Explicit computation of Gross-Stark units over real quadratic base fields

Paul Thomas Young

College of Charleston

December 19, 2012

Acknowledgments

This talk represents joint work with Brett Tangedal, UNCG.

"On p-adic multiple zeta and log gamma functions", *J. Number Theory* **131.7** (2011), 1240-1257.

"Explicit computation of Gross-Stark units over real quadratic fields", *J. Number Theory* **133.3** (2013), 1045-1061.

This work is dedicated to the memory of our mentor David R. Hayes.

Thanks to:

Acknowledgments

This talk represents joint work with Brett Tangedal, UNCG.

"On p-adic multiple zeta and log gamma functions", *J. Number Theory* **131.7** (2011), 1240-1257.

"Explicit computation of Gross-Stark units over real quadratic fields", *J. Number Theory* **133.3** (2013), 1045-1061.

This work is dedicated to the memory of our mentor David R. Hayes.

Thanks to:

- College of Charleston Mathematics Department

Acknowledgments

This talk represents joint work with Brett Tangedal, UNCG.

"On p-adic multiple zeta and log gamma functions", *J. Number Theory* **131.7** (2011), 1240-1257.

"Explicit computation of Gross-Stark units over real quadratic fields", *J. Number Theory* **133.3** (2013), 1045-1061.

This work is dedicated to the memory of our mentor David R. Hayes.

Thanks to:

- College of Charleston Mathematics Department
- Department of Mathematics and Statistics, University of North Carolina, Greensboro

and especially

Acknowledgments

This talk represents joint work with Brett Tangedal, UNCG.

"On p-adic multiple zeta and log gamma functions", *J. Number Theory* **131.7** (2011), 1240-1257.

"Explicit computation of Gross-Stark units over real quadratic fields", *J. Number Theory* **133.3** (2013), 1045-1061.

This work is dedicated to the memory of our mentor David R. Hayes.

Thanks to:

- College of Charleston Mathematics Department
- Department of Mathematics and Statistics,
  University of North Carolina, Greensboro

  and especially

- Brett, Ann, and Elise Tangedal

Hilbert's Twelfth Problem

D. Hilbert, Paris 1900: Given a finite extension field F of $\mathbb{Q}$, give an *analytic* construction of all abelian extensions K of F, using only information from F.

Hilbert's Twelfth Problem

D. Hilbert, Paris 1900: Given a finite extension field F of $\mathbb{Q}$, give an *analytic* construction of all abelian extensions K of F, using only information from F.

- **Kronecker, Weber (1877, 1886, 1896, 1908):** Every abelian extension K of $F = \mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(e^{2\pi i/n})$ for some positive integer n.

Hilbert's Twelfth Problem

D. Hilbert, Paris 1900: Given a finite extension field F of $\mathbb{Q}$, give an *analytic* construction of all abelian extensions K of F, using only information from F.

- **Kronecker, Weber (1877, 1886, 1896, 1908):** Every abelian extension K of $F = \mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(e^{2\pi i/n})$ for some positive integer n.
- That is, every abelian extension K of $\mathbb{Q}$ may be obtained from $\mathbb{Q}$ by adjoining values of the analytic function $f(z) = e^{2\pi iz}$ for $z \in \mathbb{Q}$.

Hilbert's Twelfth Problem

D. Hilbert, Paris 1900: Given a finite extension field F of $\mathbb{Q}$, give an *analytic* construction of all abelian extensions K of F, using only information from F.

- **Kronecker, Weber (1877, 1886, 1896, 1908):** Every abelian extension K of $F = \mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(e^{2\pi i/n})$ for some positive integer n.
- That is, every abelian extension K of $\mathbb{Q}$ may be obtained from $\mathbb{Q}$ by adjoining values of the analytic function $f(z) = e^{2\pi iz}$ for $z \in \mathbb{Q}$.
- **Takagi (1920):** If $F = \mathbb{Q}(\sqrt{-d})$ is an *imaginary quadratic* field, then every abelian extension K of F may be obtained by adjoining to F values of $f(z) = e^{2\pi iz}$; the elliptic modular function $j(\tau)$; and/or the Weierstrass $\wp$ function $\wp(z,\tau)$ for $z \in \mathbb{Q}$, $\tau \in F$.

Hilbert's Twelfth Problem

D. Hilbert, Paris 1900: Given a finite extension field F of $\mathbb{Q}$, give an *analytic* construction of all abelian extensions K of F, using only information from F.

- **Kronecker, Weber (1877, 1886, 1896, 1908):** Every abelian extension K of $F = \mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(e^{2\pi i/n})$ for some positive integer n.
- That is, every abelian extension K of $\mathbb{Q}$ may be obtained from $\mathbb{Q}$ by adjoining values of the analytic function $f(z) = e^{2\pi iz}$ for $z \in \mathbb{Q}$.
- **Takagi (1920):** If $F = \mathbb{Q}(\sqrt{-d})$ is an *imaginary quadratic* field, then every abelian extension K of F may be obtained by adjoining to F values of $f(z) = e^{2\pi iz}$; the elliptic modular function $j(\tau)$; and/or the Weierstrass $\wp$ function $\wp(z, \tau)$ for $z \in \mathbb{Q}$, $\tau \in F$.
- **T,Y (2012)** If K is a totally complex abelian extension of a *real quadratic* field $F = \mathbb{Q}(\sqrt{d})$, then K is generated by *p-adic* exponentials of values of our *p-adic* double log gamma function $G_{p,2}(z; (\omega_1, \omega_2))$ for $z, \omega_i \in F$.

Hilbert's Twelfth Problem

D. Hilbert, Paris 1900: Given a finite extension field F of $\mathbb{Q}$, give an *analytic* construction of all abelian extensions K of F, using only information from F.

- **Kronecker, Weber (1877, 1886, 1896, 1908):** Every abelian extension K of $F = \mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(e^{2\pi i/n})$ for some positive integer n.
- That is, every abelian extension K of $\mathbb{Q}$ may be obtained from $\mathbb{Q}$ by adjoining values of the analytic function $f(z) = e^{2\pi iz}$ for $z \in \mathbb{Q}$.
- **Takagi (1920):** If $F = \mathbb{Q}(\sqrt{-d})$ is an *imaginary quadratic* field, then every abelian extension K of F may be obtained by adjoining to F values of $f(z) = e^{2\pi iz}$; the elliptic modular function $j(\tau)$; and/or the Weierstrass $\wp$ function $\wp(z, \tau)$ for $z \in \mathbb{Q}$, $\tau \in F$.
- **T,Y (2012)** If K is a totally complex abelian extension of a *real quadratic* field $F = \mathbb{Q}(\sqrt{d})$, then K is generated by *p-adic* exponentials of values of our *p-adic* double log gamma function $G_{p,2}(z; (\omega_1, \omega_2))$ for $z, \omega_i \in F$.
- Using these p-adic functions, we give an effective, efficient algorithm that explicitly constructs K from F analytically (p-adic analytically).

Algebraic Number Fields

A *number field* K is a finite (algebraic) extension field of $\mathbb{Q}$, of dimension $n = [K : \mathbb{Q}]$. Associated to it we have:

Algebraic Number Fields

A *number field* K is a finite (algebraic) extension field of $\mathbb{Q}$, of dimension $n = [K : \mathbb{Q}]$. Associated to it we have:

- Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ of field automorphisms of K. If $|G| = [K : \mathbb{Q}]$ then K is a *Galois extension* of $\mathbb{Q}$, and if G is also abelian then K is an *abelian extension* of $\mathbb{Q}$.

Algebraic Number Fields

A *number field* K is a finite (algebraic) extension field of $\mathbb{Q}$, of dimension $n = [K : \mathbb{Q}]$. Associated to it we have:

- Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ of field automorphisms of K. If $|G| = [K : \mathbb{Q}]$ then K is a *Galois extension* of $\mathbb{Q}$, and if G is also abelian then K is an *abelian extension* of $\mathbb{Q}$.
- Ring $\mathcal{O}_K = \{\alpha \in K : \exists \,\mathrm{monic}\, f \in \mathbb{Z}[x],\ f(\alpha) = 0\}$ of *algebraic integers* of K.

Algebraic Number Fields

A *number field* K is a finite (algebraic) extension field of $\mathbb{Q}$, of dimension $n = [K : \mathbb{Q}]$. Associated to it we have:

- Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ of field automorphisms of K. If $|G| = [K : \mathbb{Q}]$ then K is a *Galois extension* of $\mathbb{Q}$, and if G is also abelian then K is an *abelian extension* of $\mathbb{Q}$.
- Ring $\mathcal{O}_K = \{\alpha \in K : \exists \, \mathrm{monic} \, f \in \mathbb{Z}[x], \ f(\alpha) = 0\}$ of *algebraic integers* of K.
- Multiplicative group $\mathcal{O}_K^\times$ of units of $\mathcal{O}_K$.

Algebraic Number Fields

A *number field* K is a finite (algebraic) extension field of $\mathbb{Q}$, of dimension $n = [K : \mathbb{Q}]$. Associated to it we have:

- Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ of field automorphisms of K. If $|G| = [K : \mathbb{Q}]$ then K is a *Galois extension* of $\mathbb{Q}$, and if G is also abelian then K is an *abelian extension* of $\mathbb{Q}$.
- Ring $\mathcal{O}_K = \{\alpha \in K : \exists \, \mathrm{monic} \, f \in \mathbb{Z}[x], \, f(\alpha) = 0\}$ of *algebraic integers* of K.
- Multiplicative group $\mathcal{O}_K^\times$ of units of $\mathcal{O}_K$.
- Every ideal $\mathcal{A}$ of $\mathcal{O}_K$ has a unique factorization as a product of prime ideals.

Algebraic Number Fields

A *number field* K is a finite (algebraic) extension field of $\mathbb{Q}$, of dimension $n = [K : \mathbb{Q}]$. Associated to it we have:

- Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ of field automorphisms of K. If $|G| = [K : \mathbb{Q}]$ then K is a *Galois extension* of $\mathbb{Q}$, and if G is also abelian then K is an *abelian extension* of $\mathbb{Q}$.
- Ring $\mathcal{O}_K = \{\alpha \in K : \exists \, \mathrm{monic} \, f \in \mathbb{Z}[x], \ f(\alpha) = 0\}$ of *algebraic integers* of K.
- Multiplicative group $\mathcal{O}_K^\times$ of units of $\mathcal{O}_K$.
- Every ideal $\mathcal{A}$ of $\mathcal{O}_K$ has a unique factorization as a product of prime ideals.
- Every nonzero ideal $\mathcal{A}$ of $\mathcal{O}_K$ has finite index in $\mathcal{O}_K$, called the *norm* of $\mathcal{A}$, $N\mathcal{A} = |\mathcal{O}_K/\mathcal{A}|$.

