The average least quadratic non-residue and further variations

Jackie Voros

University of Bristol

June 2022

Introduction

Definition

An integer a is a quadratic residue modulo p if there exists some integer x such that $x^2 \equiv a \pmod{p}$.

Introduction

Definition

An integer a is a quadratic residue modulo p if there exists some integer x such that $x^2 \equiv a \pmod{p}$.

Euler's Criterion

For p an odd prime and a an integer coprime to p we have,

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod{p} \text{ if } a \text{ is a quadratic residue modulo } p, \\ -1 \pmod{p} \text{ if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Introduction

Definition

An integer a is a quadratic residue modulo p if there exists some integer x such that $x^2 \equiv a \pmod{p}$.

Euler's Criterion

For p an odd prime and a an integer coprime to p we have,

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod{p} \text{ if } a \text{ is a quadratic residue modulo } p, \\ -1 \pmod{p} \text{ if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Trivially, 0 and 1 will always be quadratic residues.

Introduction

Definition

The Legendre symbol is defined as follows. For an odd prime p and an integer a,

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue,} \\ -1, & \text{if } a \text{ is a quadratic non-residue,} \\ 0, & \text{if } a \text{ is a multiple of p.} \end{cases}$$

Introduction

Definition

The Legendre symbol is defined as follows. For an odd prime p and an integer a,

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue,} \\ -1, & \text{if } a \text{ is a quadratic non-residue,} \\ 0, & \text{if } a \text{ is a multiple of p.} \end{cases}$$

- It is totally multiplicative

Introduction

Definition

The Legendre symbol is defined as follows. For an odd prime p and an integer a,

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue,} \\ -1, & \text{if } a \text{ is a quadratic non-residue,} \\ 0, & \text{if } a \text{ is a multiple of p.} \end{cases}$$

- It is totally multiplicative
- It has period p

Introduction

Definition

The Legendre symbol is defined as follows. For an odd prime p and an integer a,

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue,} \\ -1, & \text{if } a \text{ is a quadratic non-residue,} \\ 0, & \text{if } a \text{ is a multiple of p.} \end{cases}$$

- It is totally multiplicative
- It has period p
- It obeys the law of quadratic reciprocity

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

History and motivation

Let $n_2(p)$ denote the least integer n such that n is a quadratic non-residue modulo p. Or equivalently, the least n such that $\left(\frac{n}{p}\right) = -1$. By convention we set $n_2(2) = 1$.

History and motivation

Let $n_2(p)$ denote the least integer n such that n is a quadratic non-residue modulo p. Or equivalently, the least n such that $\left(\frac{n}{p}\right) = -1$. By convention we set $n_2(2) = 1$.

Question

What is an upper bound on $n_2(p)$ on $[1, p-1]$ for large p?

History and motivation

Let $n_2(p)$ denote the least integer n such that n is a quadratic non-residue modulo p. Or equivalently, the least n such that $\left(\frac{n}{p}\right) = -1$. By convention we set $n_2(2) = 1$.

Question

What is an upper bound on $n_2(p)$ on $[1, p-1]$ for large p?

- (Gauss, 1801) If $p \equiv 1 \pmod 8$ then $n_2(p) < 2\sqrt{p} + 1$

History and motivation

Let $n_2(p)$ denote the least integer n such that n is a quadratic non-residue modulo p. Or equivalently, the least n such that $\left(\frac{n}{p}\right) = -1$. By convention we set $n_2(2) = 1$.

Question

What is an upper bound on $n_2(p)$ on $[1, p-1]$ for large p?

- (Gauss, 1801) If $p \equiv 1 \pmod 8$ then $n_2(p) < 2\sqrt{p} + 1$
- (Vinogradoff, 1917) $n_2(p) \ll \sqrt{p} \log p$, improved to $\ll p^{1/2\sqrt{e}} \log^2 p$

History and motivation

Let $n_2(p)$ denote the least integer n such that n is a quadratic non-residue modulo p. Or equivalently, the least n such that $\left(\frac{n}{p}\right) = -1$. By convention we set $n_2(2) = 1$.

