# The Fekete-Szegö Theorem with Local Rationality Conditions on Curves

Robert Rumely

Second Annual Upstate Number Theory Conference
University of Rochester
April 28, 2012

# First Example

Consider the disc $D(0, R) \subset \mathbb{C}$. If $R > 1$, there are infinitely many algebraic integers whose conjugates all belong to $D(0, R)$. If $R < 1$ there are only finitely many.

It is not obvious, but these assertions remain true for $D(a, R)$, for any $a \in \mathbb{R}$.

Analogous assertions hold for a filled ellipse $\frac{x^2}{A^2} + \frac{y^2}{B^2} \leq 1$:

- If $(A + B)/2 > 1$, there are infinitely many algebraic integers whose conjugates all belong to the filled ellipse.
- If $(A + B)/2 < 1$, there are only finitely many.

# First Example

Consider the disc $D(0, R) \subset \mathbb{C}$. If $R > 1$, there are infinitely many algebraic integers whose conjugates all belong to $D(0, R)$. If $R < 1$ there are only finitely many.

It is not obvious, but these assertions remain true for $D(a, R)$, for any $a \in \mathbb{R}$.

Analogous assertions hold for a filled ellipse $\frac{x^2}{A^2} + \frac{y^2}{B^2} \leq 1$:

- If $(A + B)/2 > 1$, there are infinitely many algebraic integers whose conjugates all belong to the filled ellipse.
- If $(A + B)/2 < 1$, there are only finitely many.

# First Example

Consider the disc $D(0, R) \subset \mathbb{C}$. If $R > 1$, there are infinitely many algebraic integers whose conjugates all belong to $D(0, R)$. If $R < 1$ there are only finitely many.

It is not obvious, but these assertions remain true for $D(a, R)$, for any $a \in \mathbb{R}$.

Analogous assertions hold for a filled ellipse $\frac{x^2}{A^2} + \frac{y^2}{B^2} \leq 1$:

- If $(A + B)/2 > 1$, there are infinitely many algebraic integers whose conjugates all belong to the filled ellipse.
- If $(A + B)/2 < 1$, there are only finitely many.

# First Example

Consider the disc $D(0, R) \subset \mathbb{C}$. If $R > 1$, there are infinitely many algebraic integers whose conjugates all belong to $D(0, R)$. If $R < 1$ there are only finitely many.

It is not obvious, but these assertions remain true for $D(a, R)$, for any $a \in \mathbb{R}$.

Analogous assertions hold for a filled ellipse $\frac{x^2}{A^2} + \frac{y^2}{B^2} \leq 1$:

- If $(A + B)/2 > 1$, there are infinitely many algebraic integers whose conjugates all belong to the filled ellipse.
- If $(A + B)/2 < 1$, there are only finitely many.

# First Example

Consider the disc $D(0, R) \subset \mathbb{C}$. If $R > 1$, there are infinitely many algebraic integers whose conjugates all belong to $D(0, R)$. If $R < 1$ there are only finitely many.

It is not obvious, but these assertions remain true for $D(a, R)$, for any $a \in \mathbb{R}$.

Analogous assertions hold for a filled ellipse $\frac{x^2}{A^2} + \frac{y^2}{B^2} \leq 1$:

- If $(A + B)/2 > 1$, there are infinitely many algebraic integers whose conjugates all belong to the filled ellipse.
- If $(A + B)/2 < 1$, there are only finitely many.