Algebraic Number Fields

A *number field* K is a finite (algebraic) extension field of $\mathbb{Q}$, of dimension $n = [K : \mathbb{Q}]$. Associated to it we have:

- Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ of field automorphisms of K. If $|G| = [K : \mathbb{Q}]$ then K is a *Galois extension* of $\mathbb{Q}$, and if G is also abelian then K is an *abelian extension* of $\mathbb{Q}$.
- Ring $\mathcal{O}_K = \{\alpha \in K : \exists \,\mathrm{monic}\, f \in \mathbb{Z}[x],\ f(\alpha) = 0\}$ of *algebraic integers* of K.
- Multiplicative group $\mathcal{O}_K^\times$ of units of $\mathcal{O}_K$.
- Every ideal $\mathcal{A}$ of $\mathcal{O}_K$ has a unique factorization as a product of prime ideals.
- Every nonzero ideal $\mathcal{A}$ of $\mathcal{O}_K$ has finite index in $\mathcal{O}_K$, called the *norm* of $\mathcal{A}$, $N\mathcal{A} = |\mathcal{O}_K/\mathcal{A}|$.
- *Dedekind zeta function* of K, for $\Re(s) > 1$:

$$\zeta_K(s) = \sum_{\text{ideals } \mathcal{A}} N\mathcal{A}^{-s} = \prod_{\text{prime ideals } \mathcal{P}} (1 - N\mathcal{P}^{-s})^{-1}.$$

Analytic class number formula

The Dedekind zeta function ζ_K of K has an analytic continuation to $\mathbb{C}$ except for a simple pole at $s = 1$, with residue

$$\lim_{s \to 1} (s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K \sqrt{|d_K|}},$$

where

Analytic class number formula

The Dedekind zeta function ζ_K of K has an analytic continuation to $\mathbb{C}$ except for a simple pole at $s = 1$, with residue

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K \sqrt{|d_K|}},$$

where

- r_1 is the number of real embeddings of K, and r_2 is the number of pairs of complex embeddings of K;

Analytic class number formula

The Dedekind zeta function ζ_K of K has an analytic continuation to $\mathbb{C}$ except for a simple pole at $s = 1$, with residue

$$\lim_{s \to 1} (s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K \sqrt{|d_K|}},$$

where

- r_1 is the number of real embeddings of K, and r_2 is the number of pairs of complex embeddings of K;
- h_K is the *class number*, which measures how far $\mathcal{O}_K$ is from having unique factorization; $\mathcal{O}_K$ is a UFD $\iff h_K = 1$;

Analytic class number formula

The Dedekind zeta function ζ_K of K has an analytic continuation to $\mathbb{C}$ except for a simple pole at $s = 1$, with residue

$$\lim_{s \to 1} (s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K \sqrt{|d_K|}},$$

where

- r_1 is the number of real embeddings of K, and r_2 is the number of pairs of complex embeddings of K;
- h_K is the *class number*, which measures how far $\mathcal{O}_K$ is from having unique factorization; $\mathcal{O}_K$ is a UFD $\iff h_K = 1$;
- The *regulator* R_K of K is a certain determinant formed from the $r_1 + r_2 - 1$ generators of the torsion-free part of unit group $\mathcal{O}_K^\times$, which measures how "dense" the units are in $\mathcal{O}_K$;

Analytic class number formula

The Dedekind zeta function ζ_K of K has an analytic continuation to $\mathbb{C}$ except for a simple pole at $s = 1$, with residue

$$\lim_{s \to 1} (s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K \sqrt{|d_K|}},$$

where

- r_1 is the number of real embeddings of K, and r_2 is the number of pairs of complex embeddings of K;
- h_K is the *class number*, which measures how far $\mathcal{O}_K$ is from having unique factorization; $\mathcal{O}_K$ is a UFD $\iff h_K = 1$;
- The *regulator* R_K of K is a certain determinant formed from the $r_1 + r_2 - 1$ generators of the torsion-free part of unit group $\mathcal{O}_K^\times$, which measures how "dense" the units are in $\mathcal{O}_K$;
- w_K is the number of roots of unity in K;

Analytic class number formula

The Dedekind zeta function ζ_K of K has an analytic continuation to $\mathbb{C}$ except for a simple pole at $s = 1$, with residue

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K \sqrt{|d_K|}},$$

where

- r_1 is the number of real embeddings of K, and r_2 is the number of pairs of complex embeddings of K;
- h_K is the *class number*, which measures how far $\mathcal{O}_K$ is from having unique factorization; $\mathcal{O}_K$ is a UFD $\iff h_K = 1$;
- The *regulator* R_K of K is a certain determinant formed from the $r_1 + r_2 - 1$ generators of the torsion-free part of unit group $\mathcal{O}_K^\times$, which measures how "dense" the units are in $\mathcal{O}_K$;
- w_K is the number of roots of unity in K;
- d_K is the *discriminant* of K.

Partial zeta functions

Suppose K is a totally complex abelian extension of a real quadratic field F, with $G = \mathrm{Gal}(K/F)$. Choose a prime (p) of $\mathbb{Z}$ which splits as $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ in F, and such that $\mathfrak{p}$ splits completely in K. Let the set T consist of $\bar{\mathfrak{p}}$ together with all infinite primes of $\mathcal{O}_F$ and all finite primes of $\mathcal{O}_F$ which ramify in K, and $S = T \cup \{\mathfrak{p}\}$. Associated to every $\sigma \in G$ there is a *partial zeta function* $\zeta_S(s;\sigma)$ defined by

$$\zeta_S(s;\sigma) = \sum_{\sigma_{\mathcal{A}}=\sigma} N\mathcal{A}^{-s}, \qquad (\Re(s) > 1),$$

where the sum is over all ideals $\mathcal{A}$ of $\mathcal{O}_K$ relatively prime to all ideals in the set S and having the specified automorphism $\sigma_{\mathcal{A}} = \sigma$ as its image in G under the *Artin map*. It has an analytic continuation to all of $\mathbb{C}$ except a simple pole at $s = 1$.

Partial zeta functions

Suppose K is a totally complex abelian extension of a real quadratic field F, with $G = \mathrm{Gal}(K/F)$. Choose a prime (p) of $\mathbb{Z}$ which splits as $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in F, and such that $\mathfrak{p}$ splits completely in K. Let the set T consist of $\overline{\mathfrak{p}}$ together with all infinite primes of $\mathcal{O}_F$ and all finite primes of $\mathcal{O}_F$ which ramify in K, and $S = T \cup \{\mathfrak{p}\}$. Associated to every $\sigma \in G$ there is a *partial zeta function* $\zeta_S(s;\sigma)$ defined by

$$\zeta_S(s;\sigma) = \sum_{\sigma_{\mathcal{A}}=\sigma} N\mathcal{A}^{-s}, \qquad (\Re(s) > 1),$$

where the sum is over all ideals $\mathcal{A}$ of $\mathcal{O}_K$ relatively prime to all ideals in the set S and having the specified automorphism $\sigma_{\mathcal{A}} = \sigma$ as its image in G under the *Artin map*. It has an analytic continuation to all of $\mathbb{C}$ except a simple pole at $s = 1$.

- **Cassou-Nogues (1979):** There also exists a p-adic partial zeta function $\zeta_{S,p}(s,\sigma)$ for each $\sigma \in G$ such that

$$\zeta_{S,p}(-k;\sigma) = \zeta_S(-k;\sigma) \quad \text{for} \quad k \equiv 0 \pmod{p-1}$$

and $\zeta_{S,p}(s,\sigma)$ is p-adically analytic on a disc in $\mathbb{C}_p$ containing $s = 0$.

Gross' refined conjecture (1982)

Let F, K, $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, S, and T be as above, and define the subgroup

$$U_{\mathfrak{p}} = \{\beta \in K^\times : |\beta|_{\mathfrak{Q}} = 1 \quad \text{if} \quad \mathfrak{Q} \not| \, \mathfrak{p}\} \quad \text{of} \quad K^\times.$$

Fix a prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$ lying over $\mathfrak{p}$ and denote by $x \mapsto x_{\mathfrak{P}}$ the embedding of K into $\mathbb{Q}_p$ corresponding to $\mathfrak{P}$. Then there exists a unique element $\alpha \in U_{\mathfrak{p}}$ such that

Gross' refined conjecture (1982)

Let F, K, $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, S, and T be as above, and define the subgroup

$$U_{\mathfrak{p}} = \{\beta \in K^\times : |\beta|_{\mathfrak{Q}} = 1 \quad \text{if} \quad \mathfrak{Q} \not| \, \mathfrak{p}\} \quad \text{of} \quad K^\times.$$

Fix a prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$ lying over $\mathfrak{p}$ and denote by $x \mapsto x_{\mathfrak{P}}$ the embedding of K into $\mathbb{Q}_p$ corresponding to $\mathfrak{P}$. Then there exists a unique element $\alpha \in U_{\mathfrak{p}}$ such that

- $(\sigma(\alpha))_{\mathfrak{P}} = p^{w_p \zeta_T(0;\sigma)} \exp_p(-w_p \zeta'_{S,p}(0;\sigma))$ for all $\sigma \in G$, and

Gross' refined conjecture (1982)

Let F, K, $(p) = \mathfrak{p}\overline{\mathfrak{p}}$, S, and T be as above, and define the subgroup

$$U_{\mathfrak{p}} = \{\beta \in K^{\times} : |\beta|_{\mathfrak{Q}} = 1 \quad \text{if} \quad \mathfrak{Q} \not| \, \mathfrak{p}\} \quad \text{of} \quad K^{\times}.$$

Fix a prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$ lying over $\mathfrak{p}$ and denote by $x \mapsto x_{\mathfrak{P}}$ the embedding of K into $\mathbb{Q}_p$ corresponding to $\mathfrak{P}$. Then there exists a unique element $\alpha \in U_{\mathfrak{p}}$ such that

- $(\sigma(\alpha))_{\mathfrak{P}} = p^{w_p \zeta_T(0;\sigma)} \exp_p(-w_p \zeta'_{S,p}(0;\sigma))$ for all $\sigma \in G$, and
- $K(\alpha^{1/w_K})$ is an abelian extension of F.

Gross' refined conjecture (1982)

Let F, K, $(p) = \mathfrak{p}\overline{\mathfrak{p}}$, S, and T be as above, and define the subgroup

$$U_{\mathfrak{p}} = \{\beta \in K^\times : |\beta|_{\mathfrak{Q}} = 1 \quad \text{if} \quad \mathfrak{Q} \nmid \mathfrak{p}\} \quad \text{of} \quad K^\times.$$

Fix a prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$ lying over $\mathfrak{p}$ and denote by $x \mapsto x_{\mathfrak{P}}$ the embedding of K into $\mathbb{Q}_p$ corresponding to $\mathfrak{P}$. Then there exists a unique element $\alpha \in U_{\mathfrak{p}}$ such that

- $(\sigma(\alpha))_{\mathfrak{P}} = p^{w_p \zeta_T(0;\sigma)} \exp_p(-w_p \zeta'_{S,p}(0;\sigma))$ for all $\sigma \in G$, and
- $K(\alpha^{1/w_K})$ is an abelian extension of F.
- In this formula w_p denotes the number of roots of unity in $\mathbb{Q}_p$, and $\exp_p(x) = \sum_k (x^k/k!)$ is the p-adic exponential, convergent for $x \in 2p\mathbb{Z}_p$. It is known that $w_p \zeta_T(0;\sigma)$ is an integer; there are efficient algorithms for computing it (Tangedal, JNT 2007).