Question

What is an upper bound on $n_2(p)$ on $[1, p-1]$ for large p?

- (Gauss, 1801) If $p \equiv 1 \pmod 8$ then $n_2(p) < 2\sqrt{p} + 1$
- (Vinogradoff, 1917) $n_2(p) \ll \sqrt{p} \log p$, improved to $\ll p^{1/2\sqrt{e}} \log^2 p$
- (Burgess, 1957) $n_2(p) \ll_\varepsilon p^{(1/4\sqrt{e})+\varepsilon}$

History and motivation

Let $n_2(p)$ denote the least integer n such that n is a quadratic non-residue modulo p. Or equivalently, the least n such that $\left(\frac{n}{p}\right) = -1$. By convention we set $n_2(2) = 1$.

Question

What is an upper bound on $n_2(p)$ on $[1, p-1]$ for large p?

- (Gauss, 1801) If $p \equiv 1 \pmod 8$ then $n_2(p) < 2\sqrt{p} + 1$
- (Vinogradoff, 1917) $n_2(p) \ll \sqrt{p} \log p$, improved to $\ll p^{1/2\sqrt{e}} \log^2 p$
- (Burgess, 1957) $n_2(p) \ll_\varepsilon p^{(1/4\sqrt{e})+\varepsilon}$
- (Linnik, 1942) Conversely, $\#\{p \le x : n_2(p) > x^\varepsilon\} \ll_\varepsilon 1$ for all x

History and motivation

Let $n_2(p)$ denote the least integer n such that n is a quadratic non-residue modulo p. Or equivalently, the least n such that $\left(\frac{n}{p}\right) = -1$. By convention we set $n_2(2) = 1$.

Question

What is an upper bound on $n_2(p)$ on $[1, p-1]$ for large p?

- (Gauss, 1801) If $p \equiv 1 \pmod 8$ then $n_2(p) < 2\sqrt{p} + 1$
- (Vinogradoff, 1917) $n_2(p) \ll \sqrt{p} \log p$, improved to $\ll p^{1/2\sqrt{e}} \log^2 p$
- (Burgess, 1957) $n_2(p) \ll_\varepsilon p^{(1/4\sqrt{e})+\varepsilon}$
- (Linnik, 1942) Conversely, $\#\{p \leq x : n_2(p) > x^\varepsilon\} \ll_\varepsilon 1$ for all x

This is a hard problem!

History and motivation

Let $n_2(p)$ denote the least integer n such that n is a quadratic non-residue modulo p. Or equivalently, the least n such that $\left(\frac{n}{p}\right) = -1$. By convention we set $n_2(2) = 1$.

Question

What is an upper bound on $n_2(p)$ on $[1, p-1]$ for large p?

- (Gauss, 1801) If $p \equiv 1 \pmod 8$ then $n_2(p) < 2\sqrt{p} + 1$
- (Vinogradoff, 1917) $n_2(p) \ll \sqrt{p} \log p$, improved to $\ll p^{1/2\sqrt{e}} \log^2 p$
- (Burgess, 1957) $n_2(p) \ll_\varepsilon p^{(1/4\sqrt{e})+\varepsilon}$
- (Linnik, 1942) Conversely, $\#\{p \leq x : n_2(p) > x^\varepsilon\} \ll_\varepsilon 1$ for all x

This is a hard problem!
Easier problem: average case behaviour.

Heuristic view

Easier question

What is the average value for $n_2(p)$ for any prime? Or, what is,

$$\lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{p \leq x} n_2(p)?$$

Heuristic view

Easier question

What is the average value for $n_2(p)$ for any prime? Or, what is,

$$\lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{p \le x} n_2(p)?$$

First, we note that $n_2(p)$ must be prime.

Heuristic view

Easier question

What is the average value for $n_2(p)$ for any prime? Or, what is,

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} n_2(p)?$$

First, we note that $n_2(p)$ must be prime.
We know there are $(p+1)/2$ residues (including 0) and $(p-1)/2$ non-residues.