# The Classical Theorems of Fekete and Fekete-Szegö

There is a measure of size for sets $E \subset \mathbb{C}$, called the logarithmic capacity $\gamma(E)$, which arises in potential theory and has applications in arithmetic:

**Theorem (Fekete, 1923; Fekete-Szegö, 1955)**

*Let $E \subset \mathbb{C}$ be a compact set which is stable under complex conjugation, has a piecewise smooth boundary, and is the closure of its interior. If the logarithmic capacity $\gamma(E) > 1$, there are infinitely many algebraic integers whose conjugates all belong to $E$. If $\gamma(E) < 1$, there are only finitely many.*

# The Classical Theorems of Fekete and Fekete-Szegö

There is a measure of size for sets $E \subset \mathbb{C}$, called the logarithmic capacity $\gamma(E)$, which arises in potential theory and has applications in arithmetic:

**Theorem (Fekete, 1923; Fekete-Szegö, 1955)**

*Let $E \subset \mathbb{C}$ be a compact set which is stable under complex conjugation, has a piecewise smooth boundary, and is the closure of its interior. If the logarithmic capacity $\gamma(E) > 1$, there are infinitely many algebraic integers whose conjugates all belong to $E$. If $\gamma(E) < 1$, there are only finitely many.*

# Definition of the Logarithmic Capacity

The basic harmonic potential in the plane is $-\log(|z-w|)$.

Given a probability measure $\nu$ with support contained $E$, its *energy integral* is

$$I(\nu) \;=\; \iint_{E\times E} -\log(|z-w|)\, d\nu(z)d\nu(w)\;.$$

The Robin constant $V_\infty(E)$ is the infimum of the energy integrals, over all probability measures with support in $E$:

$$V_\infty(E) \;=\; \inf_{\nu \text{ on } E} \iint_{E\times E} -\log(|z-w|)\, d\nu(z)d\nu(w)\;.$$

The logarithmic capacity is defined by $\gamma(E) = e^{-V_\infty(E)}$ .

# Definition of the Logarithmic Capacity

The basic harmonic potential in the plane is $-\log(|z-w|)$.

Given a probability measure $\nu$ with support contained $E$, its *energy integral* is

$$I(\nu) \;=\; \iint_{E\times E} -\log(|z-w|)\,d\nu(z)d\nu(w)\ .$$

The Robin constant $V_\infty(E)$ is the infimum of the energy integrals, over all probability measures with support in $E$:

$$V_\infty(E) \;=\; \inf_{\nu \text{ on } E} \iint_{E\times E} -\log(|z-w|)\,d\nu(z)d\nu(w)\ .$$

The logarithmic capacity is defined by $\gamma(E) = e^{-V_\infty(E)}$ .

# Definition of the Logarithmic Capacity

The basic harmonic potential in the plane is $-\log(|z-w|)$. Given a probability measure $\nu$ with support contained $E$, its *energy integral* is

$$I(\nu) \;=\; \iint_{E\times E} -\log(|z-w|)\, d\nu(z)d\nu(w) \;.$$

The Robin constant $V_\infty(E)$ is the infimum of the energy integrals, over all probability measures with support in $E$:

$$V_\infty(E) \;=\; \inf_{\nu \text{ on } E} \iint_{E\times E} -\log(|z-w|)\, d\nu(z)d\nu(w) \;.$$

The logarithmic capacity is defined by $\gamma(E) = e^{-V_\infty(E)}$ .

# Definition of the Logarithmic Capacity

The basic harmonic potential in the plane is $-\log(|z-w|)$.

Given a probability measure $\nu$ with support contained $E$, its *energy integral* is

$$I(\nu) \ = \ \iint_{E\times E} -\log(|z-w|)\, d\nu(z)d\nu(w) \ .$$

The Robin constant $V_\infty(E)$ is the infimum of the energy integrals, over all probability measures with support in $E$:

$$V_\infty(E) \ = \ \inf_{\nu \text{ on } E} \iint_{E\times E} -\log(|z-w|)\, d\nu(z)d\nu(w) \ .$$

The logarithmic capacity is defined by $\gamma(E) = e^{-V_\infty(E)}$ .

# Computing Capacities

If $E$ is compact and $\gamma(E) > 0$, there is a unique probability measure $\nu$ on $E$, called the *equilibrium distribution*, which achieves the minimimal energy integral $V_\infty(E)$.

