Recent Developments In Hyperelliptic Curve Cryptography

Andreas Stein
CACR
Waterloo 1999

Outline

- Motivation
- Arithmetic
- Security
- Class Numbers and Mean Values

Why hyperelliptic cryptography?

- Hyperelliptic curves of genus 2, 3, and 4 provide an **alternative source** of curves suitable for **effective** cryptosystems.

- Investigate hyperelliptic curves (or, more generally, algebraic curves) to obtain results on **elliptic curves**.

- For curves of small genus, there are many difficult computational problems.

- **Interaction** with other areas such as: computational, algorithmic, and analytic number theory; algebraic geometry; function field theory; applications to coding theory.

Plus: hyperelliptic curves of genus 2, 3, and 4

- There exists an effective arithmetic.
- Same level of security as elliptic curves with parameters of the same size!
- The HCDLP appears to be as difficult. Thus, the **strength-per-key-bit** is substantially greater than in conventional discrete logarithm and integer factoring systems.

Minus:

- The arithmetic is slower than the elliptic curve arithmetic.
- Computing the order of the Jacobian of hyperelliptic curves seems to be difficult. (Avoid **Pohlig-Hellman** attack!)

Hyperelliptic curves/function fields

$k = \mathbb{F}_q$, $q = p^l$, $p > 2$

- A **hyperelliptic curve** C of genus g over k:

  a.) $\mathrm{C} : V^2 = F(U) = U^{2g+1} + \dots$

  where $F(U) \in k[U]$ squarefree.

  b.) $\mathrm{C} : Y^2 = D(X) = X^{2g+2} + \dots$

  where $D(X) \in k[X]$ squarefree.

- **Hyperelliptic function field** $k(\mathrm{C})$ of **C**:

  a.) $k(\mathrm{C}) = k(U)(V)$ **imaginary quadratic**.

  b.) $k(\mathrm{C}) = k(X)(Y)$ **real quadratic**.

$K = k(\mathbf{C})$ hyperelliptic function field.

- $J_C(K) = Div_0(K)/P(K)$ **Jacobian** of **C**, i.e. the **divisor class group** of K.

- $h = |J_C(K)|$ **divisor class number** of K.

- $h \sim q^g$.

If $K = k(X)(Y)$ is real quadratic, then

$$h = h_X \, R_X \ ,$$

where R_X is the **regulator** of K and h_X is the **ideal class number** of K w.r.t. the **maximal order** $\mathcal{O}(X) = k[X][Y]$.

Birational transformations

- **imaginary $\longrightarrow$ real**: $K = k(U)(V) = k(\mathbf{C}_i)$

$$\mathbf{C}_i : V^2 = F(U) = U^{2g+1} + \dots$$

For a suitable $\beta \in k$ we define

$X := 1/(U-\beta)\,, \quad D(X) := X^{2g+2}\, F(\beta+1/X)$

$\Rightarrow$ $\mathbf{C}_i$ is birationally equivalent to

$$\mathbf{C_r} : Y^2 = D(X) = X^{2g+2} + \dots$$

and $K = k(X)(Y) = k(\mathbf{C}_r)$ is real quadratic.

- **real $\longrightarrow$ imaginary**: Reverse the formulas. **But** need $D(\alpha) = 0$ for some $\alpha \in k$.

- $\{$ imaginary over k $\} \subseteq \{$ real over k $\}$

Examples

Curves of genus 3 over $\mathbb{F}_{100000007}$:

$$\begin{aligned} \mathbf{C_i} : V^2 &= U^7 - 3\,U^6 + 3\,U^5 + 25000003\,U^4 \\ &\quad +49999999\,U^3 + 75000009\,U^2 \\ &\quad +50000002\,U + 25000002 \end{aligned}$$

$$\begin{aligned} \mathbf{C_r} : Y^2 &= X^8 + 27281228\,X^7 + 28787256\,X^6 \\ &\quad +47891154\,X^5 + 50000006\,X^4 \\ &\quad +72718779\,X^3 + 8485099\,X^2 \\ &\quad +61345432\,X \end{aligned}$$

$\mathbf{C_i}$ and $\mathbf{C_r}$ are birationally equivalent.