Heuristic view

Easier question

What is the average value for $n_2(p)$ for any prime? Or, what is,

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} n_2(p)?$$

First, we note that $n_2(p)$ must be prime.
We know there are $(p+1)/2$ residues (including 0) and $(p-1)/2$ non-residues.
Let us assume any integer in [1,p-1] has a 50-50 chance of being a quadratic residue.

Heuristic view

Easier question

What is the average value for $n_2(p)$ for any prime? Or, what is,

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} n_2(p)?$$

First, we note that $n_2(p)$ must be prime.
We know there are $(p+1)/2$ residues (including 0) and $(p-1)/2$ non-residues.
Let us assume any integer in [1,p-1] has a 50-50 chance of being a quadratic residue.
Then $n_2(p) = p_k$ with probability 2^{-k} where p_k denotes the k^{th} prime.

Heuristic view

Easier question

What is the average value for $n_2(p)$ for any prime? Or, what is,

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} n_2(p)?$$

First, we note that $n_2(p)$ must be prime.
We know there are $(p+1)/2$ residues (including 0) and $(p-1)/2$ non-residues.
Let us assume any integer in [1,p-1] has a 50-50 chance of being a quadratic residue.
Then $n_2(p) = p_k$ with probability 2^{-k} where p_k denotes the k^{th} prime.
So we should have,

$$\sum_{k=1}^{\infty} p_k 2^{-k}.$$

Erdős's Theorem

Theorem (Erdős, 1961)

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} n_2(p) = \sum_{k=1}^{\infty} \frac{p_k}{2^k}.$$

Erdős's Theorem

Theorem (Erdős, 1961)

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\le x} n_2(p) = \sum_{k=1}^{\infty} \frac{p_k}{2^k}.$$

The two main steps to his proof are:

Erdős's Theorem

Theorem (Erdős, 1961)

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\le x} n_2(p) = \sum_{k=1}^{\infty} \frac{p_k}{2^k}.$$

The two main steps to his proof are:

1. He uses quadratic reciprocity to deal with fixed x

Erdős's Theorem

Theorem (Erdős, 1961)

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} n_2(p) = \sum_{k=1}^{\infty} \frac{p_k}{2^k}.$$

The two main steps to his proof are:

1. He uses quadratic reciprocity to deal with fixed x
2. He uses Linnik's ideas of the large sieve to show $n_2(p)$ does not get too large.

Erdős's Theorem

Theorem (Erdős, 1961)

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} n_2(p) = \sum_{k=1}^{\infty} \frac{p_k}{2^k}.$$

The two main steps to his proof are:

1. He uses quadratic reciprocity to deal with fixed x
2. He uses Linnik's ideas of the large sieve to show $n_2(p)$ does not get too large.

This result is finite, equalling approximately 3.6746...

Extensions

Erdős's result has been extended in many directions.

Extensions

Erdős's result has been extended in many directions.
For $p \equiv 1 \bmod k$, let $n_k(p)$ be the least integer that is not a k^{th} power modulo p. For other primes, $n_k(p) = 0$.

Extensions

Erdős's result has been extended in many directions.
For $p \equiv 1 \bmod k$, let $n_k(p)$ be the least integer that is not a k^{th} power modulo p. For other primes, $n_k(p) = 0$.

Theorem (Elliot, 1967)

$$\lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{p \leq x} n_k(p) = C_k$$

Extensions

Erdős's result has been extended in many directions.
For $p \equiv 1 \bmod k$, let $n_k(p)$ be the least integer that is not a k^{th} power modulo p. For other primes, $n_k(p) = 0$.

Theorem (Elliot, 1967)

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} n_k(p) = C_k$$

Let $g(p)$ denote the least primitive root modulo p.

Extensions

Erdős's result has been extended in many directions.
For $p \equiv 1 \bmod k$, let $n_k(p)$ be the least integer that is not a k^{th} power modulo p. For other primes, $n_k(p) = 0$.

Theorem (Elliot, 1967)

$$\lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{p \le x} n_k(p) = C_k$$

Let $g(p)$ denote the least primitive root modulo p.