Gross' refined conjecture (1982)

Let F, K, $(p) = \mathfrak{p}\overline{\mathfrak{p}}$, S, and T be as above, and define the subgroup

$$U_{\mathfrak{p}} = \{\beta \in K^{\times} : |\beta|_{\mathfrak{Q}} = 1 \quad \text{if} \quad \mathfrak{Q} \not| \mathfrak{p}\} \quad \text{of} \quad K^{\times}.$$

Fix a prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$ lying over $\mathfrak{p}$ and denote by $x \mapsto x_{\mathfrak{P}}$ the embedding of K into $\mathbb{Q}_p$ corresponding to $\mathfrak{P}$. Then there exists a unique element $\alpha \in U_{\mathfrak{p}}$ such that

- $(\sigma(\alpha))_{\mathfrak{P}} = p^{w_p \zeta_T(0;\sigma)} \exp_p(-w_p \zeta'_{S,p}(0;\sigma))$ for all $\sigma \in G$, and
- $K(\alpha^{1/w_K})$ is an abelian extension of F.
- In this formula w_p denotes the number of roots of unity in $\mathbb{Q}_p$, and $\exp_p(x) = \sum_k (x^k/k!)$ is the p-adic exponential, convergent for $x \in 2p\mathbb{Z}_p$. It is known that $w_p \zeta_T(0;\sigma)$ is an integer; there are efficient algorithms for computing it (Tangedal, JNT 2007).
- This theorem was recently proved (Annals 2011), in the case described above, by Darmon, Dasgupta, and Pollack, without directly constructing α.

Gross' refined conjecture (1982)

Let F, K, $(p) = \mathfrak{p}\overline{\mathfrak{p}}$, S, and T be as above, and define the subgroup

$$U_{\mathfrak{p}} = \{\beta \in K^{\times} : |\beta|_{\mathfrak{Q}} = 1 \quad \text{if} \quad \mathfrak{Q} \nmid \mathfrak{p}\} \quad \text{of} \quad K^{\times}.$$

Fix a prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$ lying over $\mathfrak{p}$ and denote by $x \mapsto x_{\mathfrak{P}}$ the embedding of K into $\mathbb{Q}_p$ corresponding to $\mathfrak{P}$. Then there exists a unique element $\alpha \in U_{\mathfrak{p}}$ such that

- $(\sigma(\alpha))_{\mathfrak{P}} = p^{w_p \zeta_T(0;\sigma)} \exp_p(-w_p \zeta'_{S,p}(0;\sigma))$ for all $\sigma \in G$, and
- $K(\alpha^{1/w_K})$ is an abelian extension of F.
- In this formula w_p denotes the number of roots of unity in $\mathbb{Q}_p$, and $\exp_p(x) = \sum_k (x^k/k!)$ is the p-adic exponential, convergent for $x \in 2p\mathbb{Z}_p$. It is known that $w_p \zeta_T(0;\sigma)$ is an integer; there are efficient algorithms for computing it (Tangedal, JNT 2007).
- This theorem was recently proved (Annals 2011), in the case described above, by Darmon, Dasgupta, and Pollack, without directly constructing α.
- Brett and I give an algorithm using $G_{p,2}$ to compute the right side in $\mathbb{Q}_p$, and explicitly gives the irreducible polynomial $f_\alpha \in F[X]$ whose roots are the $\sigma(\alpha)$.

The algorithm

First, explicitly choose a real quadratic field $F = \mathbb{Q}(\sqrt{d})$ with $d > 0$ to serve as base field; also choose a prime (p) of $\mathbb{Z}$ that splits as $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in $\mathcal{O}_F$.

The algorithm

First, explicitly choose a real quadratic field $F = \mathbb{Q}(\sqrt{d})$ with $d > 0$ to serve as base field; also choose a prime (p) of $\mathbb{Z}$ that splits as $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ in $\mathcal{O}_F$.

- Use characters on the ray class group $H_+(\mathfrak{m})$ for a suitable ideal $\mathfrak{m}$ to specify a totally complex abelian extension K of F in which $\mathfrak{p}$ splits completely; the Galois group $G = \mathrm{Gal}(K/F)$ is a specified subgroup of $H_+(\mathfrak{m})$.

The algorithm

First, explicitly choose a real quadratic field $F = \mathbb{Q}(\sqrt{d})$ with $d > 0$ to serve as base field; also choose a prime (p) of $\mathbb{Z}$ that splits as $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ in $\mathcal{O}_F$.

- Use characters on the ray class group $H_+(\mathfrak{m})$ for a suitable ideal $\mathfrak{m}$ to specify a totally complex abelian extension K of F in which $\mathfrak{p}$ splits completely; the Galois group $G = \mathrm{Gal}(K/F)$ is a specified subgroup of $H_+(\mathfrak{m})$.
- Compute the values $w_p \zeta_T(0; \sigma)$ and $\exp_p(-w_p \zeta'_{S,p}(0; \sigma))$ for all $\sigma \in G$; these are computed in $\mathbb{Q}_p$ using our $G_{p,2}$ function, to any desired accuracy.

The algorithm

First, explicitly choose a real quadratic field $F = \mathbb{Q}(\sqrt{d})$ with $d > 0$ to serve as base field; also choose a prime (p) of $\mathbb{Z}$ that splits as $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ in $\mathcal{O}_F$.

- Use characters on the ray class group $H_+(\mathfrak{m})$ for a suitable ideal $\mathfrak{m}$ to specify a totally complex abelian extension K of F in which $\mathfrak{p}$ splits completely; the Galois group $G = \mathrm{Gal}(K/F)$ is a specified subgroup of $H_+(\mathfrak{m})$.
- Compute the values $w_p \zeta_T(0;\sigma)$ and $\exp_p(-w_p \zeta'_{S,p}(0;\sigma))$ for all $\sigma \in G$; these are computed in $\mathbb{Q}_p$ using our $G_{p,2}$ function, to any desired accuracy.
- By Gross' formula, we now know all $\sigma(\alpha)$ as elements of $\mathbb{Q}_p$ to any desired accuracy; we then must realize the coefficients of the polynomial $f_\alpha(x) = \prod_{\sigma \in G}(x - \sigma(\alpha))$ as elements of F.

The algorithm

First, explicitly choose a real quadratic field $F = \mathbb{Q}(\sqrt{d})$ with $d > 0$ to serve as base field; also choose a prime (p) of $\mathbb{Z}$ that splits as $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in $\mathcal{O}_F$.

- Use characters on the ray class group $H_+(\mathfrak{m})$ for a suitable ideal $\mathfrak{m}$ to specify a totally complex abelian extension K of F in which $\mathfrak{p}$ splits completely; the Galois group $G = \mathrm{Gal}(K/F)$ is a specified subgroup of $H_+(\mathfrak{m})$.
- Compute the values $w_p\zeta_T(0;\sigma)$ and $\exp_p(-w_p\zeta'_{S,p}(0;\sigma))$ for all $\sigma \in G$; these are computed in $\mathbb{Q}_p$ using our $G_{p,2}$ function, to any desired accuracy.
- By Gross' formula, we now know all $\sigma(\alpha)$ as elements of $\mathbb{Q}_p$ to any desired accuracy; we then must realize the coefficients of the polynomial $f_\alpha(x) = \prod_{\sigma \in G}(x - \sigma(\alpha))$ as elements of F.
- Once we know the polynomial $f_\alpha \in F[x]$, then we know the field $K = F(\alpha)$ explicitly. At this point we verify computationally that $\alpha \in U_{\mathfrak{p}}$ and that $F(\alpha)$ is in fact the field K originally specified; that is, it has the correct Galois group and the correct discriminant.

The algorithm

First, explicitly choose a real quadratic field $F = \mathbb{Q}(\sqrt{d})$ with $d > 0$ to serve as base field; also choose a prime (p) of $\mathbb{Z}$ that splits as $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in $\mathcal{O}_F$.

- Use characters on the ray class group $H_+(\mathfrak{m})$ for a suitable ideal $\mathfrak{m}$ to specify a totally complex abelian extension K of F in which $\mathfrak{p}$ splits completely; the Galois group $G = \mathrm{Gal}(K/F)$ is a specified subgroup of $H_+(\mathfrak{m})$.
- Compute the values $w_p \zeta_T(0; \sigma)$ and $\exp_p(-w_p \zeta'_{S,p}(0; \sigma))$ for all $\sigma \in G$; these are computed in $\mathbb{Q}_p$ using our $G_{p,2}$ function, to any desired accuracy.
- By Gross' formula, we now know all $\sigma(\alpha)$ as elements of $\mathbb{Q}_p$ to any desired accuracy; we then must realize the coefficients of the polynomial $f_\alpha(x) = \prod_{\sigma \in G}(x - \sigma(\alpha))$ as elements of F.
- Once we know the polynomial $f_\alpha \in F[x]$, then we know the field $K = F(\alpha)$ explicitly. At this point we verify computationally that $\alpha \in U_\mathfrak{p}$ and that $F(\alpha)$ is in fact the field K originally specified; that is, it has the correct Galois group and the correct discriminant.
- And just like that, we have *explicitly* described an abelian extension K of F, which was originally described *algebraically*, using p-adic analysis. Yeah baby!

Computation of $\zeta'_{S,p}(0,\sigma)$

Using a continued fraction algorithm due to Hayes, each partial zeta function $\zeta_{S,p}(0,\sigma)$ can be decomposed into a finite sum of Shintani zeta functions

$$\zeta_S(0,\sigma) = \sum_{j=1}^{M} z_2(0,(\{z_j\},\langle w_j\rangle),(\beta_j^{(1)},\beta_j^{(2)})).$$

Computation of $\zeta'_{S,p}(0,\sigma)$

Using a continued fraction algorithm due to Hayes, each partial zeta function $\zeta_{S,p}(0,\sigma)$ can be decomposed into a finite sum of Shintani zeta functions

$$\zeta_S(0,\sigma) = \sum_{j=1}^{M} z_2(0,(\{z_j\},\langle w_j\rangle),(\beta_j^{(1)},\beta_j^{(2)})).$$

- Using a formula due to Shintani, its partial derivative at $s=0$ can be expressed as $\zeta'_S(0,\sigma)$

$$= \sum_{j=1}^{M} \log\Gamma_2(\{z_j\}+\langle w_j\rangle\beta_j^{(1)},(1,\beta_j^{(1)})) + \log\Gamma_2(\{z_j\}+\langle w_j\rangle\beta_j^{(2)},(1,\beta_j^{(2)}))$$

where $\Gamma_2(x;(\omega_1,\omega_2))$ is the complex double log gamma function.