Koblitz curve of genus 2 over $\mathbb{F}_{2^l}$:

$\mathbf{C_k} : V^2 + UV = U^5 + U^2 + 1$

Arithmetic (imaginary case)

- Arithmetic of reduced divisors in $J_C(K)$.

- Each element $\mathcal{A}$ of the Jacobian can be uniquely represented by a **reduced** divisor

$$\mathcal{A} = (Q(U), P(U)) \ ,$$

$$\deg P < \deg Q \leq g \ .$$

- **group** operation (Cantor, 1987):

  1. composition $(8g^2 + O(g))$

  2. reduction $(9g^2 + O(g))$

  Complexity: $17g^2 + O(g)$ operations in $\mathbb{F}_q$

Arithmetic (real case)

- Arithmetic of reduced ideals.

- Unique representation of a reduced ideal $\mathcal{A}$:

$$\mathcal{A} = (Q(X), P(X)) \ ,$$

$$\deg P < \deg Q \leq g \ .$$

- **Infrastructure** operation:

  1. composition $(8g^2 + O(g))$

  2. reduction $(9g^2 + O(g))$

  Complexity: $17g^2 + O(g)$ operations in $\mathbb{F}_q$

- **Baby step** operation: step in the continued fraction expansion of reduced ideals.

  Complexity: $4g + O(1)$ operations in $\mathbb{F}_q$

Composition

Input: $\mathcal{A} = (Q_1, P_1)$, $\mathcal{B} = (Q_2, P_2)$ reduced.

Output: $\mathcal{C} = (Q, P)$ such that

$$\mathcal{C} = (Q_1, P_1) \cdot (Q_2, P_2)$$

1. Compute polynomials S, A, C by the extended gcd such that

$$\begin{aligned} S &\leftarrow XGCD3(Q_1, Q_2, P_1 + P_2) \\ &= A \cdot Q_1 + B \cdot Q_2 + C \cdot (P_1 + P_2) \end{aligned}$$

2. $Q \leftarrow \dfrac{Q_1 Q_2}{S^2}$

3. $V \leftarrow P_1 + \dfrac{AQ_1(P_2 - P_1) + C(F - P_1^2)}{S} \pmod{Q}$

Reduction

Input: (Q_0, P_0) non-reduced

Output: $\mathcal{C} = (Q, P)$ reduced

1. $Q_1 \leftarrow \dfrac{F - P_0^2}{Q_0}$, $j \leftarrow 1$

2. $(a_0, P_1) \leftarrow DIVREM(-P_0, Q_1)$

3. While $\deg Q_j \geq g + 1$ do

   (a) $Q_{j+1} \leftarrow Q_{j-1} + a_{j-1}(P_j - P_{j-1})$

   (b) $(a_j, P_{j+1}) \leftarrow DIVREM(-P_j, Q_{j+1})$

   (c) $j \leftarrow j + 1$

4. $Q \leftarrow Q_j$, $P \leftarrow P_j$

Explicit complexities in the most general cases

(Quadratic operations in the finite field $\mathbb{F}_q$)

	imaginary case	real case
$\mathcal{A} * \mathcal{B}$	$17g^2 + O(g)$	$17g^2 + O(g)$
$\mathcal{A}^2$	$16g^2 + O(g)$	$16g^2 + O(g)$
baby step	$17g^2 + O(g)$	4g+O(1)

Average time of one multiplication over one baby step

g	10^1	10^2	10^3	10^4	10^5	10^6	10^7	10^8	10^9
1	4.2	4.5	4.5	4.3	4.6	4.6	4.8	4.6	4.3
2	5.7	4.8	5.3	5.5	6.5	6.2	6.4	6.4	6.5
3	7.0	8.7	9.0	8.5	10.3	10.6	11.0	11.0	11.3
4	10.5	9.9	10.6	10.7	13.2	13.0	13.2	13.4	14.0
5	14.8	14.4	13.9	13.9	17.5	16.8	18.1	18.4	18.3
6	15.3	16.9	16.1	15.6	20.0	20.4	21.2	20.8	20.9
7	16.5	20.1	19.6	19.0	24.4	23.8	26.0	26.2	25.5
8	20.8	21.1	22.4	21.6	28.2	27.5	28.6	28.7	29.8
9	24.5	25.0	25.2	25.0	31.5	31.4	33.4	33.4	33.0
10	24.9	27.7	27.6	27.6	34.4	34.2	36.3	37.0	37.1

t_m = running time for one multiplication
t_{bs} = running time for one baby step

$$\frac{t_m}{t_{bs}} \approx 4 \cdot g$$

Summary

- Multiplication: $\frac{\text{imaginary}}{\text{real}} = 1$
  (theoretically and practically)

