Fekete polynomials, quadratic residues, and arithmetic

Jan Minac, Nguyen D. Tan, **Tung T. Nguyen**

GTA Philly 2021

Western University

Introduction and motivations

Let us start our story with the beautiful Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Let us start our story with the beautiful Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

In 1734, Leonhard Euler found the following remarkable formula

$$\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \ldots = \frac{\pi^2}{6}.$$

Introduction and motivations

Let us start our story with the beautiful Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

In 1734, Leonhard Euler found the following remarkable formula

$$\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \ldots = \frac{\pi^2}{6}.$$

Indeed, Euler did much more. In particular, he showed that

$$\zeta(2k) = (-1)^{k+1} \frac{(2\pi)^{2k}}{2(2k)!} B_{2k},$$

where $\{B_n\}$ are the Bernoulli numbers defined by following Taylor's expansion

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} z^n.$$

Introduction and motivations

- $\diamond$ The values $\zeta(n)$ are called special values of the Riemann zeta function. They play a fundamental role in number theory.

Introduction and motivations

- ◇ The values $\zeta(n)$ are called special values of the Riemann zeta function. They play a fundamental role in number theory.
- ◇ There is a quite general notion of L-function of a motive.

Introduction and motivations

- The values $\zeta(n)$ are called special values of the Riemann zeta function. They play a fundamental role in number theory.
- There is a quite general notion of L-function of a motive.
- The Bloch-Kato conjecture provides a precise connection between the world of zeta functions, the world of arithmetic, and the world of automorphic forms.

Introduction and motivations

- The values $\zeta(n)$ are called special values of the Riemann zeta function. They play a fundamental role in number theory.
- There is a quite general notion of L-function of a motive.
- The Bloch-Kato conjecture provides a precise connection between the world of zeta functions, the world of arithmetic, and the world of automorphic forms.
- Today, we focus on remarkable polynomials associated with 1-dimensional motives, namely a Dirichlet character.

Let p be a prime number. For simplicity, we assume that $p \equiv 3 \pmod 4$.

Introduction and motivation

Let p be a prime number. For simplicity, we assume that $p \equiv 3 \pmod 4$. Let $\chi_p : \mathbb{Z} \to \mathbb{C}^\times$ be the quadratic character

$$\chi_p(a) = \left(\frac{a}{p}\right),$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol.

Introduction and motivation

Let p be a prime number. For simplicity, we assume that $p \equiv 3 \pmod 4$. Let $\chi_p : \mathbb{Z} \to \mathbb{C}^\times$ be the quadratic character

$$\chi_p(a) = \left(\frac{a}{p}\right),$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol. The L-function associated with χ_p is given by

$$L(\chi_p, s) = \sum_{n=1}^{\infty} \frac{\chi_p(n)}{n^s}.$$

Introduction and motivation

Let p be a prime number. For simplicity, we assume that $p \equiv 3 \pmod 4$. Let $\chi_p : \mathbb{Z} \to \mathbb{C}^\times$ be the quadratic character

$$\chi_p(a) = \left(\frac{a}{p}\right),$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol. The L-function associated with χ_p is given by

$$L(\chi_p, s) = \sum_{n=1}^{\infty} \frac{\chi_p(n)}{n^s}.$$

The special value at $s = 1$ has a nice formula

$$L(\chi_p, 1) = \int_0^1 \frac{F_p(x)}{x(1 - x^p)} dx.$$

where

$$F_p(x) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) x^a.$$

Fekete polynomials

Definition

The polynomial

$$F_p(x) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) x^a.$$

is called the Fekete polynomial associated with the p.

Fekete polynomials

Definition

The polynomial

$$F_p(x) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) x^a.$$

is called the Fekete polynomial associated with the p.

Fekete polynomials have some two trivial zeros, namely 0 and 1.
Let

$$f_p(x) = \frac{F_p(x)}{x(1-x)}.$$

Proposition

$f_p(x)$ is a reciprocal polynomial of degree $p-3$, namely

$$x^{p-3} f_p\left(\frac{1}{x}\right) = f_p(x).$$

Fekete polynomials

Because $f_p(x)$ is a reciprocal polynomial of even degree, there exists a polynomial $g_p(x)$ such that

$$f_p(x) = x^{\frac{p-3}{2}} g_p\left(x + \frac{1}{x}\right).$$

We call $g_p(x)$ the reduced Fekete polynomial.

Fekete polynomials

Because $f_p(x)$ is a reciprocal polynomial of even degree, there exists a polynomial $g_p(x)$ such that

$$f_p(x) = x^{\frac{p-3}{2}} g_p\left(x + \frac{1}{x}\right).$$

We call $g_p(x)$ the reduced Fekete polynomial.

