Universal elliptic Gauss sums and applications

Christian Berghoff

Rheinische Friedrich-Wilhelms-Universität Bonn

November 19th, 2015

Table of Contents

Classical Gauss sum

Let $q \neq 2$ be a prime, $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mu_n, n \mid q-1$, ξ an n-th root of unity and ζ a q-th root of unity, $\langle g \rangle = \mathbb{F}_q^*$. A (cyclotomic) Gauss sum is defined as

$$\sum_{i=1}^{q-1} \chi(g^i)\zeta^{g^i} = \sum_{i=1}^{q-1} \xi^{mi}\zeta^{g^i}$$

Elliptic Curves

- Recall: Elliptic curve E over finite field $\mathbb{F}_p$ ($p \neq 2, 3$): $Y^2 = X^3 + AX + B$.

  Identify E with set of points $(X, Y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p$ satisfying the equation together with $\mathcal{O}$.
- We wish to determine $\#E(\mathbb{F}_p) = \#\{(X, Y) \in \mathbb{F}_p \times \mathbb{F}_p \mid (X, Y) \text{ lies on E}\} \cup \mathcal{O}$.
- Important problem related to ECC.

Definitions and Facts

- *ℓ-torsion*: $E[\ell] = \{P \in E \mid [\ell]P = \mathcal{O}\}$.
  Later on, ℓ will be prime, $\ell \neq p$. In this case

$$E[\ell] \cong \frac{\mathbb{Z}}{\ell\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell\mathbb{Z}}.$$

- *Frobenius endomorphism*:

$$\phi_p : E \to E, \quad (X, Y) \mapsto (X^p, Y^p)$$

  By restriction, ϕ_p acts as endomorphism of $E[\ell]$.
- *division polynomials* of E: Certain sequence of polynomials, so that

$$(X, Y) \in E[\ell] \Leftrightarrow \psi_\ell(X) = 0$$

  holds.

Bounds for $\#E(\mathbb{F}_p)$

Theorem (Hasse bound (1933))

Let E be an elliptic curve over $\mathbb{F}_p$. Then

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

Hence $\#E(\mathbb{F}_p) = p + 1 - t$, where $t \in \mathbb{Z}$ and $|t| \leq 2\sqrt{p}$.

Theorem

The Frobenius endomorphism satisfies the quadratic equation

$$\chi(\phi_p) := \phi_p^2 - t\phi_p + p = 0.$$

$\rightsquigarrow$ Schoof's algorithm

Further considerations

- Consider action of ϕ_p on $E[\ell]$.
- Consider roots of $\chi_\ell(\phi_p) = \phi_p^2 - t\phi_p + p \mod \ell$.
  1. Two roots in $\mathbb{F}_\ell \to \ell$ is an *Elkies prime*.
  2. No root in $\mathbb{F}_\ell \to \ell$ is an *Atkin prime*.
- In the first case $\chi_\ell(X)$ has a linear factor over $\mathbb{F}_\ell[X]$ $\to \psi_\ell(X)$ has factor $f_\ell(X) = \prod_{a=1}^{(\ell-1)/2}(X - (aP)_x)$ where $\varphi_p(P) = \lambda P$.
  $\rightsquigarrow$ Elkies procedure with improved run-time

Elliptic Gauss sum

Let χ be a Dirichlet character of order $n \mid \ell - 1$, then we define an *elliptic Gauss sum* (Mihailescu) as

$$\tau_e(\chi) = \sum_{a=1}^{\ell-1} \chi(a)(aP)_v, \quad \begin{cases} v = x, & n \equiv 1 \ (2), \\ v = y, & n \equiv 0 \ (2). \end{cases}$$

Lemma

The elliptic Gauss sum has the following properties:

1. $\tau_e(\chi)^n \in \mathbb{F}_p[\zeta_n]$
2. $\varphi_p(\tau_e(\chi)) = \chi^{-p}(\lambda)\tau_e(\chi^p)$

Modular functions I

Definition

1. Upper half-plane $\mathbb{H} := \{\tau \in \mathbb{C} : \quad \Im(\tau) > 0\}$.
2. $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}$ via

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \quad \mathbb{H} \to \mathbb{H}, \quad \tau \mapsto \frac{a\tau + b}{c\tau + d}.$$

Modular functions II

Definition

Let $f(\tau)$ be a meromorphic function on $\mathbb{H}$, $k \in \mathbb{Z}$. We call $f(\tau)$ a *modular function of weight* k for $\Gamma' \subseteq \mathrm{SL}_2(\mathbb{Z})$ (where we require $(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix})) \in \Gamma'$ for some $N \in \mathbb{N}$) if it satisfies the following conditions

1. $f(\gamma\tau) = (c\tau + d)^k f(\tau) \quad \forall \gamma = (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in \Gamma'$.
   In particular, this implies there is a Laurent series for $f(\tau)$ in terms of $q_N = \exp(\frac{2\pi i\tau}{N})$.
2. In the Laurent series for $f(\gamma\tau) = \sum_{n\in\mathbb{Z}} a_n q_N^n$ we have $a_n = 0$ for $n < n_0, n_0 \in \mathbb{Z} \; \forall \gamma \in \mathrm{SL}_2(\mathbb{Z})$.