The *Green's function* $G(z, \infty; E)$ is defined by

$$G(z, \infty; E) \ = \ -V_\infty(E) + \int_E \log(|z - w|) \, d\mu(z) \ .$$

When $E$ has a piecewise smooth boundary, the Green's function has the following properties:

- $G(z, \infty; E) = 0$ on $E$;
- $G(z, \infty; E)$ is continuous on $\mathbb{C}$, and harmonic and positive in $\mathbb{C} \backslash E$;
- $G(z, \infty; E) = \log(|z|) - V_\infty(E) + o(1)$ as $z \to \infty$.

Furthermore, it is uniquely characterized by these properties.

# Computing Capacities

If $E$ is compact and $\gamma(E) > 0$, there is a unique probability measure $\nu$ on $E$, called the *equilibrium distribution*, which achieves the minimimal energy integral $V_\infty(E)$.

The *Green's function* $G(z,\infty;E)$ is defined by

$$G(z,\infty;E) \;=\; -V_\infty(E) + \int_E \log(|z-w|)\,d\mu(z)\;.$$

When $E$ has a piecewise smooth boundary, the Green's function has the following properties:

- $G(z,\infty;E) = 0$ on $E$;
- $G(z,\infty;E)$ is continuous on $\mathbb{C}$, and harmonic and positive in $\mathbb{C}\backslash E$;
- $G(z,\infty;E) = \log(|z|) - V_\infty(E) + o(1)$ as $z \to \infty$.

Furthermore, it is uniquely characterized by these properties.

# Computing Capacities

If $E$ is compact and $\gamma(E) > 0$, there is a unique probability measure $\nu$ on $E$, called the *equilibrium distribution*, which achieves the minimimal energy integral $V_\infty(E)$.

The *Green's function* $G(z, \infty; E)$ is defined by

$$G(z, \infty; E) \;=\; -V_\infty(E) + \int_E \log(|z-w|)\, d\mu(z)\;.$$

When $E$ has a piecewise smooth boundary, the Green's function has the following properties:

- $G(z, \infty; E) = 0$ on $E$;
- $G(z, \infty; E)$ is continuous on $\mathbb{C}$, and harmonic and positive in $\mathbb{C}\backslash E$;
- $G(z, \infty; E) = \log(|z|) - V_\infty(E) + o(1)$ as $z \to \infty$.

Furthermore, it is uniquely characterized by these properties.

# Computing Capacities

If $E$ is compact and $\gamma(E) > 0$, there is a unique probability measure $\nu$ on $E$, called the *equilibrium distribution*, which achieves the minimimal energy integral $V_\infty(E)$.

The *Green's function* $G(z, \infty; E)$ is defined by

$$G(z, \infty; E) \;=\; -V_\infty(E) + \int_E \log(|z - w|)\, d\mu(z)\ .$$

When $E$ has a piecewise smooth boundary, the Green's function has the following properties:

- $G(z, \infty; E) = 0$ on $E$;
- $G(z, \infty; E)$ is continuous on $\mathbb{C}$, and harmonic and positive in $\mathbb{C} \backslash E$;
- $G(z, \infty; E) = \log(|z|) - V_\infty(E) + o(1)$ as $z \to \infty$.

Furthermore, it is uniquely characterized by these properties.

# Computing Capacities

If $E$ is compact and $\gamma(E) > 0$, there is a unique probability measure $\nu$ on $E$, called the *equilibrium distribution*, which achieves the minimimal energy integral $V_\infty(E)$.

The *Green's function* $G(z, \infty; E)$ is defined by

$$G(z, \infty; E) \;=\; -V_\infty(E) + \int_E \log(|z - w|)\, d\mu(z)\ .$$

When $E$ has a piecewise smooth boundary, the Green's function has the following properties:

- $G(z, \infty; E) = 0$ on $E$;
- $G(z, \infty; E)$ is continuous on $\mathbb{C}$, and harmonic and positive in $\mathbb{C} \backslash E$;
- $G(z, \infty; E) = \log(|z|) - V_\infty(E) + o(1)$ as $z \to \infty$.