It turns out that $g_p(x)$ has remarkable properties. Furthermore, it contains lot of important arithemtic information.

A concrete example

Let take $p = 7$.

- $F_7(x) = \sum_{a=1}^{6} \left(\frac{a}{p}\right) x^a = x + x^2 - x^2 + x^4 - x^5 - x^6.$

A concrete example

Let take $p = 7$.

- $F_7(x) = \sum_{a=1}^{6} \left(\frac{a}{p}\right) x^a = x + x^2 - x^2 + x^4 - x^5 - x^6$.
- $f_7(x) = \frac{F_7(x)}{x(1-x)} = x^4 + 2x^3 + x^2 + 2x + 1$.

A concrete example

Let take $p = 7$.

- $F_7(x) = \sum_{a=1}^{6} \left(\frac{a}{p}\right) x^a = x + x^2 - x^2 + x^4 - x^5 - x^6.$
- $f_7(x) = \frac{F_7(x)}{x(1-x)} = x^4 + 2x^3 + x^2 + 2x + 1.$
- We have

$$f_7(x) = x^2 \left(x^2 + \frac{1}{x^2} + 2(x + \frac{1}{x}) + 1 \right).$$

A concrete example

Let take $p = 7$.

- $F_7(x) = \sum_{a=1}^{6} \left(\frac{a}{p}\right) x^a = x + x^2 - x^2 + x^4 - x^5 - x^6$.
- $f_7(x) = \frac{F_7(x)}{x(1-x)} = x^4 + 2x^3 + x^2 + 2x + 1$.
- We have

$$f_7(x) = x^2 \left(x^2 + \frac{1}{x^2} + 2(x + \frac{1}{x}) + 1\right).$$

Let $u = x + \frac{1}{x}$.

A concrete example

Let take $p = 7$.

- $F_7(x) = \sum_{a=1}^{6} \left(\frac{a}{p}\right) x^a = x + x^2 - x^2 + x^4 - x^5 - x^6$.
- $f_7(x) = \frac{F_7(x)}{x(1-x)} = x^4 + 2x^3 + x^2 + 2x + 1$.
- We have

$$f_7(x) = x^2 \left(x^2 + \frac{1}{x^2} + 2(x + \frac{1}{x}) + 1 \right).$$

Let $u = x + \frac{1}{x}$. Then $u^2 = x^2 + \frac{1}{x^2} + 2$.

A concrete example

Let take $p = 7$.

- $F_7(x) = \sum_{a=1}^{6} \left(\frac{a}{p}\right) x^a = x + x^2 - x^2 + x^4 - x^5 - x^6$.
- $f_7(x) = \frac{F_7(x)}{x(1-x)} = x^4 + 2x^3 + x^2 + 2x + 1$.
- We have

$$f_7(x) = x^2 \left(x^2 + \frac{1}{x^2} + 2(x + \frac{1}{x}) + 1 \right).$$

Let $u = x + \frac{1}{x}$. Then $u^2 = x^2 + \frac{1}{x^2} + 2$. Therefore

$$f_7(x) = x^2(u^2 + 2u - 1).$$

A concrete example

Let take $p = 7$.

- $F_7(x) = \sum_{a=1}^{6} \left(\frac{a}{p}\right) x^a = x + x^2 - x^2 + x^4 - x^5 - x^6$.
- $f_7(x) = \frac{F_7(x)}{x(1-x)} = x^4 + 2x^3 + x^2 + 2x + 1$.
- We have

$$f_7(x) = x^2 \left(x^2 + \frac{1}{x^2} + 2(x + \frac{1}{x}) + 1 \right).$$

Let $u = x + \frac{1}{x}$. Then $u^2 = x^2 + \frac{1}{x^2} + 2$. Therefore

$$f_7(x) = x^2(u^2 + 2u - 1).$$

We conclude that $g_7(x) = x^2 + 2x - 1$.

Values of reduced Fekete polynomials at $x = 2$

Our first theorem is the following.

Theorem

$$g_p(2) = f_p(1) = ph(-p).$$

Here $h(-p)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$.

Values of reduced Fekete polynomials at $x = 2$

Our first theorem is the following.

Theorem

$$g_p(2) = f_p(1) = ph(-p).$$

Here $h(-p)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$.