- Inversion: $\frac{\text{imaginary}}{\text{real}} = 1$

- **Baby step**: $\frac{\text{imaginary}}{\text{real}} \approx 4g$

- **Baby step-giant step** algorithm:
$$\frac{\text{imaginary}}{\text{real}} \geq 2\sqrt{g}$$

- **Pollard's kangaroo** method:
$$\frac{\text{imaginary}}{\text{real}} \geq 2\sqrt{g}$$

- **Key exchange**: $\frac{\text{imaginary}}{\text{real}} \approx 1.2$

Binary

input: $\mathcal{A}$ reduced, $n = \sum_{i=0}^{l} b_i 2^{l-i}$.

output: $\mathcal{B} = \mathcal{A}^n$

1. $\mathcal{B} \leftarrow \mathcal{A}$

2. For $i = 1$ to l do

   (a) $\mathcal{B} \leftarrow \mathcal{B} * \mathcal{B}$

   (b) if $(b_i = 1)$ $\mathcal{B} \leftarrow \mathcal{B} * \mathcal{A}$

3. return($\mathcal{B}$)

Complexity:
$\frac{3}{2}\lfloor \log_2 n \rfloor$ multiplications $= \frac{3}{2}\lfloor \log_2 n \rfloor t_m$

Binary (real case)

input: $n = \sum_{i=0}^{l} b_i 2^{l-i}$.

output: $\mathcal{B}$ such that $\delta(\mathcal{B}) = n$.

1. $\mathcal{B} \leftarrow \mathcal{A}$, where $\delta(\mathcal{A})$ small

2. For $i = 1$ to l do

   (a) $\mathcal{B} \leftarrow \mathcal{B} * \mathcal{B}$

   (b) if $(b_i = 1)$ $\mathcal{B} \leftarrow$ **baby**$(\mathcal{B})$

3. return$(\mathcal{B})$.

Complexity:
$\lfloor \log_2 n \rfloor$ multiplications and $\frac{1}{2}\lfloor \log_2 n \rfloor$ baby steps

$$\approx \lfloor \log_2 n \rfloor (1 + \frac{1}{8g}) \cdot t_m$$

So far

- Two choices of arithmetic:

    1. Imaginary; **Koblitz** (1989) via Cantor (1987). See for instance **Spallek** (1994), **Krieger** (1997), and **Smart** (1998).

    2. Real; **Scheidler, S., Williams** (1996) via Shanks.

- One group operation in the imaginary case.

- One infrastructure operation and one baby step operation in the real case.

- The real case is technically more involved, but generally gives a speed-up of algorithms.

- The main operation has a complexity of $17g^2 + O(g)$ quadratic operations in $\mathbb{F}_q$.

Security

- The hyperelliptic curve discrete logarithm problem (HCDLP) is the discrete logarithm problem in the Jacobian group.

- HCDLP $\Rightarrow$ breaking the protocol.

- The infrastructure discrete logarithm problem (IDLP) is the discrete logarithm problem in the set of reduced principal ideals of real quadratic curves/function fields.

- HCDLP $\Leftrightarrow$ IDLP. (**S.** 1997, **Zuccherato** 1997, **Paulus, Rück** 1999)

- Choose parameters q and g such that
$$|J_C(K)| \sim q^g \sim 10^{50}$$
For $q = 2^l$ let $160 \leq l \cdot g \leq 163$

Known Attack to the HCDLP

- **Frey, Rück** 1994: Fast methods for supersingular hyperelliptic curves.

- **Rück** 1997: Fast methods for anomalous curves or curves with a large p-subgroup.