Furthermore, it is uniquely characterized by these properties.

# Computing Capacities

If $E$ is compact and $\gamma(E) > 0$, there is a unique probability measure $\nu$ on $E$, called the *equilibrium distribution*, which achieves the minimimal energy integral $V_\infty(E)$.

The *Green's function* $G(z, \infty; E)$ is defined by

$$G(z, \infty; E) \;=\; -V_\infty(E) + \int_E \log(|z - w|)\, d\mu(z)\ .$$

When $E$ has a piecewise smooth boundary, the Green's function has the following properties:

- $G(z, \infty; E) = 0$ on $E$;
- $G(z, \infty; E)$ is continuous on $\mathbb{C}$, and harmonic and positive in $\mathbb{C} \backslash E$;
- $G(z, \infty; E) = \log(|z|) - V_\infty(E) + o(1)$ as $z \to \infty$.

Furthermore, it is uniquely characterized by these properties.

# Computing Capacities

If $E$ is compact and $\gamma(E) > 0$, there is a unique probability measure $\nu$ on $E$, called the *equilibrium distribution*, which achieves the minimimal energy integral $V_\infty(E)$.

The *Green's function* $G(z, \infty; E)$ is defined by

$$G(z, \infty; E) \ = \ -V_\infty(E) + \int_E \log(|z - w|)\, d\mu(z)\ .$$

When $E$ has a piecewise smooth boundary, the Green's function has the following properties:

- $G(z, \infty; E) = 0$ on $E$;
- $G(z, \infty; E)$ is continuous on $\mathbb{C}$, and harmonic and positive in $\mathbb{C} \backslash E$;
- $G(z, \infty; E) = \log(|z|) - V_\infty(E) + o(1)$ as $z \to \infty$.

Furthermore, it is uniquely characterized by these properties.

# Computing Capacities

The best way to compute capacities is to guess the Green's function, then read off the Robin constant by

$$V_\infty(E) \;=\; \lim_{z\to\infty} G(z,\infty;E) - \log(|z|) \;.$$

For example, when $E = D(0,R)$,

then $G(z,\infty;E) = \log^+(|z|/R)$

so $V_\infty(E) = -\log(R)$

and $\gamma(E) = e^{-(-\log(R))} = R$ .

If $E$ is connected, its Green's function can be computed by finding a conformal mapping from $\mathbb{P}^1(\mathbb{C})\backslash E$ to $\mathbb{P}^1(\mathbb{C})\backslash D(0,1)$ which takes $\infty \to \infty$.

# Computing Capacities

The best way to compute capacities is to guess the Green's function, then read off the Robin constant by

$$V_\infty(E) = \lim_{z\to\infty} G(z,\infty;E) - \log(|z|) .$$

For example, when $E = D(0,R)$,
then $G(z,\infty;E) = \log^+(|z|/R)$
so $V_\infty(E) = -\log(R)$
and $\gamma(E) = e^{-(-\log(R))} = R$ .

If $E$ is connected, its Green's function can be computed by finding a conformal mapping from $\mathbb{P}^1(\mathbb{C})\backslash E$ to $\mathbb{P}^1(\mathbb{C})\backslash D(0,1)$ which takes $\infty \to \infty$.

# Computing Capacities

The best way to compute capacities is to guess the Green's function, then read off the Robin constant by

$$V_\infty(E) \;=\; \lim_{z\to\infty} G(z,\infty;E) - \log(|z|)\;.$$

For example, when $E = D(0,R)$,
then $G(z,\infty;E) = \log^+(|z|/R)$
so $V_\infty(E) = -\log(R)$
and $\gamma(E) = e^{-(-\log(R))} = R$ .