Proof of the theorem 1

We have

$$xf_p(x) = \frac{F_p(x)}{1-x}.$$

Proof of the theorem 1

We have

$$xf_p(x) = \frac{F_p(x)}{1-x}.$$

Taking the limit when $x \to 1$, we get

$$f_p(1) = F_p^{'}(1) = -\sum_{r=1}^{p-1} \left(\frac{r}{p}\right) r.$$

Proof of the theorem 1

We have

$$xf_p(x) = \frac{F_p(x)}{1-x}.$$

Taking the limit when $x \to 1$, we get

$$f_p(1) = F_p'(1) = -\sum_{r=1}^{p-1} \left(\frac{r}{p}\right) r.$$

Now, by the class number formula we have

$$\sum_{r=1}^{p-1} \left(\frac{r}{p}\right) r = -ph(-p).$$

Proof of the theorem 1

We have

$$xf_p(x) = \frac{F_p(x)}{1-x}.$$

Taking the limit when $x \to 1$, we get

$$f_p(1) = F_p^{'}(1) = -\sum_{r=1}^{p-1} \left(\frac{r}{p}\right) r.$$

Now, by the class number formula we have

$$\sum_{r=1}^{p-1} \left(\frac{r}{p}\right) r = -ph(-p).$$

Hence we see that

$$g_p(2) = f_p(1) = ph(-p).$$

Values of reduced Fekete polynomials at other integers

More generally, we have the following.

Theorem

- $g_p(-2) = f_p(-1) = -\left(2\left(\frac{2}{p}\right) - 1\right) h(-p)$.
- $g_p(-1) = -\frac{1}{2}\left(\left(\frac{p}{3}\right) + 3\right) h(-p)$.
- $g_p(0) = g_p(-2) = -\left(2\left(\frac{2}{p}\right) - 1\right) h(-p)$.
- $g_p(1) = -\frac{h(-p)}{2}\left(\frac{6}{p}\right)\left[6 - 3\left(\frac{2}{p}\right) - 2\left(\frac{3}{p}\right) + \left(\frac{6}{p}\right)\right]$.

Values of reduced Fekete polynomials at other integers

More generally, we have the following.

Theorem

- $g_p(-2) = f_p(-1) = -\left(2\left(\frac{2}{p}\right) - 1\right) h(-p)$.
- $g_p(-1) = -\frac{1}{2}\left(\left(\frac{p}{3}\right) + 3\right) h(-p)$.
- $g_p(0) = g_p(-2) = -\left(2\left(\frac{2}{p}\right) - 1\right) h(-p)$.
- $g_p(1) = -\frac{h(-p)}{2}\left(\frac{6}{p}\right)\left[6 - 3\left(\frac{2}{p}\right) - 2\left(\frac{3}{p}\right) + \left(\frac{6}{p}\right)\right]$.

Main idea of the proof: Compute $F_p(x)$ at $x = -1$, 1, i, ζ_3, and ζ_6.

Sketch of the proof for $g_p(-2)$

Substitute $x = -1$ we have

$$g_p(-2) = f_p(-1) = \frac{F_p(-1)}{(-1)(1+1)} = -\frac{F_p(-1)}{2}.$$

Sketch of the proof for $g_p(-2)$

Substitute $x = -1$ we have

$$g_p(-2) = f_p(-1) = \frac{F_p(-1)}{(-1)(1+1)} = -\frac{F_p(-1)}{2}.$$

By definition

$$F_p(-1) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) (-1)^a.$$

Sketch of the proof for $g_p(-2)$

Substitute $x = -1$ we have

$$g_p(-2) = f_p(-1) = \frac{F_p(-1)}{(-1)(1+1)} = -\frac{F_p(-1)}{2}.$$

By definition

$$F_p(-1) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)(-1)^a.$$

$$\begin{aligned}\sum_{a=1}^{p-1} \left(\frac{a}{p}\right)(-1)^a &= \sum_{a=1}^{\frac{p-1}{2}} \left[\left(\frac{2a}{p}\right)(-1)^{2a} + \left(\frac{p-2a}{p}\right)(-1)^{p-2a}\right] \\ &= 2\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{2a}{p}\right) = 2\left(\frac{2}{p}\right)\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right).\end{aligned}$$

Sketch the proof of $g_p(-2)$

By a classical theorem of Berndt, we have

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) = \left(2 - \left(\frac{2}{p}\right)\right) h(-p).$$

Sketch the proof of $g_p(-2)$

By a classical theorem of Berndt, we have

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) = \left(2 - \left(\frac{2}{p}\right)\right) h(-p).$$

From the above equality, we conclude that

$$g_p(-2) = f_p(-1) = -\left(2\left(\frac{2}{p}\right) - 1\right) h(-p).$$

Galois theory for Fekete polynomials

Let $s_p = f_p(1)f_p(-1) = g_p(2)g_p(-2)$. Then by the second theorem

$$s_p = -(2\left(\frac{2}{p}\right) - 1)ph(-p)^2.$$

Galois theory for Fekete polynomials

Let $s_p = f_p(1)f_p(-1) = g_p(2)g_p(-2)$. Then by the second theorem

$$s_p = -(2\left(\frac{2}{p}\right) - 1)ph(-p)^2.$$

It can be shown that

$$\Delta(f_p) = s_p \times \Delta(g_p)^2.$$

where $\Delta(f)$ is the discriminant of a polynomial f.