- **Adleman, DeMarrais, Huang** 1994 and **S., Müller, Thiel** 1999: For $2g > \log q$ (conjectured) subexponential

$$L_{q^{2g+1}}[2.18] \quad \text{resp.} \quad L_{q^{2g+2}}[1.44].$$

- Pollard's ρ and kangaroo methods

$$O(\, g^2 \, q^{\frac{g}{2}} \, (\log q)^\alpha \,)$$

- **Gaudry** 1999: conjectured

$$O(\, g^2 \, g! \, q \, (\log q)^\alpha) + O(\, g^3 \, q^2 \, (\log q)^\alpha \,)$$

Gaudry's algorithm

- assumes that $|J_C(K)|$ is known

- assumes that the prime divisors of degree 1 generate the Jacobian.

- uses a random walk (**Pollard** 1978, **Teske** 1998) to generate a sparse relation matrix.

- uses Lancos and/or Wiedemann's (1986) algorithm for sparse linear algebra.

- appears to be better than Pollard's rho method for $g \geq 5$ or 6

- should turn out to be subexponential for $2g > \log q$.

Use of automorphisms

Assume that there exists an automorphism of order m that can be evaluated quickly.

- Speed-up (Pollard's rho) by a factor $\sqrt{m}$:

  $$O(\, g^2\, q^{\frac{g}{2}}\, (\log q)^{\alpha}\,)/\sqrt{m}$$

- Speed-up (Gaudry) by a factor m^2 for fixed size of a factor base:

  $O(\, g^2\, g!\, (q/m)\, (\log q)^{\alpha}) + O(\, g^3\, (q/m)^2\, (\log q)^{\alpha}\,)$

  (Duursma, Gaudry, Morain 1999)

- Generalization of ideas of **Gallant, Lambert, Vanstone** 1999, and **Wiener, Zuccherato** 1999 for elliptic curves.

- Example: $k = \mathbb{F}_{2^l}$ and let **C** be a **Koblitz curve**, i.e. **C** is defined over $\mathbb{F}_2$. Then $\tau : (x, y) \to (x^2, y^2)$ is of order l and $m = 2l$.

Computing the cardinality of $J_C(K)$

$$|J_C(K)| = h \sim q^g$$

Pila 1996: There exists a **"polynomial"** time method to compute $|J_C(K)|$.

- Idea: Compute the characteristic polynomial of the Frobenius endomorphism.

- Complexity: $O(g^\beta (\log q)^{g^{O(1)}})$

- Related work: **Adleman, Huang, Wong, Ierardi** 1996, 1998

- Problem: Totally ineffective!
  (see **Kampkötter, Frey** 1991)

General (effective) methods

- $2g > \log q$: (conjectured) subexponential

$$L_{q^{2g+1}}[2.18] \quad \text{resp.} \quad L_{q^{2g+2}}[1.44].$$

- **S., Teske, Williams** 1998, 1999: Approximation + baby step-giant step or Pollard's kangaroo

$$O\left(g^2\, q^{\frac{2g-1}{5}}\, (\log q)^{\alpha}\right) \ .$$

- **Koblitz** 1989: $q = p^l$

$$O\,(\,p^g\, g\, (\log p)^{\alpha}\,)$$

Special Curves

- **Koblitz** 1989: Curves defined over $\mathbb{F}_2$ with base field $\mathbb{F}_{2^l}$. (Autom. of order $2l$)

- **Spallek** 1994: CM-method for $g = 2$; use quartic CM-fields of small class numbers.

- **Frey, Müller 1998**: $X_0(N)$-method; use modular curves.

- **Buhler, Koblitz** 1998: $V^2 + V = U^{2g+1}$ with base field $\mathbb{F}_p$ and complex multiplication by ζ_{2g+1}. (Autom. of order $2(2g+1)$)

- **Duursma, Sakurai** 1998: $V^2 = U^p - U + 1$ with base field $\mathbb{F}_{p^l}$. (Autom. of order $2lp$).

- **Chao, Matsuda, Nakamura, Tsujii** 1997/8: Global CM-method.

Approximation method

Situation:

- $k = \mathbb{F}_q$, $q = p^l$, $p > 2$
- $D(X) = X^{2g+2} + \ldots$ is a **randomly** selected squarefree polynomial.
- $\mathbf{C} : Y^2 = D(X) = X^{2g+2} + \ldots$
- $K = k(\mathbf{C}) = k(X)(Y)$ is a real quadratic function field of genus g over k.