If $E$ is connected, its Green's function can be computed by finding a conformal mapping from $\mathbb{P}^1(\mathbb{C})\backslash E$ to $\mathbb{P}^1(\mathbb{C})\backslash D(0,1)$ which takes $\infty \to \infty$.

# Computing Capacities

The best way to compute capacities is to guess the Green's function, then read off the Robin constant by

$$V_\infty(E) \;=\; \lim_{z\to\infty} G(z,\infty;E) - \log(|z|)\ .$$

For example, when $E = D(0,R)$,

then $G(z,\infty;E) = \log^+(|z|/R)$

so $V_\infty(E) = -\log(R)$

and $\gamma(E) = e^{-(-\log(R))} = R\ .$

If $E$ is connected, its Green's function can be computed by finding a conformal mapping from $\mathbb{P}^1(\mathbb{C})\backslash E$ to $\mathbb{P}^1(\mathbb{C})\backslash D(0,1)$ which takes $\infty \to \infty$.

# Computing Capacities

The best way to compute capacities is to guess the Green's function, then read off the Robin constant by

$$V_\infty(E) \;=\; \lim_{z\to\infty} G(z,\infty;E) - \log(|z|)\ .$$

For example, when $E = D(0,R)$,

then $G(z,\infty;E) = \log^+(|z|/R)$

so $V_\infty(E) = -\log(R)$

and $\gamma(E) = e^{-(-\log(R))} = R$ .

If $E$ is connected, its Green's function can be computed by finding a conformal mapping from $\mathbb{P}^1(\mathbb{C})\backslash E$ to $\mathbb{P}^1(\mathbb{C})\backslash D(0,1)$ which takes $\infty \to \infty$.

# Sketch of the Proof of the Fekete-Szegö Theorem

Suppose $\gamma(E) > 1$.
Let $U$ be the interior of $E$, then shrink $E$ inside $U$.

By discretizing the equilibrium distribution, construct a monic polynomial $P(z) \in \mathbb{R}[z]$ of degree $n$ whose normalized logarithm $\frac{1}{n}\log(|P(z)|)$ approximates $G(z,\infty;E) + V_\infty(E)$ outside $E$. Since $\gamma(E) > 1$, we have

$$\{z \in \mathbb{C} : |P(z)| \le 1\} \subset U .$$

By a process called *patching*, we can use $P(z)$ to construct a monic polynomial $Q(z) \in \mathbb{Z}[z]$ with much higher degree such that

$$\{z \in \mathbb{C} : |Q(z)| \le 1\} \subset U .$$

The algebraic integers in the Fekete-Szegö theorem are the roots of $R(z)^N - 1 = 0$ for $N = 1, 2, 3, \ldots$.

# Sketch of the Proof of the Fekete-Szegö Theorem

Suppose $\gamma(E) > 1$.
Let $U$ be the interior of $E$, then shrink $E$ inside $U$.

By discretizing the equilibrium distribution, construct a monic polynomial $P(z) \in \mathbb{R}[z]$ of degree $n$ whose normalized logarithm $\frac{1}{n}\log(|P(z)|)$ approximates $G(z, \infty; E) + V_\infty(E)$ outside $E$. Since $\gamma(E) > 1$, we have

$$\{z \in \mathbb{C} : |P(z)| \le 1\} \subset U .$$

By a process called *patching*, we can use $P(z)$ to construct a monic polynomial $Q(z) \in \mathbb{Z}[z]$ with much higher degree such that

$$\{z \in \mathbb{C} : |Q(z)| \le 1\} \subset U .$$

The algebraic integers in the Fekete-Szegö theorem are the roots of $R(z)^N - 1 = 0$ for $N = 1, 2, 3, \ldots$.

# Sketch of the Proof of the Fekete-Szegö Theorem

Suppose $\gamma(E) > 1$.
Let $U$ be the interior of $E$, then shrink $E$ inside $U$.