Theorem (Burgess, Elliot, 1968)

$$\frac{1}{\pi(x)} \sum_{p \le x} g(p) \ll (\log x)^2 (\log \log x)^4.$$

This was sharpened by Elliot and Murata under GRH, and with an additional hypothesis, shown to be finite.

Extensions

For a positive integer m, let $n_2(m)$ be the least integer n relatively prime to m that is a quadratic non-residue modulo m.

Extensions

For a positive integer m, let $n_2(m)$ be the least integer n relatively prime to m that is a quadratic non-residue modulo m.

Theorem (Pollack, 2012)

$$\lim_{x\to\infty} \frac{1}{x} \sum_{m\le x} n_2(m) = \sum_{k=1}^{\infty} \frac{p_k - 1}{p_1 \cdot \ldots \cdot p_{k-1}}.$$

Extensions

For a positive integer m, let $n_2(m)$ be the least integer n relatively prime to m that is a quadratic non-residue modulo m.

Theorem (Pollack, 2012)

$$\lim_{x\to\infty} \frac{1}{x} \sum_{m\leq x} n_2(m) = \sum_{k=1}^{\infty} \frac{p_k - 1}{p_1 \cdot \ldots \cdot p_{k-1}}.$$

For a non-principal Dirichlet character χ, let n_χ denote the least integer n such that $\chi(n) \notin \{0, 1\}$. Order them by fundamental discriminant, D, so $\left(\frac{D}{\cdot}\right)$ is the associated Kronecker symbol.

Extensions

For a positive integer m, let $n_2(m)$ be the least integer n relatively prime to m that is a quadratic non-residue modulo m.

Theorem (Pollack, 2012)

$$\lim_{x\to\infty} \frac{1}{x} \sum_{m\le x} n_2(m) = \sum_{k=1}^{\infty} \frac{p_k - 1}{p_1 \cdot \ldots \cdot p_{k-1}}.$$

For a non-principal Dirichlet character χ, let n_χ denote the least integer n such that $\chi(n) \notin \{0,1\}$. Order them by fundamental discriminant, D, so $\left(\frac{D}{\cdot}\right)$ is the associated Kronecker symbol.

Theorem (Pollack, 2012)

$$\lim_{x\to\infty} \Big(\sum_{|D|<x} 1\Big)^{-1} \Big(\sum_{|D|<x} n_{\left(\frac{D}{\cdot}\right)}\Big) = \Theta \approx 4.9809\ldots$$

Extensions

For a positive integer m, let $n_2(m)$ be the least integer n relatively prime to m that is a quadratic non-residue modulo m.

Theorem (Pollack, 2012)

$$\lim_{x\to\infty} \frac{1}{x} \sum_{m\leq x} n_2(m) = \sum_{k=1}^{\infty} \frac{p_k - 1}{p_1 \cdot \ldots \cdot p_{k-1}}.$$

For a non-principal Dirichlet character χ, let n_χ denote the least integer n such that $\chi(n) \notin \{0,1\}$. Order them by fundamental discriminant, D, so $\left(\frac{D}{\cdot}\right)$ is the associated Kronecker symbol.

Theorem (Pollack, 2012)

$$\lim_{x\to\infty} \Big(\sum_{|D|<x} 1 \Big)^{-1} \Big(\sum_{|D|<x} n_{\left(\frac{D}{\cdot}\right)} \Big) = \Theta \approx 4.9809\ldots$$

This result was further extended to all non-principal characters.

Analogous results

We can view the following problems as almost identical the problems we have just seen.

Analogous results

We can view the following problems as almost identical the problems we have just seen.

Pollack, along with Martin, investigated the following.

Analogous results

We can view the following problems as almost identical the problems we have just seen.
Pollack, along with Martin, investigated the following.

- The average least non-split prime in the quadratic field of conductor p, where p is an odd prime.

Analogous results

We can view the following problems as almost identical the problems we have just seen.

Pollack, along with Martin, investigated the following.