Computation of $\zeta'_{S,p}(0,\sigma)$

Using a continued fraction algorithm due to Hayes, each partial zeta function $\zeta_{S,p}(0,\sigma)$ can be decomposed into a finite sum of Shintani zeta functions

$$\zeta_S(0,\sigma) = \sum_{j=1}^{M} z_2(0,(\{z_j\},\langle w_j\rangle),(\beta_j^{(1)},\beta_j^{(2)})).$$

- Using a formula due to Shintani, its partial derivative at $s=0$ can be expressed as $\zeta'_S(0,\sigma)$

$$= \sum_{j=1}^{M} \log\Gamma_2(\{z_j\}+\langle w_j\rangle\beta_j^{(1)},(1,\beta_j^{(1)})) + \log\Gamma_2(\{z_j\}+\langle w_j\rangle\beta_j^{(2)},(1,\beta_j^{(2)}))$$

  where $\Gamma_2(x;(\omega_1,\omega_2))$ is the complex double log gamma function.
- Using results of Kashio and T.-Y., the p-adic analogue $\zeta'_{S,p}(0,\sigma)$

$$= \sum_{j=1}^{M} G_{p,2}(\{z_j\}+\langle w_j\rangle(\beta_j)_{\mathfrak{p}},(1,(\beta_j)_{\mathfrak{p}})) + G_{p,2}(\{z_j\}+\langle w_j\rangle(\beta_j)_{\overline{\mathfrak{p}}},(1,(\beta_j)_{\overline{\mathfrak{p}}}))$$

  also holds, where $G_{p,2}(x;(\omega_1,\omega_2))$ is our p-adic double log gamma function.

The p-adic double log gamma function $G_{p,2}$

Initially defined on $\mathbb{C}_p \setminus \mathbb{Z}_p$ by a p-adic double integral, we actually compute these $G_{p,2}$ values by our "large x" expansion

$$\begin{aligned} G_{p,2}(x;\bar{\omega}) &= -\frac{1}{2} B_{2,2}(x;\bar{\omega}) \log_p x + \frac{3}{4\omega_1\omega_2} x^2 + B_{2,1}(0;\bar{\omega}) x \\ &\quad + \sum_{j=3}^{\infty} \frac{(-1)^j B_{2,j}(0;\bar{\omega})}{j(j-1)(j-2)} x^{2-j}, \end{aligned}$$

which converges for $|x|_p > \max\{|\omega_1|_p, |\omega_2|_p\}$. Here the $B_{2,j}(x;\bar{\omega})$ are second-order Bernoulli polynomials.

The p-adic double log gamma function $G_{p,2}$

Initially defined on $\mathbb{C}_p \setminus \mathbb{Z}_p$ by a p-adic double integral, we actually compute these $G_{p,2}$ values by our "large x" expansion

$$\begin{aligned} G_{p,2}(x;\bar{\omega}) &= -\frac{1}{2} B_{2,2}(x;\bar{\omega}) \log_p x + \frac{3}{4\omega_1\omega_2} x^2 + B_{2,1}(0;\bar{\omega}) x \\ &\quad + \sum_{j=3}^{\infty} \frac{(-1)^j B_{2,j}(0;\bar{\omega})}{j(j-1)(j-2)} x^{2-j}, \end{aligned}$$

which converges for $|x|_p > \max\{|\omega_1|_p, |\omega_2|_p\}$. Here the $B_{2,j}(x;\bar{\omega})$ are second-order Bernoulli polynomials.

- If this series is truncated after the $j = m$ term, the approximation obtained for $G_{p,2}(x,(\omega_1,\omega_2))$ is accurate to at least k p-adic digits, where

$$k \geq \begin{cases} m - 3 - \left\lceil \frac{\log(m+1)}{\log p} \right\rceil, & p > 2\,; \\ m - 4 - \left\lceil \frac{\log(m+1)}{\log p} \right\rceil, & p = 2\,. \end{cases}$$

Realizing the coefficients in $F = \mathbb{Q}(\sqrt{d})$

So we can compute the p-adic expansions of the coefficients λ_i of

$$f_\alpha(x) = \prod_{\sigma \in G} (x - \sigma(\alpha)) = x^n - \lambda_{n-1}x^{n-1} + \lambda_{n-2}x^{n-2} - \cdots + \lambda_0 \in F[x]$$

in $\mathbb{Q}_p$ to as many p-adic digits as we like. How do we realize them in $F = \mathbb{Q}(\sqrt{d})$?

Realizing the coefficients in $F = \mathbb{Q}(\sqrt{d})$

So we can compute the p-adic expansions of the coefficients λ_i of

$$f_\alpha(x) = \prod_{\sigma \in G} (x - \sigma(\alpha)) = x^n - \lambda_{n-1}x^{n-1} + \lambda_{n-2}x^{n-2} - \cdots + \lambda_0 \in F[x]$$

in $\mathbb{Q}_p$ to as many p-adic digits as we like. How do we realize them in $F = \mathbb{Q}(\sqrt{d})$?

- **Lemma.** If $\lambda_j = a_j + b_j\theta$ with $a_j, b_j \in \mathbb{Q}$, then a_j, b_j are both of the form cp^ν where $\nu \in \mathbb{Z}$ are given in terms of the integers $\{w_p\zeta_T(0,\sigma)\}_{\sigma \in G}$, and

$$|b_j| \le 2\binom{n}{j}/\sqrt{d}$$

and

$$|a_j| \le \begin{cases} \binom{n}{j}, & d \equiv 0 \bmod (4), \\ \binom{n}{j}(1 + 1/\sqrt{d}), & d \equiv 1 \bmod (4). \end{cases}$$

Realizing the coefficients in $F = \mathbb{Q}(\sqrt{d})$

So we can compute the p-adic expansions of the coefficients λ_i of

$$f_\alpha(x) = \prod_{\sigma \in G} (x - \sigma(\alpha)) = x^n - \lambda_{n-1}x^{n-1} + \lambda_{n-2}x^{n-2} - \cdots + \lambda_0 \in F[x]$$

in $\mathbb{Q}_p$ to as many p-adic digits as we like. How do we realize them in $F = \mathbb{Q}(\sqrt{d})$?

- **Lemma.** If $\lambda_j = a_j + b_j\theta$ with $a_j, b_j \in \mathbb{Q}$, then a_j, b_j are both of the form cp^ν where $\nu \in \mathbb{Z}$ are given in terms of the integers $\{w_p\zeta_T(0,\sigma)\}_{\sigma \in G}$, and

$$|b_j| \leq 2\binom{n}{j}/\sqrt{d}$$

  and

$$|a_j| \leq \begin{cases} \binom{n}{j}, & d \equiv 0 \bmod (4), \\ \binom{n}{j}(1 + 1/\sqrt{d}), & d \equiv 1 \bmod (4). \end{cases}$$

- Here $\{1, \theta\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_F$ satisfying $\theta_{\mathfrak{p}} - \theta_{\overline{\mathfrak{p}}} = \sqrt{d}$; that is,

$$\theta = \begin{cases} \sqrt{d}/2, & d \equiv 0 \bmod (4), \\ (1 + \sqrt{d})/2, & d \equiv 1 \bmod (4). \end{cases}$$

Realizing the coefficients, continued

The "trace" coefficient $\lambda_{n-1} = \sum_{\sigma \in G} \sigma(\alpha) \in F$ has $\mathfrak{p}$-adic absolute value $|\lambda_{n-1}|_{\mathfrak{p}} = p^r$, where $r = \max\{w_p \zeta_T(0, \sigma)\}_{\sigma \in G}$; but since $\alpha \in U_{\mathfrak{p}}$ it has $\overline{\mathfrak{p}}$-adic absolute value $|\lambda_{n-1}|_{\overline{\mathfrak{p}}} \leq 1$.

Realizing the coefficients, continued

The "trace" coefficient $\lambda_{n-1} = \sum_{\sigma \in G} \sigma(\alpha) \in F$ has $\mathfrak{p}$-adic absolute value $|\lambda_{n-1}|_{\mathfrak{p}} = p^r$, where $r = \max\{w_p \zeta_T(0, \sigma)\}_{\sigma \in G}$; but since $\alpha \in U_{\mathfrak{p}}$ it has $\overline{\mathfrak{p}}$-adic absolute value $|\lambda_{n-1}|_{\overline{\mathfrak{p}}} \leq 1$.

- If $\lambda_{n-1} = (c_{n-1} + e_{n-1}\theta)/p^r$ with $c_{n-1}, e_{n-1} \in \mathbb{Z}$, and we obtain an approximation $\beta \in \mathbb{Z}_p$ to $p^r(\lambda_{n-1})_{\mathfrak{p}}$ accurate to N digits, where $N \geq r$, then

$$
\begin{gathered}
|c_{n-1} + e_{n-1}\theta_{\mathfrak{p}} - \beta|_p \leq p^{-N} \quad \text{and} \quad |c_{n-1} + e_{n-1}\theta_{\overline{\mathfrak{p}}}|_p \leq p^{-r} \\
\Longrightarrow |c_{n-1} + e_{n-1}\theta_{\mathfrak{p}} - \beta - (c_{n-1} + e_{n-1}\theta_{\overline{\mathfrak{p}}})|_p \leq p^{-r} \\
\Longrightarrow |e_{n-1}(\theta_{\mathfrak{p}} - \theta_{\overline{\mathfrak{p}}}) - \beta|_p = |e_{n-1}\sqrt{d} - \beta|_p \leq p^{-r} \\
\Longrightarrow |e_{n-1} - \beta/\sqrt{d}|_p \leq p^{-r}
\end{gathered}
$$

so $\beta/\sqrt{d}$ gives the *integer* e_{n-1} accurate to at least r base p digits.

Realizing the coefficients, continued

The "trace" coefficient $\lambda_{n-1} = \sum_{\sigma \in G} \sigma(\alpha) \in F$ has $\mathfrak{p}$-adic absolute value $|\lambda_{n-1}|_{\mathfrak{p}} = p^r$, where $r = \max\{w_p \zeta_T(0, \sigma)\}_{\sigma \in G}$; but since $\alpha \in U_{\mathfrak{p}}$ it has $\overline{\mathfrak{p}}$-adic absolute value $|\lambda_{n-1}|_{\overline{\mathfrak{p}}} \leq 1$.