By discretizing the equilibrium distribution, construct a monic polynomial $P(z) \in \mathbb{R}[z]$ of degree $n$ whose normalized logarithm $\frac{1}{n}\log(|P(z)|)$ approximates $G(z,\infty;E) + V_\infty(E)$ outside $E$. Since $\gamma(E) > 1$, we have

$$\{z \in \mathbb{C} : |P(z)| \le 1\} \ \subset \ U \, .$$

By a process called *patching*, we can use $P(z)$ to construct a monic polynomial $Q(z) \in \mathbb{Z}[z]$ with much higher degree such that

$$\{z \in \mathbb{C} : |Q(z)| \le 1\} \ \subset \ U \, .$$

The algebraic integers in the Fekete-Szegö theorem are the roots of $R(z)^N - 1 = 0$ for $N = 1, 2, 3, \ldots$.

# Sketch of the Proof of the Fekete-Szegö Theorem

Suppose $\gamma(E) > 1$.
Let $U$ be the interior of $E$, then shrink $E$ inside $U$.

By discretizing the equilibrium distribution, construct a monic polynomial $P(z) \in \mathbb{R}[z]$ of degree $n$ whose normalized logarithm $\frac{1}{n}\log(|P(z)|)$ approximates $G(z, \infty; E) + V_\infty(E)$ outside $E$. Since $\gamma(E) > 1$, we have

$$\{z \in \mathbb{C} : |P(z)| \leq 1\} \subset U .$$

By a process called *patching*, we can use $P(z)$ to construct a monic polynomial $Q(z) \in \mathbb{Z}[z]$ with much higher degree such that

$$\{z \in \mathbb{C} : |Q(z)| \leq 1\} \subset U .$$

The algebraic integers in the Fekete-Szegö theorem are the roots of $R(z)^N - 1 = 0$ for $N = 1, 2, 3, \ldots$.

# Sketch of the Proof of the Fekete-Szegö Theorem

Suppose $\gamma(E) > 1$.
Let $U$ be the interior of $E$, then shrink $E$ inside $U$.

By discretizing the equilibrium distribution, construct a monic polynomial $P(z) \in \mathbb{R}[z]$ of degree $n$ whose normalized logarithm $\frac{1}{n}\log(|P(z)|)$ approximates $G(z, \infty; E) + V_\infty(E)$ outside $E$. Since $\gamma(E) > 1$, we have

$$\{z \in \mathbb{C} : |P(z)| \leq 1\} \subset U .$$

By a process called *patching*, we can use $P(z)$ to construct a monic polynomial $Q(z) \in \mathbb{Z}[z]$ with much higher degree such that

$$\{z \in \mathbb{C} : |Q(z)| \leq 1\} \subset U .$$

The algebraic integers in the Fekete-Szegö theorem are the roots of $R(z)^N - 1 = 0$ for $N = 1, 2, 3, ....$

# Second Example

The capacity of a segment $E = [a, b]$ is $\gamma(E) = (b - a)/4$.

**Theorem (Robinson, 1964)**

*Let $[a, b] \subset \mathbb{R}$ be an interval. If $(b - a)/4 > 1$ there are infinitely many totally real algebraic integers whose conjugates belong to $[a, b]$; if $(b - a)/4 < 1$ there are only finitely many.*

Here the conjugates belong to the *real* interior of $E$.

The theorem is proved by constructing Chebyshev-like polynomials in $\mathbb{Z}[z]$ which are monic and have large oscillations on $[a, b]$. Their roots are the totally real algebraic integers in the theorem.

# Second Example

The capacity of a segment $E = [a, b]$ is $\gamma(E) = (b - a)/4$.

**Theorem (Robinson, 1964)**

*Let $[a, b] \subset \mathbb{R}$ be an interval. If $(b - a)/4 > 1$ there are infinitely many totally real algebraic integers whose conjugates belong to $[a, b]$; if $(b - a)/4 < 1$ there are only finitely many.*

Here the conjugates belong to the *real* interior of $E$.