- The average least non-split prime in the quadratic field of conductor p, where p is an odd prime.
    - p splits in $\mathbb{Q}(\sqrt{a})$ if and only if a is a quadratic residue modulo p.

Analogous results

We can view the following problems as almost identical the problems we have just seen.

Pollack, along with Martin, investigated the following.

- The average least non-split prime in the quadratic field of conductor p, where p is an odd prime.
  - p splits in $\mathbb{Q}(\sqrt{a})$ if and only if a is a quadratic residue modulo p.
- The average least inert prime, taken over all quadratic fields and ordered by discriminant.

Analogous results

We can view the following problems as almost identical the problems we have just seen.

Pollack, along with Martin, investigated the following.

- The average least non-split prime in the quadratic field of conductor p, where p is an odd prime.
  - p splits in $\mathbb{Q}(\sqrt{a})$ if and only if a is a quadratic residue modulo p.
- The average least inert prime, taken over all quadratic fields and ordered by discriminant.
- The average least non-split prime taken over cyclic cubic extensions of prime conductor.

Analogous results

We can view the following problems as almost identical the problems we have just seen.

Pollack, along with Martin, investigated the following.

- The average least non-split prime in the quadratic field of conductor p, where p is an odd prime.
    - p splits in $\mathbb{Q}(\sqrt{a})$ if and only if a is a quadratic residue modulo p.
- The average least inert prime, taken over all quadratic fields and ordered by discriminant.
- The average least non-split prime taken over cyclic cubic extensions of prime conductor.
- The average least non-split prime taken over all cubic extensions of $\mathbb{Q}$.

Analogous results

We can view the following problems as almost identical the problems we have just seen.

Pollack, along with Martin, investigated the following.

- The average least non-split prime in the quadratic field of conductor p, where p is an odd prime.
  - p splits in $\mathbb{Q}(\sqrt{a})$ if and only if a is a quadratic residue modulo p.
- The average least inert prime, taken over all quadratic fields and ordered by discriminant.
- The average least non-split prime taken over cyclic cubic extensions of prime conductor.
- The average least non-split prime taken over all cubic extensions of $\mathbb{Q}$.

Greg Martin and Paul Pollack. "The average least character non-residue and further variations on a theme of Erdős" (2013)

Modular forms

Our final variation on this theme involves Hecke eigenvalues.

Modular forms

Our final variation on this theme involves Hecke eigenvalues.
A modular form is a function on the complex upper half plane satisfying certain holomorphic and transformation conditions.

Modular forms

Our final variation on this theme involves Hecke eigenvalues.
A modular form is a function on the complex upper half plane satisfying certain holomorphic and transformation conditions. The weight, k, and the level, N, are associated integers of a modular form.

$$f(z)|_k\gamma = (cz+d)^{-k}f(\gamma z), \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \gamma z = \frac{az+b}{cz+d}$$

Modular forms

Our final variation on this theme involves Hecke eigenvalues.
A modular form is a function on the complex upper half plane satisfying certain holomorphic and transformation conditions. The weight, k, and the level, N, are associated integers of a modular form.

$$f(z)|_k\gamma = (cz+d)^{-k} f(\gamma z), \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \gamma z = \frac{az+b}{cz+d}$$

Principal congruence subgroup

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}$$

Modular forms

Our final variation on this theme involves Hecke eigenvalues.
A modular form is a function on the complex upper half plane satisfying certain holomorphic and transformation conditions. The weight, k, and the level, N, are associated integers of a modular form.

$$f(z)|_k\gamma = (cz+d)^{-k} f(\gamma z), \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \gamma z = \frac{az+b}{cz+d}$$

Principal congruence subgroup

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}$$

Congruence subgroup

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\}$$

Modular forms

All modular forms necessarily admit a Fourier expansion,

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}, \qquad a_n \in \mathbb{C}.$$

Modular forms

All modular forms necessarily admit a Fourier expansion,

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}, \qquad a_n \in \mathbb{C}.$$

A cusp form is a modular form whose Fourier expansion has $a_0 = 0$.