- If $\lambda_{n-1} = (c_{n-1} + e_{n-1}\theta)/p^r$ with $c_{n-1}, e_{n-1} \in \mathbb{Z}$, and we obtain an approximation $\beta \in \mathbb{Z}_p$ to $p^r(\lambda_{n-1})_{\mathfrak{p}}$ accurate to N digits, where $N \geq r$, then

$$|c_{n-1} + e_{n-1}\theta_{\mathfrak{p}} - \beta|_p \leq p^{-N} \quad \text{and} \quad |c_{n-1} + e_{n-1}\theta_{\overline{\mathfrak{p}}}|_p \leq p^{-r}$$
$$\implies |c_{n-1} + e_{n-1}\theta_{\mathfrak{p}} - \beta - (c_{n-1} + e_{n-1}\theta_{\overline{\mathfrak{p}}})|_p \leq p^{-r}$$
$$\implies |e_{n-1}(\theta_{\mathfrak{p}} - \theta_{\overline{\mathfrak{p}}}) - \beta|_p = |e_{n-1}\sqrt{d} - \beta|_p \leq p^{-r}$$
$$\implies |e_{n-1} - \beta/\sqrt{d}|_p \leq p^{-r}$$

  so $\beta/\sqrt{d}$ gives the *integer* e_{n-1} accurate to at least r base p digits.

- This specifies the integer e_{n-1} to one of at most $\lceil 4n/\sqrt{d} \rceil$ candidates; exactly one of these has $c_{n-1} = \beta - e_{n-1}\theta_{\mathfrak{p}}$ recognizable as an integer.

Realizing the coefficients, continued

The "trace" coefficient $\lambda_{n-1} = \sum_{\sigma \in G} \sigma(\alpha) \in F$ has $\mathfrak{p}$-adic absolute value $|\lambda_{n-1}|_{\mathfrak{p}} = p^r$, where $r = \max\{w_p \zeta_T(0, \sigma)\}_{\sigma \in G}$; but since $\alpha \in U_{\mathfrak{p}}$ it has $\overline{\mathfrak{p}}$-adic absolute value $|\lambda_{n-1}|_{\overline{\mathfrak{p}}} \leq 1$.

- If $\lambda_{n-1} = (c_{n-1} + e_{n-1}\theta)/p^r$ with $c_{n-1}, e_{n-1} \in \mathbb{Z}$, and we obtain an approximation $\beta \in \mathbb{Z}_p$ to $p^r(\lambda_{n-1})_{\mathfrak{p}}$ accurate to N digits, where $N \geq r$, then

$$\begin{gathered} |c_{n-1} + e_{n-1}\theta_{\mathfrak{p}} - \beta|_p \leq p^{-N} \quad \text{and} \quad |c_{n-1} + e_{n-1}\theta_{\overline{\mathfrak{p}}}|_p \leq p^{-r} \\ \implies |c_{n-1} + e_{n-1}\theta_{\mathfrak{p}} - \beta - (c_{n-1} + e_{n-1}\theta_{\overline{\mathfrak{p}}})|_p \leq p^{-r} \\ \implies |e_{n-1}(\theta_{\mathfrak{p}} - \theta_{\overline{\mathfrak{p}}}) - \beta|_p = |e_{n-1}\sqrt{d} - \beta|_p \leq p^{-r} \\ \implies |e_{n-1} - \beta/\sqrt{d}|_p \leq p^{-r} \end{gathered}$$

  so $\beta/\sqrt{d}$ gives the *integer* e_{n-1} accurate to at least r base p digits.

- This specifies the integer e_{n-1} to one of at most $\lceil 4n/\sqrt{d} \rceil$ candidates; exactly one of these has $c_{n-1} = \beta - e_{n-1}\theta_{\mathfrak{p}}$ recognizable as an integer.

- An analogous argument realizes the other coefficients $\lambda_i = (c_i + e_i\theta)/p^{r_i}$.

An example over the real quadratic field $F = \mathbb{Q}(\sqrt{29})$

The real quadratic field $F = \mathbb{Q}(\sqrt{29})$ is the splitting field over $\mathbb{Q}$ of the polynomial $f_{29}(x) = x^2 - x - 7$. The prime ideal (7) of $\mathbb{Z}$ splits as $(7) = \mathfrak{p}\overline{\mathfrak{p}} = (6 + \sqrt{29})(6 - \sqrt{29})$ in $\mathcal{O}_F$; there are two embeddings of F into $\mathbb{Q}_7$ corresponding to $\mathfrak{p}$ and $\overline{\mathfrak{p}}$; the two roots of f_{29} are $\theta_{\mathfrak{p}}, \theta_{\overline{\mathfrak{p}}} = (1 \pm \sqrt{29})/2$.

An example over the real quadratic field $F = \mathbb{Q}(\sqrt{29})$

The real quadratic field $F = \mathbb{Q}(\sqrt{29})$ is the splitting field over $\mathbb{Q}$ of the polynomial $f_{29}(x) = x^2 - x - 7$. The prime ideal (7) of $\mathbb{Z}$ splits as $(7) = \mathfrak{p}\overline{\mathfrak{p}} = (6 + \sqrt{29})(6 - \sqrt{29})$ in $\mathcal{O}_F$; there are two embeddings of F into $\mathbb{Q}_7$ corresponding to $\mathfrak{p}$ and $\overline{\mathfrak{p}}$; the two roots of f_{29} are $\theta_{\mathfrak{p}}, \theta_{\overline{\mathfrak{p}}} = (1 \pm \sqrt{29})/2$.

- We set $T = \{\mathfrak{p}_\infty^{(1)}, \mathfrak{p}_\infty^{(2)}, \mathfrak{q}, \overline{\mathfrak{p}}\}$ and $\mathfrak{m} = \mathfrak{q}\,\overline{\mathfrak{p}}$, where $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_F$ lying over (13). The narrow ray class group $H_+(\mathfrak{m})$ is isomorphic to $C_6 \times C_2$ and there is a sextic character χ on $H_+(\mathfrak{m})$ with conductor $\mathfrak{f}(\chi) = \mathfrak{m}\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}$; by class field theory there exists an abelian extension K/F corresponding to the subgroup of characters generated by χ with $G = \mathrm{Gal}(K/F)$ cyclic of order 6.

An example over the real quadratic field $F = \mathbb{Q}(\sqrt{29})$

The real quadratic field $F = \mathbb{Q}(\sqrt{29})$ is the splitting field over $\mathbb{Q}$ of the polynomial $f_{29}(x) = x^2 - x - 7$. The prime ideal (7) of $\mathbb{Z}$ splits as $(7) = \mathfrak{p}\overline{\mathfrak{p}} = (6+\sqrt{29})(6-\sqrt{29})$ in $\mathcal{O}_F$; there are two embeddings of F into $\mathbb{Q}_7$ corresponding to $\mathfrak{p}$ and $\overline{\mathfrak{p}}$; the two roots of f_{29} are $\theta_{\mathfrak{p}}, \theta_{\overline{\mathfrak{p}}} = (1 \pm \sqrt{29})/2$.

- We set $T = \{\mathfrak{p}_\infty^{(1)}, \mathfrak{p}_\infty^{(2)}, \mathfrak{q}, \overline{\mathfrak{p}}\}$ and $\mathfrak{m} = \mathfrak{q}\,\overline{\mathfrak{p}}$, where $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_F$ lying over (13). The narrow ray class group $H_+(\mathfrak{m})$ is isomorphic to $C_6 \times C_2$ and there is a sextic character χ on $H_+(\mathfrak{m})$ with conductor $\mathfrak{f}(\chi) = \mathfrak{m}\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}$; by class field theory there exists an abelian extension K/F corresponding to the subgroup of characters generated by χ with $G = \mathrm{Gal}(K/F)$ cyclic of order 6.
- By the form of the conductor $\mathfrak{f}(\chi)$ and the fact that $\chi(\mathfrak{p}) = 1$ we know that K is totally complex, both $\mathfrak{q}$ and $\overline{\mathfrak{p}}$ ramify in the extension K/F, no other primes of $\mathcal{O}_F$ ramify, and $\mathfrak{p}$ splits completely in K/F.

An example over the real quadratic field $F = \mathbb{Q}(\sqrt{29})$

The real quadratic field $F = \mathbb{Q}(\sqrt{29})$ is the splitting field over $\mathbb{Q}$ of the polynomial $f_{29}(x) = x^2 - x - 7$. The prime ideal (7) of $\mathbb{Z}$ splits as $(7) = \mathfrak{p}\overline{\mathfrak{p}} = (6 + \sqrt{29})(6 - \sqrt{29})$ in $\mathcal{O}_F$; there are two embeddings of F into $\mathbb{Q}_7$ corresponding to $\mathfrak{p}$ and $\overline{\mathfrak{p}}$; the two roots of f_{29} are $\theta_{\mathfrak{p}}, \theta_{\overline{\mathfrak{p}}} = (1 \pm \sqrt{29})/2$.

- We set $T = \{\mathfrak{p}_\infty^{(1)}, \mathfrak{p}_\infty^{(2)}, \mathfrak{q}, \overline{\mathfrak{p}}\}$ and $\mathfrak{m} = \mathfrak{q}\,\overline{\mathfrak{p}}$, where $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_F$ lying over (13). The narrow ray class group $H_+(\mathfrak{m})$ is isomorphic to $C_6 \times C_2$ and there is a sextic character χ on $H_+(\mathfrak{m})$ with conductor $\mathfrak{f}(\chi) = \mathfrak{m}\mathfrak{p}_\infty^{(1)}\mathfrak{p}_\infty^{(2)}$; by class field theory there exists an abelian extension K/F corresponding to the subgroup of characters generated by χ with $G = \mathrm{Gal}(K/F)$ cyclic of order 6.
- By the form of the conductor $\mathfrak{f}(\chi)$ and the fact that $\chi(\mathfrak{p}) = 1$ we know that K is totally complex, both $\mathfrak{q}$ and $\overline{\mathfrak{p}}$ ramify in the extension K/F, no other primes of $\mathcal{O}_F$ ramify, and $\mathfrak{p}$ splits completely in K/F.
- Our goal is to 7-adically compute the six conjugates $\{\sigma(\alpha)\}_{\sigma\in G}$ of the Gross-Stark unit $\alpha \in K$ for the extension K/F and the prime $p = 7$, and recognize the minimal polynomial $f_\alpha \in F[x]$, using only information from F.

Absolute values of the Gross-Stark unit

Choose an embedding of K into $\mathbb{Q}_7$ corresponding to some prime ideal $\mathfrak{P}$ in $\mathcal{O}_K$ lying above $\mathfrak{p}$ in $\mathcal{O}_F$.

Absolute values of the Gross-Stark unit

Choose an embedding of K into $\mathbb{Q}_7$ corresponding to some prime ideal $\mathfrak{P}$ in $\mathcal{O}_K$ lying above $\mathfrak{p}$ in $\mathcal{O}_F$.

- Using a partial fraction algorithm we compute the values $\zeta_T(0,\sigma_0) = 0$ for the identity σ_0, and $\zeta_T(0,\sigma) = -2$, $\zeta_T(0,\sigma^2) = \zeta_T(0,\sigma^3) = 0$, $\zeta_T(0,\sigma^4) = 2$, and $\zeta_T(0,\sigma^5) = 0$, where σ is the generator of G corresponding to χ.