Theorem: (F. K. Schmidt, 1931)

$$h = |J_C(K))| = h_X \, R_X \ ,$$

where R_X is the **regulator** of K and h_X is the **ideal class number** of K with respect to the **maximal order** $\mathcal{O}(X) = k[X][Y]$.

Aim: Find R, h_X, and h.

Example (record)

$$
\begin{aligned}
q &= 100000007 \approx 10^8 \\
D(X) &= X^8 + 11607007X^7 + 14154736X^6 \\
&+ 2837523X^5 + 18736251X^4 + 22879699X^3 \\
&+ 3879894X^2 + 48555574X + 77756256 \\
g &= 3 \\
R_X &= 1000008785601260429574717 \approx 10^{24} \\
h_X &= 1 \\
h &= 1000008785601260429574717 \approx 10^{24}
\end{aligned}
$$

Running time on a Pentium Pro/200 under Linux with SIMATH: 10 h 3 min

Comparison with “polynomial” time methods

Number of bit-operations of the approximation method:

$$O\left(g^2\, q^{\frac{2g-1}{5}}\, (\log q)^{\alpha}\right)\ .$$

In the record example, $g = 3$ and

$$q = 100000007 \approx (\log q)^6$$

Essentials of the algorithm

1. Compute an approximation E of $h = h'R$ and an integer L such that
$$|h - E| < L^2 \ .$$

2. Find a **multiple** h_0 of the regulator R in the interval $[E - L^2, E + L^2]$ by a **baby step-giant step** or by a **Kangaroo** approach.

3. Find R by trying the factors of h_0 and compute h and h'.

Aim: Find a **good** approximation E of h and a **sharp** bound L^2 on $|h - E|$.

Approximation ($g \le 2$)

Theorem (Hasse, Weil):

$$(\sqrt{q}-1)^{2g} \le h \le (\sqrt{q}+1)^{2g}$$

$g = 1$:

$$\begin{aligned} E &:= q+1\ , \\ L &:= \lceil \sqrt{2}\, q^{1/4} \rceil\ . \end{aligned}$$

$g = 2$:

$$\begin{aligned} E &:= q^2+6q+1\ , \\ L &:= \lceil 2\, q^{1/4} \sqrt{q+1} \rceil\ . \end{aligned}$$

Idea for $g > 2$

Assume h to be given as a product and

$$h = E' \cdot e^B$$

Find a sharp bound ψ on B, i.e.

$$|B| = |\log h - \log E'| < \psi.$$

Then $|e^B - 1| < e^\psi - 1$. We put

$$\begin{aligned} E &= \text{round}(E') \\ L &= \left\lceil \sqrt{E'(e^\psi - 1) + \tfrac{1}{2}} \right\rceil \end{aligned}$$

Then

$$\begin{aligned} |h - E| &\leq |h - E'| + |E' - E| \\ &\leq E'|e^B - 1| + \tfrac{1}{2} \\ &< E'(e^\psi - 1) + \tfrac{1}{2} \\ &\leq L^2 \end{aligned}$$

Analytic class number formula

$Y^2 = D(X)$ and $K = k(X)(Y)$ real quadratic

$\chi(P) := \left[\frac{D(X)}{P(X)}\right]$ for $P(X) \in k[X]$ monic, prime

$$h = \frac{q^{g+1}}{q-1} \prod_P \frac{1}{1 - \chi(P) q^{-\deg(P)}}$$

Then for any integer $n \geq 1$, we have

$$h = E'(n) \cdot e^{B(n)}$$

with

$$\begin{aligned} E'(n) &= \frac{q^{g+1}}{q-1} \prod_{\deg(P) \leq n} \frac{1}{1 - \chi(P) q^{-\deg(P)}} \\ B(n) &= \log \prod_{\deg(P) > n} \frac{1}{1 - \chi(P) q^{-\deg(P)}} \end{aligned}$$

Aim: Find an accurate bound $\psi(n)$ on $B(n)$ and a sufficient value of n.