In applications we focus on

$$\Gamma' = \Gamma_0(\ell) = \left\{\gamma = (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in \mathrm{SL}_2(\mathbb{Z}) : \quad c \equiv 0(\ell)\right\}, \quad \ell \text{ prime.}$$

Examples

$$E_{2k}(\tau) = \frac{1}{\zeta(2k)} \sum_{n,m\in\mathbb{Z}}{}' \frac{1}{(m+n\tau)^{2k}} \text{ for } k > 1,$$

$$\Delta(\tau) = \frac{E_4(\tau)^3 - E_6(\tau)^2}{1728},$$

$$j(\tau) = \frac{E_4(\tau)^3}{\Delta(\tau)},$$

$$\eta(q) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n),$$

$$m_\ell(\tau) = \ell^s \left(\frac{\eta(\ell\tau)}{\eta(\tau)}\right)^{2s}, \quad s = \min_{s\in\mathbb{N}} \left\{ s : \frac{s(\ell-1)}{12} \in \mathbb{N} \right\},$$

$$j(\ell\tau).$$

Facts on modular functions

Lemma

Modular functions of weight 0 form a field $\mathbf{A}_0(\Gamma')$.

Theorem

With notation as on the last slide, we have

1. $\mathbf{A}_0(\Gamma) = \mathbb{C}(j)$,
2. $\mathbf{A}_0(\Gamma_0(\ell)) = \mathbb{C}(j, f)$ *for* $f \in \mathbf{A}_0(\Gamma_0(\ell)) \setminus \mathbb{C}(j)$.

So, given $g \in \mathbf{A}_0(\Gamma_0(\ell))$, there exist $P_1, P_2 \in \mathbb{C}[X, Y]$ s. t.

$$g = \frac{P_1(f, j)}{P_2(f, j)}$$

We now focus on $f = m_\ell(\tau)$.

Facts on modular functions II

Lemma (B)

Let $g \in \mathbf{A}_0(\Gamma_0(\ell))$ *be holomorphic. Then* g *admits a representation of the form*

$$g(\tau) = \frac{Q(m_\ell, j)}{m_\ell^k \frac{\partial G_\ell}{\partial Y}(m_\ell, j)},$$

for some $k \geq 0$ *and a polynomial* $Q(X,Y) \in \mathbb{C}[X,Y]$, *where*

$$\deg_Y(Q) < \deg_Y(G_\ell) = \min_{s \in \mathbb{N}} \left\{ v = \frac{s(\ell-1)}{12} : v \in \mathbb{N} \right\}$$

and $G_\ell(X,j)$ *is the minimal polynomial of* m_ℓ *over* $\mathbb{C}(j)$.

Tate curve

Proposition (Tate)

Let E_4, E_6 be as before. Then the quantities

$$x(w,q) = \frac{1}{12} + \frac{w}{(1-w)^2} + \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} mq^{nm}(w^m + w^{-m}) - 2mq^{nm},$$

$$y(w,q) = \frac{w+w^2}{2(1-w)^3} + \frac{1}{2}\sum_{n=1}^{\infty}\sum_{m=1}^{\infty} \frac{m(m+1)}{2}\Big(q^{nm}(w^m - w^{-m}) + q^{n(m+1)}(w^{m+1} - w^{-(m+1)})\Big)$$

satisfy

$$E_q : \quad y(w,q)^2 = x(w,q)^3 - \frac{E_4(q)}{48}x(w,q) + \frac{E_6(q)}{864}.$$

E_q is called the Tate curve which parametrizes isomorphism classes of elliptic curves over $\mathbb{C}$.

Universal elliptic Gauss sums

Lemma (B)

Let ℓ be a prime, $n \mid \ell - 1$, $\chi : \mathbb{F}_\ell^* \mapsto \mu_n$ a Dirichlet character, ζ an ℓ-th root of unity and let r, e_Δ be appropriately chosen integers. Let in addition $V = x$ for odd and $V = y$ for even n and define

$$G_{\ell,n}(q) = \sum_{\lambda \in \mathbb{F}_\ell^*} \chi(\lambda) V(\zeta^\lambda, q), \quad p_1(q) = \sum_{\lambda \in \mathbb{F}_\ell^*} x(\zeta^\lambda, q).$$

Then

$$\tau_{\ell,n}(q) := \frac{G_{\ell,n}(q)^n p_1(q)^r}{\Delta(q)^{e_\Delta}},$$

is a modular function of weight 0 for $\Gamma_0(\ell)$, holomorphic on $\mathbb{H}$ and has coefficients in $\mathbb{Q}[\zeta_n]$. We call it a universal elliptic Gauss sum.