Absolute values of the Gross-Stark unit

Choose an embedding of K into $\mathbb{Q}_7$ corresponding to some prime ideal $\mathfrak{P}$ in $\mathcal{O}_K$ lying above $\mathfrak{p}$ in $\mathcal{O}_F$.

- Using a partial fraction algorithm we compute the values $\zeta_T(0,\sigma_0) = 0$ for the identity σ_0, and $\zeta_T(0,\sigma) = -2$, $\zeta_T(0,\sigma^2) = \zeta_T(0,\sigma^3) = 0$, $\zeta_T(0,\sigma^4) = 2$, and $\zeta_T(0,\sigma^5) = 0$, where σ is the generator of G corresponding to χ.
- The p-adic absolute values of the $\sigma(\alpha)$ are of the form p^{-r} where $r = w_p\zeta_T(0,\sigma)$; since $w_7 = 6$ we have the 7-adic absolute values $\{7^{12}, 1, 1, 1, 1, 7^{-12}\}$ for $\alpha_{\mathfrak{P}}$ and its conjugates.

Absolute values of the Gross-Stark unit

Choose an embedding of K into $\mathbb{Q}_7$ corresponding to some prime ideal $\mathfrak{P}$ in $\mathcal{O}_K$ lying above $\mathfrak{p}$ in $\mathcal{O}_F$.

- Using a partial fraction algorithm we compute the values $\zeta_T(0, \sigma_0) = 0$ for the identity σ_0, and $\zeta_T(0, \sigma) = -2$, $\zeta_T(0, \sigma^2) = \zeta_T(0, \sigma^3) = 0$, $\zeta_T(0, \sigma^4) = 2$, and $\zeta_T(0, \sigma^5) = 0$, where σ is the generator of G corresponding to χ.
- The p-adic absolute values of the $\sigma(\alpha)$ are of the form p^{-r} where $r = w_p \zeta_T(0, \sigma)$; since $w_7 = 6$ we have the 7-adic absolute values $\{7^{12}, 1, 1, 1, 1, 7^{-12}\}$ for $\alpha_{\mathfrak{P}}$ and its conjugates.
- Recall that, since $\alpha \in U_{\mathfrak{p}}$, the absolute value of α with respect to every other absolute value on K is 1.

Absolute values of the Gross-Stark unit

Choose an embedding of K into $\mathbb{Q}_7$ corresponding to some prime ideal $\mathfrak{P}$ in $\mathcal{O}_K$ lying above $\mathfrak{p}$ in $\mathcal{O}_F$.

- Using a partial fraction algorithm we compute the values $\zeta_T(0, \sigma_0) = 0$ for the identity σ_0, and $\zeta_T(0, \sigma) = -2$, $\zeta_T(0, \sigma^2) = \zeta_T(0, \sigma^3) = 0$, $\zeta_T(0, \sigma^4) = 2$, and $\zeta_T(0, \sigma^5) = 0$, where σ is the generator of G corresponding to χ.
- The p-adic absolute values of the $\sigma(\alpha)$ are of the form p^{-r} where $r = w_p \zeta_T(0, \sigma)$; since $w_7 = 6$ we have the 7-adic absolute values $\{7^{12}, 1, 1, 1, 1, 7^{-12}\}$ for $\alpha_{\mathfrak{P}}$ and its conjugates.
- Recall that, since $\alpha \in U_{\mathfrak{p}}$, the absolute value of α with respect to every other absolute value on K is 1.
- The minimal polynomial of α over F is of the form

$$f_\alpha(x) = x^6 - \lambda_5 x^5 + \lambda_4 x^4 - \lambda_3 x^3 + \lambda_2 x^2 - \lambda_1 x + 1 \in F[x]$$

  where each $\lambda_i = (c_i + e_i \theta)/7^{12}$ for some $c_i, e_i \in \mathbb{Z}$, and $\theta = (1 + \sqrt{29})/2$.

Absolute values of the Gross-Stark unit

Choose an embedding of K into $\mathbb{Q}_7$ corresponding to some prime ideal $\mathfrak{P}$ in $\mathcal{O}_K$ lying above $\mathfrak{p}$ in $\mathcal{O}_F$.

- Using a partial fraction algorithm we compute the values $\zeta_T(0, \sigma_0) = 0$ for the identity σ_0, and $\zeta_T(0, \sigma) = -2$, $\zeta_T(0, \sigma^2) = \zeta_T(0, \sigma^3) = 0$, $\zeta_T(0, \sigma^4) = 2$, and $\zeta_T(0, \sigma^5) = 0$, where σ is the generator of G corresponding to χ.
- The p-adic absolute values of the $\sigma(\alpha)$ are of the form p^{-r} where $r = w_p \zeta_T(0, \sigma)$; since $w_7 = 6$ we have the 7-adic absolute values $\{7^{12}, 1, 1, 1, 1, 7^{-12}\}$ for $\alpha_{\mathfrak{P}}$ and its conjugates.
- Recall that, since $\alpha \in U_{\mathfrak{p}}$, the absolute value of α with respect to every other absolute value on K is 1.
- The minimal polynomial of α over F is of the form

$$f_\alpha(x) = x^6 - \lambda_5 x^5 + \lambda_4 x^4 - \lambda_3 x^3 + \lambda_2 x^2 - \lambda_1 x + 1 \in F[x]$$

  where each $\lambda_i = (c_i + e_i\theta)/7^{12}$ for some $c_i, e_i \in \mathbb{Z}$, and $\theta = (1 + \sqrt{29})/2$.
- We can recognize all the c_i, e_i by computing all the $\sigma(\alpha)_{\mathfrak{P}}$ accurate to just a few more than twelve 7-adic digits.

Computation of the values $\zeta'_{S,7}(0;\sigma)$

Gross' formula states that $(\sigma(\alpha))_{\mathfrak{P}} = p^{w_p \zeta_T(0;\sigma)} \exp_p(-w_p \zeta'_{S,p}(0;\sigma))$ for all $\sigma \in G$.

We will compute the six values $(\sigma(\alpha))_{\mathfrak{P}} = 7^{6\zeta_T(0;\sigma)} \exp_7(-6\zeta'_{S,7}(0;\sigma))$ in $\mathbb{Q}_7$.

Computation of the values $\zeta'_{S,7}(0;\sigma)$

Gross' formula states that $(\sigma(\alpha))_{\mathfrak{P}} = p^{w_p \zeta_T(0;\sigma)} \exp_p(-w_p \zeta'_{S,p}(0;\sigma))$ for all $\sigma \in G$.

We will compute the six values $(\sigma(\alpha))_{\mathfrak{P}} = 7^{6\zeta_T(0;\sigma)} \exp_7(-6\zeta'_{S,7}(0;\sigma))$ in $\mathbb{Q}_7$.

- It is not obvious that $-6\zeta'_{S,7}(0;\sigma)$ lies in the domain $7\mathbb{Z}_7$ of $\exp_7$.

  Especially since we compute these values as sums of 7-adically large values.

Computation of the values $\zeta'_{S,7}(0;\sigma)$

Gross' formula states that $(\sigma(\alpha))_{\mathfrak{P}} = p^{w_p \zeta_T(0;\sigma)} \exp_p(-w_p \zeta'_{S,p}(0;\sigma))$ for all $\sigma \in G$.

We will compute the six values $(\sigma(\alpha))_{\mathfrak{P}} = 7^{6\zeta_T(0;\sigma)} \exp_7(-6\zeta'_{S,7}(0;\sigma))$ in $\mathbb{Q}_7$.

- It is not obvious that $-6\zeta'_{S,7}(0;\sigma)$ lies in the domain $7\mathbb{Z}_7$ of $\exp_7$.

  Especially since we compute these values as sums of 7-adically large values.

- It is remarkable that the values $\exp_7(-6\zeta'_{S,7}(0;\sigma))$ should be algebraic.

Computation of the values $\zeta'_{S,7}(0;\sigma)$

Gross' formula states that $(\sigma(\alpha))_{\mathfrak{P}} = p^{w_p \zeta_T(0;\sigma)} \exp_p(-w_p \zeta'_{S,p}(0;\sigma))$ for all $\sigma \in G$.

We will compute the six values $(\sigma(\alpha))_{\mathfrak{P}} = 7^{6\zeta_T(0;\sigma)} \exp_7(-6\zeta'_{S,7}(0;\sigma))$ in $\mathbb{Q}_7$.

- It is not obvious that $-6\zeta'_{S,7}(0;\sigma)$ lies in the domain $7\mathbb{Z}_7$ of $\exp_7$.

  Especially since we compute these values as sums of 7-adically large values.

- It is remarkable that the values $\exp_7(-6\zeta'_{S,7}(0;\sigma))$ should be algebraic.

- We compute these values in $\mathbb{Q}_7$. But Gross' assertion that $\alpha \in U_{\mathfrak{p}}$ tells us the absolute values of the $\sigma(\alpha)$ with respect to every other embedding of K into $\mathbb{C}$ or a p-adic field.

Computation of the values $\zeta'_{S,7}(0;\sigma)$

Gross' formula states that $(\sigma(\alpha))_{\mathfrak{P}} = p^{w_p \zeta_T(0;\sigma)} \exp_p(-w_p \zeta'_{S,p}(0;\sigma))$ for all $\sigma \in G$.

We will compute the six values $(\sigma(\alpha))_{\mathfrak{P}} = 7^{6\zeta_T(0;\sigma)} \exp_7(-6\zeta'_{S,7}(0;\sigma))$ in $\mathbb{Q}_7$.

- It is not obvious that $-6\zeta'_{S,7}(0;\sigma)$ lies in the domain $7\mathbb{Z}_7$ of $\exp_7$.

  Especially since we compute these values as sums of 7-adically large values.

- It is remarkable that the values $\exp_7(-6\zeta'_{S,7}(0;\sigma))$ should be algebraic.

- We compute these values in $\mathbb{Q}_7$. But Gross' assertion that $\alpha \in U_{\mathfrak{p}}$ tells us the absolute values of the $\sigma(\alpha)$ with respect to every other embedding of K into $\mathbb{C}$ or a p-adic field.

- So not only are these values computable in $\mathbb{Q}_7$, and algebraic, but they are *recognizable* as specific algebraic numbers.

Computation of the values $\zeta'_{S,7}(0;\sigma)$

Gross' formula states that $(\sigma(\alpha))_{\mathfrak{P}} = p^{w_p \zeta_T(0;\sigma)} \exp_p(-w_p \zeta'_{S,p}(0;\sigma))$ for all $\sigma \in G$.

We will compute the six values $(\sigma(\alpha))_{\mathfrak{P}} = 7^{6\zeta_T(0;\sigma)} \exp_7(-6\zeta'_{S,7}(0;\sigma))$ in $\mathbb{Q}_7$.

- It is not obvious that $-6\zeta'_{S,7}(0;\sigma)$ lies in the domain $7\mathbb{Z}_7$ of $\exp_7$.