Galois theory for Fekete polynomials

Let $s_p = f_p(1)f_p(-1) = g_p(2)g_p(-2)$. Then by the second theorem

$$s_p = -(2\left(\frac{2}{p}\right) - 1)ph(-p)^2.$$

It can be shown that

$$\Delta(f_p) = s_p \times \Delta(g_p)^2.$$

where $\Delta(f)$ is the discriminant of a polynomial f. A direct corollary of this relation is

Theorem

$\sqrt{s_p}$ belongs the splitting field of f_p.

Galois theory for Fekete polynomials

Let $\mathbb{Q}(f_p)$, $\mathbb{Q}(g_p)$ be the splitting fields of f_p and g_p respectively.

Galois theory for Fekete polynomials

Let $\mathbb{Q}(f_p)$, $\mathbb{Q}(g_p)$ be the splitting fields of f_p and g_p respectively. It is easy to see that

$$[\mathbb{Q}(f):\mathbb{Q}(g)] \leq 2^{\frac{p-3}{2}},$$

and

$$(\frac{p-3}{2})! \geq [\mathbb{Q}(g_p):\mathbb{Q}] \geq \frac{[\mathbb{Q}(f_p):\mathbb{Q}]}{2^{\frac{p-3}{2}}}.$$

Galois theory for Fekete polynomials

Let $\mathbb{Q}(f_p)$, $\mathbb{Q}(g_p)$ be the splitting fields of f_p and g_p respectively. It is easy to see that

$$[\mathbb{Q}(f):\mathbb{Q}(g)] \leq 2^{\frac{p-3}{2}},$$

and

$$(\frac{p-3}{2})! \geq [\mathbb{Q}(g_p):\mathbb{Q}] \geq \frac{[\mathbb{Q}(f_p):\mathbb{Q}]}{2^{\frac{p-3}{2}}}.$$

Using the computer program PARI, we found that these are equality for $p \leq 43$.

Let $\mathbb{Q}(f_p)$, $\mathbb{Q}(g_p)$ be the splitting fields of f_p and g_p respectively. It is easy to see that

$$[\mathbb{Q}(f):\mathbb{Q}(g)] \leq 2^{\frac{p-3}{2}},$$

and

$$(\frac{p-3}{2})! \geq [\mathbb{Q}(g_p):\mathbb{Q}] \geq \frac{[\mathbb{Q}(f_p):\mathbb{Q}]}{2^{\frac{p-3}{2}}}.$$

Using the computer program PARI, we found that these are equality for $p \leq 43$. We conclude that

Theorem

Let p be a prime number such that $p \leq 43$. Then $\mathbb{Q}(g_p)/\mathbb{Q}$ is a Galois extension with Galois group S_{h_p} where $h_p = \frac{p-3}{2} = \deg(g_p)$. Additionally, $\mathbb{Q}(f_p)/\mathbb{Q}$ is a Galois extension of degree $2^{h_p}(h_p)!$

Some conjectures

Conjecture (Strong form)

f_p and g_p are irreducible over $\mathbb{Q}$. Furthermore, there is a split short exact sequence

$$1 \to (\mathbb{Z}/2)^{h_p} \to Gal(\mathbb{Q}(f_p)/\mathbb{Q}) \to Gal(\mathbb{Q}(g_p)/\mathbb{Q}) \cong S_{h_p} \to 1.$$

Here $h_p = \deg(g_p)$. Consequently, $Gal(\mathbb{Q}(f_p)/\mathbb{Q})$ is a semi-direct product of $(\mathbb{Z}/2)^{h_p}$ and S_{h_p}.

Some conjectures

Conjecture (Strong form)

f_p and g_p are irreducible over $\mathbb{Q}$. Furthermore, there is a split short exact sequence

$$1 \to (\mathbb{Z}/2)^{h_p} \to Gal(\mathbb{Q}(f_p)/\mathbb{Q}) \to Gal(\mathbb{Q}(g_p)/\mathbb{Q}) \cong S_{h_p} \to 1.$$

Here $h_p = \deg(g_p)$. Consequently, $Gal(\mathbb{Q}(f_p)/\mathbb{Q})$ is a semi-direct product of $(\mathbb{Z}/2)^{h_p}$ and S_{h_p}.

A weaker form of the above conjecture is.

Conjecture (Weak form)

f_p and g_p have no repeated roots.

Thank you