u+s)}{(u+R)}\left[\frac{ku(u+s)}{(u+R)} + r\right]\left[\frac{ku(u+s)}{(u+R)} + s\right] \\ &= k^3v^2(u+R)^{-4}(u^2 + 2Ru + RS)^2. \end{aligned}$$

Letting $c = \pm\sqrt{k}$ with appropriate sign, we find

$$y = c^3v(u+R)^{-2}(u^2 + 2Ru + RS).$$

Now compute

$$\frac{du}{2v} = \varphi^*\left(\frac{dx}{2y}\right) = \frac{d\left(\frac{ku(u+S)}{u+R}\right)}{2c^3v(u+R)^{-2}(u^2+2Ru+RS)} = c^{-1}\frac{du}{2v}$$

and conclude that $c = 1$ and $k = 1$.

We solve for R and S in terms of r and s and summarize what we've done:

$$E\colon y^2 = x(x+r)(x+s) \quad \text{periods } \gamma, \delta$$
$$S = \sqrt{rs}$$
$$R = \tfrac{1}{2}(\tfrac{1}{2}(r+s) + S)$$

$$F\colon v^2 = u(u+R)(u+S) \quad \text{periods } \gamma, 2\delta$$
$$\frac{du}{2v} = \frac{dx}{2y}$$
$$x = u(u+S)/(u+R)$$
$$y = v(u^2 + 2Ru + RS)/(u+R)^2.$$

It turns out that we can avoid complex arithmetic here. Write $(x+r)(x+s) = x^2 + bx + c$. Our assumptions about r and s imply that $c > 0$. We find

$$S = +\sqrt{c}$$
$$R = \tfrac{1}{2}(\tfrac{1}{2}b + S)$$

and that R and S are real and positive.

Now we repeat this period-stretching procedure forever. Let $L_n = \mathbb{Z}\gamma + \mathbb{Z}2^n\delta$. We find the corresponding elliptic curve E_n (for $n \geqq 1$) as follows

$$E_n\colon y_n^2 = x_n(x_n^2 + b_n x_n + c_n)$$
$$S_n = \sqrt{c_{n-1}}$$
$$R_n = \tfrac{1}{2}(\tfrac{1}{2}b_{n-1} + S_n)$$
$$b_n = R_n + S_n$$
$$c_n = R_n S_n$$
$$x_{n-1} = x_n(x_n + S_n)/(x_n + R_n)$$
$$y_{n-1} = y_n(x_n^2 + 2R_n x_n + R_n S_n)/(x_n + R_n)^2.$$

(We set $R_0 = r$, $S_0 = s$, and notice $R_1 = R$, $S_1 = S$, $b_0 = b$, $c_0 = c$.)

To see the relation with the arithogeometric mean we set $A_n = \sqrt{R_n}$ and $B_n = \sqrt{S_n}$, and observe that $A_n = \frac{1}{2}(A_{n-1} + B_{n-1})$ and $B_n = \sqrt{A_{n-1}B_{n-1}}$. The limit $M = \lim A_n = \lim B_n$ exists and is the arithogeometric mean $\operatorname{agm}(A_0, B_0)$. We may compute it as $M = \sqrt{R_\infty} = \sqrt{S_\infty}$ where $R_\infty = \lim R_n$ and $S_\infty = \lim S_n$.

Introduce variables X and Y satisfying $Y^2 = X(X+R_\infty)(X+S_\infty) = X(X+M^2)^2$. Then we compute the real period

$$\gamma = 2\int_0^\infty \frac{dx_0}{2y_0} = \int_0^\infty \frac{dx_0}{y_0} = \int_0^\infty \frac{dx_1}{y_1} = \cdots = \int_0^\infty \frac{dY}{Y} = \int_0^\infty \frac{dX}{\sqrt{X}(X+M^2)}$$
$$= 2\int_0^\infty \frac{dt}{t^2+M^2} = \frac{2}{M}\int_0^\infty \frac{ds}{s^2+1} = \frac{\pi}{M}.$$

The substitutions used above were $t = \sqrt{X}$ and $s = t/M$ which amount to $X = M^2 s^2$ and $Y = M^3 s(s^2 + 1)$. We will use these later.