  Especially since we compute these values as sums of 7-adically large values.
- It is remarkable that the values $\exp_7(-6\zeta'_{S,7}(0;\sigma))$ should be algebraic.
- We compute these values in $\mathbb{Q}_7$. But Gross' assertion that $\alpha \in U_{\mathfrak{p}}$ tells us the absolute values of the $\sigma(\alpha)$ with respect to every other embedding of K into $\mathbb{C}$ or a p-adic field.
- So not only are these values computable in $\mathbb{Q}_7$, and algebraic, but they are *recognizable* as specific algebraic numbers.
- Not only that, but they are *special* algebraic numbers - they generate a specific *abelian* extension of $F = \mathbb{Q}(\sqrt{29})$.

Computation of the values $\zeta'_{S,7}(0;\sigma)$

Each $\zeta'_{S,7}(0;\sigma)$ is a finite sum of $\zeta'_{\mathfrak{mp},7}(0;\mathcal{C}_+)$ values over all ideal classes $\mathcal{C}_+$ in a coset of a subgroup of the narrow ray class group $H_+(\mathfrak{mp})$.

Computation of the values $\zeta'_{S,7}(0;\sigma)$

Each $\zeta'_{S,7}(0;\sigma)$ is a finite sum of $\zeta'_{\mathfrak{mp},7}(0;\mathcal{C}_+)$ values over all ideal classes $\mathcal{C}_+$ in a coset of a subgroup of the narrow ray class group $H_+(\mathfrak{mp})$.

- The partial fraction algorithm produces an ordered sequence of $\mathbb{Z}$-bases for an ideal $\mathfrak{mc}$ of $\mathcal{O}_F$ in the class $\mathcal{C}_+$.

Computation of the values $\zeta'_{S,7}(0;\sigma)$

Each $\zeta'_{S,7}(0;\sigma)$ is a finite sum of $\zeta'_{\mathfrak{mp},7}(0;\mathcal{C}_+)$ values over all ideal classes $\mathcal{C}_+$ in a coset of a subgroup of the narrow ray class group $H_+(\mathfrak{mp})$.

- The partial fraction algorithm produces an ordered sequence of $\mathbb{Z}$-bases for an ideal $\mathfrak{mc}$ of $\mathcal{O}_F$ in the class $\mathcal{C}_+$.
- This decomposes each term $\zeta'_{\mathfrak{mp},7}(0;\mathcal{C}_+)$ into a finite sum of derivatives of Shintani zeta functions, which we compute as a finite sum of values $G_{7,2}(x_i;\bar{\omega}_i)$, where the x_i and $\bar{\omega}_i$ are given in terms of the parameters of the bases, and all satisfy $|x_i|_7 > ||\bar{\omega}_i||_7$.

Computation of the values $\zeta'_{S,7}(0;\sigma)$

Each $\zeta'_{S,7}(0;\sigma)$ is a finite sum of $\zeta'_{\mathfrak{mp},7}(0;\mathcal{C}_+)$ values over all ideal classes $\mathcal{C}_+$ in a coset of a subgroup of the narrow ray class group $H_+(\mathfrak{mp})$.

- The partial fraction algorithm produces an ordered sequence of $\mathbb{Z}$-bases for an ideal $\mathfrak{mc}$ of $\mathcal{O}_F$ in the class $\mathcal{C}_+$.
- This decomposes each term $\zeta'_{\mathfrak{mp},7}(0;\mathcal{C}_+)$ into a finite sum of derivatives of Shintani zeta functions, which we compute as a finite sum of values $G_{7,2}(x_i;\bar{\omega}_i)$, where the x_i and $\bar{\omega}_i$ are given in terms of the parameters of the bases, and all satisfy $|x_i|_7 > ||\bar{\omega}_i||_7$.
- This means we can compute each of these terms in $\mathbb{Q}_7$ using our "large x" expansion

$$\begin{aligned} G_{7,2}(x;\bar{\omega}) &= -\frac{1}{2}B_{2,2}(x;\bar{\omega})\log_7 x + \frac{3}{4\omega_1\omega_2}x^2 + B_{2,1}(0;\bar{\omega})x \\ &+ \sum_{j=3}^{\infty}\frac{(-1)^j B_{2,j}(0;\bar{\omega})}{j(j-1)(j-2)}x^{2-j}. \end{aligned}$$

Computation of the values $\zeta'_{S,7}(0;\sigma)$

Each $\zeta'_{S,7}(0;\sigma)$ is a finite sum of $\zeta'_{\mathfrak{mp},7}(0;\mathcal{C}_+)$ values over all ideal classes $\mathcal{C}_+$ in a coset of a subgroup of the narrow ray class group $H_+(\mathfrak{mp})$.

- The partial fraction algorithm produces an ordered sequence of $\mathbb{Z}$-bases for an ideal $\mathfrak{mc}$ of $\mathcal{O}_F$ in the class $\mathcal{C}_+$.
- This decomposes each term $\zeta'_{\mathfrak{mp},7}(0;\mathcal{C}_+)$ into a finite sum of derivatives of Shintani zeta functions, which we compute as a finite sum of values $G_{7,2}(x_i;\bar{\omega}_i)$, where the x_i and $\bar{\omega}_i$ are given in terms of the parameters of the bases, and all satisfy $|x_i|_7 > ||\bar{\omega}_i||_7$.
- This means we can compute each of these terms in $\mathbb{Q}_7$ using our "large x" expansion

$$\begin{aligned} G_{7,2}(x;\bar{\omega}) &= -\frac{1}{2}B_{2,2}(x;\bar{\omega})\log_7 x + \frac{3}{4\omega_1\omega_2}x^2 + B_{2,1}(0;\bar{\omega})x \\ &\quad + \sum_{j=3}^{\infty}\frac{(-1)^j B_{2,j}(0;\bar{\omega})}{j(j-1)(j-2)}x^{2-j}. \end{aligned}$$

- We have programmed all of this in PARI routines.

Realizing the trace coefficient λ_5

By this method we compute the 7-adic approximation

$$\begin{aligned}\beta &= 7^{12} \cdot \sum_{\sigma \in G} 7^{\,6\zeta_T(0,\sigma)} \cdot \exp_7(-6\zeta'_{S,7}(0,\sigma)) \\ &= 1 + 3\cdot 7 + 3\cdot 7^2 + 7^3 + 4\cdot 7^4 + 7^5 + 3\cdot 7^7 + 3\cdot 7^8 \\ &+ 6\cdot 7^9 + 6\cdot 7^{10} + 0\cdot 7^{11} + O(7^{12}) = (133141033660...)_7\end{aligned}$$

to $7^{12}\lambda_5 = c_5 + e_5\theta_{\mathfrak{p}}$, which in turn yields the approximation $\beta/\sqrt{29} = (113016104651...)_7$ to the integer e_5.

Realizing the trace coefficient λ_5

By this method we compute the 7-adic approximation

$$\begin{aligned}\beta &= 7^{12} \cdot \sum_{\sigma \in G} 7^{\,6\zeta_T(0,\sigma)} \cdot \exp_7(-6\zeta'_{S,7}(0,\sigma)) \\ &= 1 + 3 \cdot 7 + 3 \cdot 7^2 + 7^3 + 4 \cdot 7^4 + 7^5 + 3 \cdot 7^7 + 3 \cdot 7^8 \\ &+ 6 \cdot 7^9 + 6 \cdot 7^{10} + 0 \cdot 7^{11} + O(7^{12}) = (133141033660\ldots)_7\end{aligned}$$

to $7^{12}\lambda_5 = c_5 + e_5\theta_{\mathfrak{p}}$, which in turn yields the approximation $\beta/\sqrt{29} = (113016104651\ldots)_7$ to the integer e_5.

- We truncate this 7-adic expansion mod 7^{12} as indicated, giving the integer $e = 3655104881$; considering the bound $2\binom{6}{5}/\sqrt{29} = 2.2283\ldots$, we know that e_5 must be exactly one of $\{e - 2 \cdot 7^{12}, e - 7^{12}, e, e + 7^{12}\}$.

Realizing the trace coefficient λ_5

By this method we compute the 7-adic approximation

$$\begin{aligned}\beta &= 7^{12} \cdot \sum_{\sigma \in G} 7^{\,6\zeta_T(0,\sigma)} \cdot \exp_7(-6\zeta'_{S,7}(0,\sigma)) \\ &= 1 + 3\cdot 7 + 3 \cdot 7^2 + 7^3 + 4 \cdot 7^4 + 7^5 + 3 \cdot 7^7 + 3 \cdot 7^8 \\ &+\ 6 \cdot 7^9 + 6 \cdot 7^{10} + 0 \cdot 7^{11} + O(7^{12}) = (133141033660\ldots)_7\end{aligned}$$

to $7^{12}\lambda_5 = c_5 + e_5\theta_{\mathfrak{p}}$, which in turn yields the approximation $\beta/\sqrt{29} = (113016104651\ldots)_7$ to the integer e_5.

- We truncate this 7-adic expansion mod 7^{12} as indicated, giving the integer $e = 3655104881$; considering the bound $2\binom{6}{5}/\sqrt{29} = 2.2283\ldots$, we know that e_5 must be exactly one of $\{e - 2 \cdot 7^{12}, e - 7^{12}, e, e + 7^{12}\}$.
- Exactly one of these choices for e_5 should be such that $\beta - e_5\theta_{\mathfrak{p}}$ is recognizable as an integer c_5 satisfying the bound $|c_5| \leq \binom{6}{5}(1 + 1/\sqrt{29}) \cdot 7^{12}$.

Realizing the trace coefficient λ_5

By this method we compute the 7-adic approximation

$$
\begin{aligned}
\beta &= 7^{12} \cdot \sum_{\sigma \in G} 7^{\,6\zeta_T(0,\sigma)} \cdot \exp_7(-6\zeta'_{S,7}(0,\sigma)) \\
&= 1 + 3 \cdot 7 + 3 \cdot 7^2 + 7^3 + 4 \cdot 7^4 + 7^5 + 3 \cdot 7^7 + 3 \cdot 7^8 \\
&+ 6 \cdot 7^9 + 6 \cdot 7^{10} + 0 \cdot 7^{11} + O(7^{12}) = (133141033660\ldots)_7
\end{aligned}
$$

to $7^{12}\lambda_5 = c_5 + e_5\theta_{\mathfrak{p}}$, which in turn yields the approximation $\beta/\sqrt{29} = (113016104651\ldots)_7$ to the integer e_5.

- We truncate this 7-adic expansion mod 7^{12} as indicated, giving the integer $e = 3655104881$; considering the bound $2\binom{6}{5}/\sqrt{29} = 2.2283\ldots$, we know that e_5 must be exactly one of $\{e - 2 \cdot 7^{12}, e - 7^{12}, e, e + 7^{12}\}$.
- Exactly one of these choices for e_5 should be such that $\beta - e_5\theta_{\mathfrak{p}}$ is recognizable as an integer c_5 satisfying the bound $|c_5| \leq \binom{6}{5}(1 + 1/\sqrt{29}) \cdot 7^{12}$.
- Beyond the 7^{12}s digit, such an integer must have 7-adic digits either all zeros or all sixes.