The theorem is proved by constructing Chebyshev-like polynomials in $\mathbb{Z}[z]$ which are monic and have large oscillations on $[a, b]$. Their roots are the totally real algebraic integers in the theorem.

# Second Example

The capacity of a segment $E = [a, b]$ is $\gamma(E) = (b - a)/4$.

**Theorem (Robinson, 1964)**

*Let $[a, b] \subset \mathbb{R}$ be an interval. If $(b - a)/4 > 1$ there are infinitely many totally real algebraic integers whose conjugates belong to $[a, b]$; if $(b - a)/4 < 1$ there are only finitely many.*

Here the conjugates belong to the *real* interior of $E$.

The theorem is proved by constructing Chebyshev-like polynomials in $\mathbb{Z}[z]$ which are monic and have large oscillations on $[a, b]$. Their roots are the totally real algebraic integers in the theorem.

# Second Example

The capacity of a segment $E = [a, b]$ is $\gamma(E) = (b - a)/4$.

**Theorem (Robinson, 1964)**

*Let $[a, b] \subset \mathbb{R}$ be an interval. If $(b - a)/4 > 1$ there are infinitely many totally real algebraic integers whose conjugates belong to $[a, b]$; if $(b - a)/4 < 1$ there are only finitely many.*

Here the conjugates belong to the *real* interior of $E$.

The theorem is proved by constructing Chebyshev-like polynomials in $\mathbb{Z}[z]$ which are monic and have large oscillations on $[a, b]$. Their roots are the totally real algebraic integers in the theorem.

# Third Example

**Theorem (R, 2000)**

*Let $[a, b] \subset \mathbb{R}$ be an interval, and let $S = \{p_1, \ldots, p_r\}$ be a finite set of primes. If*

$$\frac{b-a}{4} \cdot \prod_{p \in S} p^{-1/(p-1)} \; > \; 1,$$

*there are infinitely many totally real algebraic integers $\alpha$ such that each $p \in S$ splits completely in $\mathbb{Q}(\alpha)$. If the reverse inequality holds, there are only finitely many.*

There are capacities of $p$-adic sets too. The condition that $p$ splits completely is equivalent to requiring the conjugates in $\mathbb{C}_p$ (the completion of the algebraic closure of $\mathbb{Q}_p$) to belong to $\mathbb{Q}_p$.

# Third Example

**Theorem (R, 2000)**

*Let $[a, b] \subset \mathbb{R}$ be an interval, and let $S = \{p_1, \ldots, p_r\}$ be a finite set of primes. If*

$$\frac{b-a}{4} \cdot \prod_{p \in S} p^{-1/(p-1)} \ > \ 1,$$

*there are infinitely many totally real algebraic integers $\alpha$ such that each $p \in S$ splits completely in $\mathbb{Q}(\alpha)$. If the reverse inequality holds, there are only finitely many.*

There are capacities of $p$-adic sets too. The condition that $p$ splits completely is equivalent to requiring the conjugates in $\mathbb{C}_p$ (the completion of the algebraic closure of $\mathbb{Q}_p$) to belong to $\mathbb{Q}_p$.

# Third Example

**Theorem (R, 2000)**

*Let $[a, b] \subset \mathbb{R}$ be an interval, and let $S = \{p_1, \ldots, p_r\}$ be a finite set of primes. If*

$$\frac{b-a}{4} \cdot \prod_{p \in S} p^{-1/(p-1)} \; > \; 1,$$

*there are infinitely many totally real algebraic integers $\alpha$ such that each $p \in S$ splits completely in $\mathbb{Q}(\alpha)$. If the reverse inequality holds, there are only finitely many.*

There are capacities of $p$-adic sets too. The condition that $p$ splits completely is equivalent to requiring the conjugates in $\mathbb{C}_p$ (the completion of the algebraic closure of $\mathbb{Q}_p$) to belong to $\mathbb{Q}_p$.