Bound $B(n)$

$$\begin{aligned} B(n) &= \log \prod_{\deg(P)>n} \frac{1}{1-\chi(P)q^{-\deg(P)}} \\ &= \sum_{l=n+1} \frac{1}{l\,q^l} \sum_{\nu|l,\,\nu>l} \nu \sum_{\deg(P)=\nu} \chi(P)^{\frac{l}{\nu}} \end{aligned}$$

Theorem (S., Teske 1999): For $l \geq 1$

$$\sum_{\nu|l} \nu \sum_{\deg(P)=\nu} \chi(P)^{\frac{l}{\nu}} = -1 - \sum_{i=1}^{2g} \omega_i^l \ ,$$

where $|\omega_i| = \sqrt{q}$.

Möbius inversion yields for $\nu \geq 1$:

$$\nu \sum_{\deg(P)=\nu} \chi(P) = -\sum_{i=1}^{2g} \omega_i^{\nu} - \epsilon(\nu)\, q^{\frac{\nu}{2}} + O(\, q^{\frac{\nu}{6}}) \ ,$$

where $\epsilon(\nu) = 1$ if ν even, and 0 otherwise.

If we use that

$$\sum_{i=1}^{2g} \omega_i^{\nu} \leq 2g \cdot q^{\frac{\nu}{2}} \ ,$$

then

$$|B(n)| < \psi(n) = \tfrac{(2g+1)}{(n+1)}\, q^{-\frac{n+1}{2}} + O(\, q^{-\frac{n+2}{2}}\,) \ .$$

Put $E(n) = \mathrm{round}(E')$ and

$$L(n) = \left\lceil \sqrt{E'(n)(e^{\psi(n)} - 1) + \frac{1}{2}} \right\rceil \ .$$

Then for any integer $n \geq 1$:

$$|\, h \, - \, E(n) \,| \, < \, L(n)^2$$

and, since $e^{\psi(n)} - 1 \approx \psi(n)$,

$$L(n) = O(q^{\frac{g}{2} - \frac{n+1}{4}})$$

Optimal choice: $n := \mathrm{round}\left(\dfrac{2g-1}{5}\right) \ .$

Summary of the approximation

Let $n := \text{round}\left(\frac{2g-1}{5}\right)$. Compute

$$E' = \frac{q^{g+1}}{q-1} \prod_{\deg(P)\le n} \frac{1}{1-\chi(P)q^{-\deg(P)}} ,$$

where $P(X)$ runs through all monic prime polynomials of degree less than or equal to n and $\chi(P) = [D(X)/P(X)]$. Evaluate

$$\psi = \frac{(2g+1)}{(n+1)}\, q^{-\frac{n+1}{2}} + \epsilon$$

and put

$$\begin{aligned} E &:= \mathrm{Ne}\,(\,E'\,)\ , \\ L &= \left\lceil \sqrt{E'(e^{\psi}-1)+\frac{1}{2}} \right\rceil \end{aligned}$$

$\Rightarrow \left|\log \frac{h}{E'}\right| < \psi$ and

$$|\, h - E \,| < L^2$$

How sharp is the bound?

1. We estimated

$$\sum_{i=1}^{2g} \omega_i^{\nu} \leq 2g \cdot q^{\frac{\nu}{2}}$$

   For $q = p^2$, there exists **maximal function fields**, for which

$$\left| \sum_{i=1}^{2g} \omega_i^{\nu} \right| = 2g \cdot q^{\frac{\nu}{2}}$$

2. For $g = 3$ and $q = 10009$, we found polynomial $D(X)$, for which

$$|h - E| > 0.86 \cdot L^2$$

Heuristic Results

- In 99 % of all cases:

$$|h-E| \le \tfrac{1}{2}L^2$$

- In 50 % of all cases:

$$|h-E| \le \tfrac{1}{2g}L^2$$

- Average value of

$$\frac{|h-E|}{L^2} \sim \frac{1}{\alpha(g)}$$

  where $\alpha(g)$ appeared to be close to $2g$.

Remark: The knowledge of the average value of $|h-E|/L^2$ helps to speed up algorithms.

Question: Where does $\alpha(g)$ come from?

Let $\omega_j = \sqrt{q}e^{i\varphi_j}$, $\varphi_j \in [0, 2\pi[$, $j = 1, \ldots, 2g$, and $\varphi_{g+j} = -\varphi_j$ for $j = 1, \ldots, g$. Recall that $n = \text{round}\left(\frac{2g-1}{5}\right)$.