Modular forms

All modular forms necessarily admit a Fourier expansion,

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}, \qquad a_n \in \mathbb{C}.$$

A cusp form is a modular form whose Fourier expansion has $a_0 = 0$.
$S_k(\Gamma_0(N))$ denotes the set of cusp forms of weight k and level N under $\Gamma_0(N)$.

$$S_k(\Gamma_0(N)) = S_k^{\text{old}}(\Gamma_0(N)) \oplus S_k^{\text{new}}(\Gamma_0(N))$$

Modular forms

All modular forms necessarily admit a Fourier expansion,

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}, \qquad a_n \in \mathbb{C}.$$

A cusp form is a modular form whose Fourier expansion has $a_0 = 0$. $S_k(\Gamma_0(N))$ denotes the set of cusp forms of weight k and level N under $\Gamma_0(N)$.

$$S_k(\Gamma_0(N)) = S_k^{\text{old}}(\Gamma_0(N)) \oplus S_k^{\text{new}}(\Gamma_0(N))$$

A Hecke operator is a linear operator, T_n for each n, that acts on modular forms. An eigenform is a modular form that is an eigenvector for all T_n. The eigenvalues are its Fourier coefficients.

$$T_n(f) = a_n f$$

Newforms

Then a newform is in $S_k^{\text{new}}(\Gamma_0(N))$ and it is a cuspform, it is normalised and it is a Hecke eigenform. It has Fourier expansion,

$$f(z) = \sum_{n=1}^{\infty} \lambda_f(n) n^{(k-1)/2} e(nz), \qquad e(nz) = e^{2\pi i n z}.$$

Newforms

Then a newform is in $S_k^{\text{new}}(\Gamma_0(N))$ and it is a cuspform, it is normalised and it is a Hecke eigenform. It has Fourier expansion,

$$f(z) = \sum_{n=1}^{\infty} \lambda_f(n) n^{(k-1)/2} e(nz), \qquad e(nz) = e^{2\pi i n z}.$$

- $\lambda_f(n)$ is multiplicative

Newforms

Then a newform is in $S_k^{\text{new}}(\Gamma_0(N))$ and it is a cuspform, it is normalised and it is a Hecke eigenform. It has Fourier expansion,

$$f(z) = \sum_{n=1}^{\infty} \lambda_f(n) n^{(k-1)/2} e(nz), \qquad e(nz) = e^{2\pi i n z}.$$

- $\lambda_f(n)$ is multiplicative
- $\lambda_f(p)^2 = 1 + \lambda_f(p^2)$

Newforms

Then a newform is in $S_k^{\text{new}}(\Gamma_0(N))$ and it is a cuspform, it is normalised and it is a Hecke eigenform. It has Fourier expansion,

$$f(z) = \sum_{n=1}^{\infty} \lambda_f(n) n^{(k-1)/2} e(nz), \qquad e(nz) = e^{2\pi i n z}.$$

- $\lambda_f(n)$ is multiplicative
- $\lambda_f(p)^2 = 1 + \lambda_f(p^2)$
- $|\lambda_f(n)| \leq \tau(n)$, the divisor function

Possible analogous result?

Question

When is the first sign change in $\lambda_f(p)$ for prime p?

Possible analogous result?

Question

When is the first sign change in $\lambda_f(p)$ for prime p?

We have the following result. Let (ε_p) be a sequence of signs.

Theorem (Kowalski, Lau, Soundararajan, Wu, 2010)

Let $N = \Gamma_0(N)$. For any $\varepsilon > 0$, $\varepsilon < 1/2$, there exists $c > 0$ such that,

$$\frac{1}{|S_k^{\text{new}}(N)|} |\{f \in S_k^{\text{new}}(N) : \lambda_f(p) \text{ has sign } \varepsilon_p \text{ for } p \leq z\}| \geq \left(\frac{1}{2} - \varepsilon\right)^{\pi(z)}.$$

For $z = c\sqrt{(\log kN)(\log\log kN)}$, for kN large enough.

Thank you for listening!

Any questions?