Proof.

Study behaviour of Weierstraß $\wp$-function under action of $SL_2(\mathbb{Z})$ and use connection between $x(w, q), y(w, q)$ and $\wp(z, \tau), \wp'(z, \tau)$. □

An algorithm for computing

By general lemma we find

$$\tau_{\ell,n}(q) = \frac{Q(m_\ell, j)}{m_\ell^k \frac{\partial G_\ell}{\partial Y}(m_\ell, j)}.$$

So use the following algorithm:

1. Compute $\tau_{\ell,n}(q)\frac{\partial G_\ell}{\partial Y}(m_\ell, j) =: s$ up to precision $\mathrm{prec}(\ell, n)$, $Q := 0$.
2. Determine $o = \mathrm{ord}(s)$ and $(i, k): \ iv - k = o$ and $k < v$.
3. Compute $s := s - cm_\ell^i j^k$, $Q := Q + cX^i Y^k$
4. Repeat 2 and 3 until $s = 0$.

Required precision

Lemma (B.)

We can take $\mathrm{prec}(\ell, n) = (v + e_\Delta)\ell$.

Run-time:

- Compute $\tau_{\ell,n}(q)$: $\tilde{\mathcal{O}}(\ell n v)$
- Determine Q: $\tilde{\mathcal{O}}(\ell^2 v^2)$

Application

Recall Schoof's algorithm (1985)

- Compute $\#E(\mathbb{F}_p) = p + 1 - t$, $|t| \leq 2\sqrt{p}$
- $\rightsquigarrow$ Determine $t \mod \ell$ for small primes ℓ by finding t s. t. $\varphi_p^2 - t\varphi_p + p \equiv 0 \mod \ell$, then use CRT
- First polynomial algorithm (in $\log p$)
- If ℓ is Elkies prime: Use polynomials of lower degree $\Rightarrow$ power saving in run-time
- If ℓ is Atkin prime: Generic approach of equal run-time + sophisticated BSGS

$\rightsquigarrow$ SEA combines Elkies (mostly) + Atkin procedures

Elkies procedure

Need to find λ s. t. $\varphi_p(P) = \lambda P$ for ℓ-torsion point P.
$\rightsquigarrow$ Compute in $\mathbb{F}_p[X]/(f_\ell(X))$, extension of degree $\mathcal{O}(\ell)$.

Lemma (Mihailescu, 2006)

Let ℓ be a prime, χ be a character with $\operatorname{ord}(\chi) = n || \ell - 1$. Let $\tau_e(\chi)$ be the elliptic Gauss sum. Then

$$\varphi_p(\tau_e(\chi)) = \chi^{-p}(\lambda)\tau_e(\chi^p)$$

Writing $p = nq + m$, one obtains

$$(\tau_e(\chi))^n)^q \cdot \frac{\tau_e(\chi)^m}{\tau_e(\chi^m)} = \chi^{-m}(\lambda)$$

Both factors lie in $\mathbb{F}_p[\zeta_n]$, computations can be done in extension of degree $\mathcal{O}(n)$ and no searching for λ is required.

Compute the factors

Use universal elliptic Gauss sums: We know

$$\tau_{\ell,n}(q) = \frac{G_{\ell,n}(q)^n p_1(q)^r}{\Delta(q)^{e_\Delta}} = R(j(q), m_\ell(q)).$$

Substitute $q = \exp(2\pi i \tau(E)) \Rightarrow \tau_{\ell,n}(E) = R(j(E), m_\ell(E))$ for curve E in question.
Hence, compute $j(E), \Delta(E), p_1(E)$ and obtain $m_\ell(E)$ as root of $G_\ell(X, j(E))$. $\rightsquigarrow$ Compute $\tau_e(\chi)^n$ for our E
Similar approach for Jacobi sums $\rightsquigarrow$ determine $\lambda \mod n$ for all $n || \ell - 1$.
CRT gives index of λ in $(\mathbb{Z}/\ell\mathbb{Z})^*$ $\rightsquigarrow$ $t = \lambda + p/\lambda \mod \ell$ and t.

Further research

1. Replace m_ℓ by other modular functions to improve run-time
2. Analyse coefficient size
3. ?

Merci pour votre attention