To write the formula above in the classical fashion we consider two cases. First, the case where r and s are real yields the formula

$$\gamma = \int_{e_3}^{\infty} \frac{dx}{2\sqrt{(x-e_1)(x-e_2)(x-e_3)}} = \frac{\pi}{\operatorname{agm}(\sqrt{e_3-e_1}, \sqrt{e_3-e_2})}$$

where $e_1 < e_2 < e_3$ are real, and after substituting x for $x - e_3$ we find $r = e_3 - e_1$ and $s = e_3 - e_2$. Second, if $P(x)$ is a monic cubic polynomial with just one real root β, then substituting x for $x - \beta$ yields $x(x^2 + bx + c) = P(x + \beta)$, and so $b = \frac{1}{2} P''(\beta)$, $c = P'(\beta)$. We find

$$\begin{aligned} M &= \operatorname{agm}(\sqrt{S}, \sqrt{R}) \\ &= \operatorname{agm}\left(\left(\frac{1}{2}\left(\frac{1}{2} b + S\right)\right)^{\frac{1}{2}}, c^{\frac{1}{4}}\right) \\ &= c^{\frac{1}{4}} \operatorname{agm}\left(1, \sqrt{\frac{1}{2} + \frac{P''(\beta)}{8\sqrt{P'(\beta)}}}\right) \end{aligned}$$

(using the homogeneity and symmetry of the agm) and

$$\gamma = \int_{\beta}^{\infty} \frac{dx}{2\sqrt{P(x)}} = \frac{\pi}{M}.$$

Let E_∞ be the nodal cubic given by the equation $Y^2 = X(X + M^2)^2$, and let E'_∞ be the complement of the node. Let $\Phi_\infty : \mathbb{C}/\mathbb{Z}\gamma \xrightarrow{\approx} E'_\infty(\mathbb{C})$ be the analytic isomorphism with $\Phi_\infty^*\left(\frac{dx}{2y}\right) = dz$ and $\Phi_\infty(0) = \infty$. Let $\Phi_n : \mathbb{C}/L_n \xrightarrow{\approx} E_n(\mathbb{C})$ be the analogous isomorphisms for $n = 0, 1, 2, \ldots$.

Consider the sequence of analytic maps

$$E'_\infty(\mathbb{C}) \longrightarrow E_n(\mathbb{C}) \longrightarrow E_{n-1}(\mathbb{C}) \longrightarrow \cdots \longrightarrow E_0(\mathbb{C}).$$

Given $z \in \mathbb{C}/\mathbb{Z}\gamma$ we set $P_\infty = \Phi(z)$ and $P_n = \Phi_n(z)$, obtaining a compatible family of points $P_n \in E_n$. Choosing a path from 0 to z provides paths from ∞ to P_n below, so we may write

$$\begin{aligned} z &= \int_0^z dz = \int_\infty^{P_0} \frac{dx_0}{2y_0} = \int_\infty^{P_\infty} \frac{dX}{2Y} \\ &= \frac{1}{M} \int_\infty^s \frac{ds}{s^2+1} = -\frac{1}{M} \operatorname{arccot}(s). \end{aligned}$$

Thus $s = -\cot(Mz)$, and this determines X and Y as above so that $P_\infty = (X, Y)$. If we pick N very large, then $X \approx x_N$ and $Y \approx y_N$, where $P_N = (x_N, y_N)$. Using the formulas above we descend one step at a time, eventually arriving at $(x_0, y_0) = P_0$. We summarize the algorithm:

Algorithm. Given b_0, c_0, and z, compute $(x_0, y_0) = \Phi_0(z)$ approximately:
Compute S_n, R_n, b_n, c_n as above, stopping when $S_N \approx R_N$

$$\begin{aligned} M &\longleftarrow \sqrt{R_N} \\ s &\longleftarrow -\cot(Mz) \\ x_N &\longleftarrow M^2 s^2 \\ y_N &\longleftarrow M^3 s(s^2+1) \\ x_{n-1} &\longleftarrow x_n(x_n + S_n)/(x_n + R_n) \\ y_{n-1} &\longleftarrow y_n(x_n^2 + 2R_n x_n + R_n S_n)/(x_n + R_n)^2 \\ &\quad \text{for } n = N, N-1, \ldots, 1. \end{aligned}$$

We can easily turn this around and get an algorithm for computing z from $P_0 = (x_0, y_0)$, as follows.

Algorithm. Given b_0, c_0, and $P_0 = (x_0, y_0) \in E_0(\mathbb{C})$, compute $z \in \mathbb{C}/L_0$ approximately.

Compute S_n, R_n, b_n, c_n for $n = 1, \ldots, N$, and M, as before

$$\begin{aligned} x_n &\longleftarrow \tfrac{1}{2}[x_{n-1} - S_n \pm \sqrt{x_{n-1}^2 + b_{n-1}x_{n-1} + c_{n-1}}] \\ y_n &\longleftarrow y_{n-1}(x_n + R_n)^2/(x_n^2 + 2R_n x_n + R_n^2 + R_n S_n) \\ &\quad \text{for } n = 1, \ldots, N \\ z &\longleftarrow -\frac{1}{M}\operatorname{arccot}\left(\frac{y_N}{M(x_N + M^2)}\right). \end{aligned}$$

Finally we show how to compute the complex period δ. We consider the case $b^2 - 4c < 0$ first. Then we may assume $\operatorname{Re}\delta = \frac{1}{2}\gamma$, so $2\delta - \gamma$ is the smallest purely imaginary period. One sees that

$$2\delta - \gamma = \int_{-\infty}^{0} \frac{dx}{[x(x^2 + bx + c)]^{1/2}} = \sqrt{-1}\int_{0}^{\infty} \frac{dx}{[x(x^2 - bx + c)]^{1/2}};$$

the latter integral is the real period of the curve obtained from E_0 by replacing b by $-b$, and can be computed as above.

Now consider the case $b^2 - 4c > 0$.

Then we may assume $r > s > 0$. Now we may assume δ is the smallest purely imaginary period, so

$$\begin{aligned} \delta &= \int_{-\infty}^{-r} \frac{dx}{[x(x+r)(x+s)]^{1/2}} \\ &= \sqrt{-1}\int_{0}^{\infty} \frac{dx}{[x(x+r)(x+r-s)]^{1/2}}; \end{aligned}$$

the latter integral is the real period of the curve obtained from E by replacing s by $r - s$, and can be computed as before.

Here is a numerical example which can be used for checking accuracy because x_0, y_0 turn out to be integers

$$b_0 = \tfrac{49}{4} \qquad c_0 = 16$$
$$\gamma \cong 1.479\,677\,927\,794$$
$$\delta \cong 0.993\,481\,858\,506\sqrt{-1}$$
$$\Phi_0(\tfrac{1}{4}\gamma) = (4, -18)$$
$$\Phi_0(\tfrac{1}{8}\gamma + \tfrac{1}{2}\delta) = (-8, 12).$$

References

[1] D. COX, The arithmetic-geometric mean of Gauss. Enseign. Math. **30**, 275–330 (1984).
[2] J. SILVERMAN, The arithmetic of Elliptic Curves. Berlin-Heidelberg-New York 1985.

Eingegangen am 21. 10. 1987

Anschrift des Autors:

Daniel R. Grayson
Department of Mathematics
University of Illinois
Urbana, Illinois 61801
USA