Realizing the trace coefficient λ_5

By this method we compute the 7-adic approximation

$$\begin{aligned}\beta &= 7^{12}\cdot\sum_{\sigma\in G} 7^{\,6\zeta_T(0,\sigma)}\cdot \exp_7(-6\zeta'_{S,7}(0,\sigma))\\ &= 1+3\cdot 7+3\cdot 7^2+7^3+4\cdot 7^4+7^5+3\cdot 7^7+3\cdot 7^8\\ &+\ 6\cdot 7^9+6\cdot 7^{10}+0\cdot 7^{11}+O(7^{12})=(133141033660\ldots)_7\end{aligned}$$

to $7^{12}\lambda_5 = c_5 + e_5\theta_{\mathfrak{p}}$, which in turn yields the approximation $\beta/\sqrt{29} = (113016104651\ldots)_7$ to the integer e_5.

- We truncate this 7-adic expansion mod 7^{12} as indicated, giving the integer $e = 3655104881$; considering the bound $2\binom{6}{5}/\sqrt{29} = 2.2283\ldots$, we know that e_5 must be exactly one of $\{e-2\cdot 7^{12}, e-7^{12}, e, e+7^{12}\}$.
- Exactly one of these choices for e_5 should be such that $\beta - e_5\theta_{\mathfrak{p}}$ is recognizable as an integer c_5 satisfying the bound $|c_5| \le \binom{6}{5}(1+1/\sqrt{29})\cdot 7^{12}$.
- Beyond the 7^{12}s digit, such an integer must have 7-adic digits either all zeros or all sixes.
- We find that $e_5 = e - 7^{12} = -10186182320$ and $c_5 = -849169895$.

The Gross-Stark unit α given explicitly

The same method determines the other coefficients λ_i, which are also symmetric functions of the $\sigma(\alpha)$. The minimal polynomial satisfied by the Gross-Stark unit α over F is

$$y^6 + \frac{849169895 + 101861823320\theta}{7^{12}} y^5 + \frac{46850752816 + 9893163304\theta}{7^{12}} y^4$$
$$+ \frac{1168907600 + 183029652480\theta}{7^{12}} y^3 + \frac{46850752816 + 9893163304\theta}{7^{12}} y^2$$
$$+ \frac{849169895 + 101861823320\theta}{7^{12}} y + 1$$

where $\theta = (1+\sqrt{29})/2$ is a root of the polynomial $x^2 - x - 7$ such that $\{1, \theta\}$ is a basis for $\mathcal{O}_F$ over $\mathbb{Z}$. We verified this numerically to sixty-seven 7-adic digits.

The Gross-Stark unit α given explicitly

The same method determines the other coefficients λ_i, which are also symmetric functions of the $\sigma(\alpha)$. The minimal polynomial satisfied by the Gross-Stark unit α over F is

$$y^6 + \frac{849169895 + 101861823320\theta}{7^{12}} y^5 + \frac{46850752816 + 989316304\theta}{7^{12}} y^4 + \frac{1168907600 + 183029652448\theta}{7^{12}} y^3 + \frac{46850752816 + 9893163304\theta}{7^{12}} y^2 + \frac{849169895 + 101861823320\theta}{7^{12}} y + 1$$

where $\theta = (1+\sqrt{29})/2$ is a root of the polynomial $x^2 - x - 7$ such that $\{1, \theta\}$ is a basis for $\mathcal{O}_F$ over $\mathbb{Z}$. We verified this numerically to sixty-seven 7-adic digits.

- We verify computationally that α is indeed a square in K and that $K = F(\alpha)$ is in fact the totally complex extension originally specified.

The Gross-Stark unit α given explicitly

The same method determines the other coefficients λ_i, which are also symmetric functions of the $\sigma(\alpha)$. The minimal polynomial satisfied by the Gross-Stark unit α over F is

$$y^6 + \frac{849169895 + 101861823320\theta}{7^{12}} y^5 + \frac{46850752816 + 9893163304\theta}{7^{12}} y^4 + \frac{1168907600 + 183029652480\theta}{7^{12}} y^3 + \frac{46850752816 + 9893163304\theta}{7^{12}} y^2 + \frac{849169895 + 101861823320\theta}{7^{12}} y + 1$$

where $\theta = (1 + \sqrt{29})/2$ is a root of the polynomial $x^2 - x - 7$ such that $\{1, \theta\}$ is a basis for $\mathcal{O}_F$ over $\mathbb{Z}$. We verified this numerically to sixty-seven 7-adic digits.

- We verify computationally that α is indeed a square in K and that $K = F(\alpha)$ is in fact the totally complex extension originally specified.
- In the spirit of Hilbert's Twelfth Problem, we have given a 7-adic analytic construction of a specific totally complex abelian extension K of of F, using only information from F.

Problems for the next century

So we can calculate the Gross-Stark units α attached to relative abelian totally complex extensions of real quadratic fields; now what?

Problems for the next century

So we can calculate the Gross-Stark units α attached to relative abelian totally complex extensions of real quadratic fields; now what?

- Improve the implementation in PARI; find more efficient ways to choose the prime $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, for example.

Problems for the next century

So we can calculate the Gross-Stark units α attached to relative abelian totally complex extensions of real quadratic fields; now what?

- Improve the implementation in PARI; find more efficient ways to choose the prime $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, for example.
- We found some new relations in the course of this work; for example, for each class $\mathcal{C}_+ \in H_+(\mathfrak{m}\mathfrak{p})$ we have $\zeta'_{\mathfrak{m}\mathfrak{p},p}(0, [\nu]_+\mathcal{C}_+) = \zeta'_{\mathfrak{m}\mathfrak{p},p}(0, \mathcal{C}_+)$, where $\nu := \mathrm{N}(\mathfrak{m}\mathfrak{p}) - 1$ and $[\nu]_+$ denotes the narrow class modulo $\mathfrak{m}\mathfrak{p}$ to which the principal ideal (ν) belongs; are there others? Can we exploit them?

Problems for the next century

So we can calculate the Gross-Stark units α attached to relative abelian totally complex extensions of real quadratic fields; now what?

- Improve the implementation in PARI; find more efficient ways to choose the prime $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, for example.
- We found some new relations in the course of this work; for example, for each class $\mathcal{C}_+ \in H_+(\mathfrak{m}\mathfrak{p})$ we have $\zeta'_{\mathfrak{m}\mathfrak{p},p}(0, [\nu]_+\mathcal{C}_+) = \zeta'_{\mathfrak{m}\mathfrak{p},p}(0, \mathcal{C}_+)$, where $\nu := \mathrm{N}(\mathfrak{m}\mathfrak{p}) - 1$ and $[\nu]_+$ denotes the narrow class modulo $\mathfrak{m}\mathfrak{p}$ to which the principal ideal (ν) belongs; are there others? Can we exploit them?
- Can we use our explicit analytic construction of the Gross-Stark units to suggest an *algebraic* description of them? For example, in the case where the base field is $F = \mathbb{Q}$ the Gross-Stark units are roots of unity or sums thereof.

Problems for the next century

So we can calculate the Gross-Stark units α attached to relative abelian totally complex extensions of real quadratic fields; now what?

- Improve the implementation in PARI; find more efficient ways to choose the prime $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, for example.
- We found some new relations in the course of this work; for example, for each class $\mathcal{C}_+ \in H_+(\mathfrak{m}\mathfrak{p})$ we have $\zeta'_{\mathfrak{m}\mathfrak{p},p}(0, [\nu]_+\mathcal{C}_+) = \zeta'_{\mathfrak{m}\mathfrak{p},p}(0, \mathcal{C}_+)$, where $\nu := \mathrm{N}(\mathfrak{m}\mathfrak{p}) - 1$ and $[\nu]_+$ denotes the narrow class modulo $\mathfrak{m}\mathfrak{p}$ to which the principal ideal (ν) belongs; are there others? Can we exploit them?
- Can we use our explicit analytic construction of the Gross-Stark units to suggest an *algebraic* description of them? For example, in the case where the base field is $F = \mathbb{Q}$ the Gross-Stark units are roots of unity or sums thereof.
- Can a more constructive independent proof of Darmon-Dasgupta-Pollack theorem be given?

Problems for the next century

So we can calculate the Gross-Stark units α attached to relative abelian totally complex extensions of real quadratic fields; now what?

- Improve the implementation in PARI; find more efficient ways to choose the prime $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, for example.
- We found some new relations in the course of this work; for example, for each class $\mathcal{C}_+ \in H_+(\mathfrak{m}\mathfrak{p})$ we have $\zeta'_{\mathfrak{m}\mathfrak{p},p}(0, [\nu]_+\mathcal{C}_+) = \zeta'_{\mathfrak{m}\mathfrak{p},p}(0, \mathcal{C}_+)$, where $\nu := \mathrm{N}(\mathfrak{m}\mathfrak{p}) - 1$ and $[\nu]_+$ denotes the narrow class modulo $\mathfrak{m}\mathfrak{p}$ to which the principal ideal (ν) belongs; are there others? Can we exploit them?
- Can we use our explicit analytic construction of the Gross-Stark units to suggest an *algebraic* description of them? For example, in the case where the base field is $F = \mathbb{Q}$ the Gross-Stark units are roots of unity or sums thereof.
- Can a more constructive independent proof of Darmon-Dasgupta-Pollack theorem be given?
- Extend the algorithm to higher-degree totally real base fields F, using higher p-adic multiple log gamma functions we have developed. (note: the Gross-Stark conjecture is only known *conditionally* in the general case)

Thanks!

Thanks!

- Thanks for the opportunity to speak!

Thanks!

- Thanks for the opportunity to speak!
- Preprints may be found at

$$\texttt{http} : //\texttt{youngp.people.cofc.edu}/$$

Thanks!

- Thanks for the opportunity to speak!
- Preprints may be found at

$$\texttt{http://youngp.people.cofc.edu/}$$

- Video abstract "On p-adic multiple zeta and log gamma functions" may be found at

$$\texttt{http://www.youtube.com/watch?v=I9Bv\_CycEd8}$$

or

$$\texttt{http://www.youtube.com/user/JournalNumberTheory}$$

Thanks!

- Thanks for the opportunity to speak!
- Preprints may be found at

$$\texttt{http : //youngp.people.cofc.edu/}$$

- Video abstract "On p-adic multiple zeta and log gamma functions" may be found at

$$\texttt{http : //www.youtube.com/watch?v = I9Bv\_CycEd8}$$

  or

$$\texttt{http : //www.youtube.com/user/JournalNumberTheory}$$

- Video abstract "Explicit computation of Gross-Stark units over real quadratic fields" may be found at

$$\texttt{http : //www.youtube.com/watch?v = 8h1 - GW - sTNc}$$