For large q and small genus, the observation $\text{mean}(|h - E|/L^2) \approx 1/\alpha(g)$ is equivalent to

1.

$$\text{mean}\left(\left|1 + \sum_{j=1}^{2g} e^{i(n+1)\varphi_j}\right|\right) = \frac{2g+1}{\alpha(g)}\ , \qquad n \text{ odd}$$

2.

$$\text{mean}\left(\left|\sum_{j=1}^{2g} e^{i(n+1)\varphi_j}\right|\right) = \frac{2g}{\alpha(g)}\ , \qquad n \text{ even}$$

Example: $g = 3$, $n = 1$,

$$\text{mean}\left(|1 + 2\sum_{i=1}^{3} cos(2\varphi_i)|\right) = \frac{7}{\alpha(3)}$$

Given

$$f(\varphi_1, \ldots, \varphi_g) = |1 + \sum_{j=1}^{2g} e^{i(n+1)\varphi_j}|$$

$$= |1 + \sum_{j=1}^{g} 2cos((n+1)\varphi_j)|$$

Then

$$\text{mean}(f) = \int_A f d\mu_g$$

$$= \int_{a_1}^{b_1} \ldots \int_{a_g}^{b_g} f(\varphi_1, \ldots, \varphi_g)\mu_g(d\varphi_1, \ldots, d\varphi_g)$$

Question: What is the correct distribution? What is μ_g?

$$g = 1$$

Birch 1968, **Sato, Tate** 1963:

The equidistribution takes place with respect to the Sato-Tate measure

$$\mu_1 = \tfrac{2}{\pi} \sin^2(\varphi_1) d\varphi_1 \quad (0 \leq \varphi_1 \leq \pi)$$

For instance, if $g = 1$ and $n = 1$, then

$$\begin{aligned} \text{mean}(f) &= \int_0^\pi f(\varphi_1)\mu_1(d\varphi_1) \\ &= \tfrac{2}{\pi} \int_0^\pi |1 + 2cos(2\varphi_1)| \sin^2(\varphi_1) d\varphi_1 \\ &= \tfrac{3\sqrt{3}}{2\pi} = 0.8269... \end{aligned}$$

$$g > 1$$

Katz, Sarnak 1999:
The equidistribution takes place with respect to the Haar measure of a maximal subgroup of the symplectic group Sp_{2g}. The explicit value of μ_g is due to **Weyl** 1946:

$$\mu_g = \frac{1}{g!} \prod_{i=1}^{2g} \frac{2}{\pi} \sin^2(\varphi_i) \prod_{i<j} 4(\cos(\varphi_i) - \cos(\varphi_j))^2 d\varphi_1 \cdots d\varphi_g$$

with $0 \leq \varphi_j \leq \pi$ for $j = 1, \ldots, g$.

For instance, if $g = 3$ and $n = 1$, then

$$f(\varphi_1, \varphi_2, \varphi_3) = |1 + 2cos(2\varphi_1) + 2cos(2\varphi_2) + 2cos(2\varphi_3)|$$

$$\begin{aligned} \mathrm{mean}(f) &= \int_0^\pi \int_0^\pi \int_0^\pi f(\varphi_1, \varphi_2, \varphi_3) \mu_3(d\varphi_1, d\varphi_2, d\varphi_3) \\ &= c \cdot \int_0^\pi \int_0^x \int_0^y f(x, y, z) \cdot a(x, y, z) dx dy dz \end{aligned}$$

with $c = 512/\pi^3$ and

$$\begin{aligned} a(x, y, z) &= \sin^2(x) \sin^2(y) \sin^2(z) (\cos(x) - \cos(y))^2 \\ &\quad \cdot (\cos(x) - \cos(z))^2 (\cos(y) - \cos(z))^2 \end{aligned}$$

Numerical evidence

Serre suggests

1. numerical integration: $g = 3$, $n = 1$

   $$\text{mean}(f) \approx 1.144...$$

   Compare with $1 + 1/2g = 7/6 = 1.166...$ and experimental results

   $$1.39 \le \text{mean}(f) \le 1.146$$

2. $f = |t|$. Find a **good polynomial approximation** $P(t)$ of $\sqrt{t}$ so that $P^2(t)$ is an even polynomial. If $\deg P(t)$ is reasonably small, then the integral can be evaluated.