# Integrality means avoiding $\infty$

What about the conjugates in $\mathbb{C}_p$ for $p \notin S$?

They all belong to $D_p(0,1) = \{z \in \mathbb{C}_p : |z|_p \leq 1\}$.

An algebraic number is an algebraic integer if and only if its $p$-adic conjugates belong to $D_p(0,1)$ for all $p$.

Another way of viewing the integrality condition is to say that the conjugates *avoid* $\infty$ in $\mathbb{P}^1(\mathbb{C}_p)$ for all finite primes. Note that $D_p(0,1) = \mathbb{P}^1(\mathbb{C}_p) \backslash B(\infty,1)^-$.

By allowing more general sets at nonarchimedean places, one can construct algebraic numbers which satisfy prescribed conditions at finitely many places, and are integral at the remaining places.

# Integrality means avoiding $\infty$

What about the conjugates in $\mathbb{C}_p$ for $p \notin S$?
They all belong to $D_p(0,1) = \{z \in \mathbb{C}_p : |z|_p \leq 1\}$.

An algebraic number is an algebraic integer if and only if its $p$-adic conjugates belong to $D_p(0,1)$ for all $p$.

Another way of viewing the integrality condition is to say that the conjugates *avoid* $\infty$ in $\mathbb{P}^1(\mathbb{C}_p)$ for all finite primes. Note that $D_p(0,1) = \mathbb{P}^1(\mathbb{C}_p) \backslash B(\infty,1)^-$.

By allowing more general sets at nonarchimedean places, one can construct algebraic numbers which satisfy prescribed conditions at finitely many places, and are integral at the remaining places.

# Integrality means avoiding $\infty$

What about the conjugates in $\mathbb{C}_p$ for $p \notin S$?
They all belong to $D_p(0,1) = \{z \in \mathbb{C}_p : |z|_p \leq 1\}$.

An algebraic number is an algebraic integer if and only if its $p$-adic conjugates belong to $D_p(0,1)$ for all $p$.

Another way of viewing the integrality condition is to say that the conjugates *avoid* $\infty$ in $\mathbb{P}^1(\mathbb{C}_p)$ for all finite primes. Note that $D_p(0,1) = \mathbb{P}^1(\mathbb{C}_p) \backslash B(\infty,1)^-$.

By allowing more general sets at nonarchimedean places, one can construct algebraic numbers which satisfy prescribed conditions at finitely many places, and are integral at the remaining places.

# Integrality means avoiding $\infty$

What about the conjugates in $\mathbb{C}_p$ for $p \notin S$?
They all belong to $D_p(0,1) = \{z \in \mathbb{C}_p : |z|_p \leq 1\}$.

An algebraic number is an algebraic integer if and only if its $p$-adic conjugates belong to $D_p(0,1)$ for all $p$.

Another way of viewing the integrality condition is to say that the conjugates *avoid* $\infty$ in $\mathbb{P}^1(\mathbb{C}_p)$ for all finite primes. Note that $D_p(0,1) = \mathbb{P}^1(\mathbb{C}_p) \backslash B(\infty,1)^-$.

By allowing more general sets at nonarchimedean places, one can construct algebraic numbers which satisfy prescribed conditions at finitely many places, and are integral at the remaining places.

# Integrality means avoiding $\infty$

What about the conjugates in $\mathbb{C}_p$ for $p \notin S$?
They all belong to $D_p(0,1) = \{z \in \mathbb{C}_p : |z|_p \leq 1\}$.

An algebraic number is an algebraic integer if and only if its $p$-adic conjugates belong to $D_p(0,1)$ for all $p$.

Another way of viewing the integrality condition is to say that the conjugates *avoid* $\infty$ in $\mathbb{P}^1(\mathbb{C}_p)$ for all finite primes. Note that $D_p(0,1) = \mathbb{P}^1(\mathbb{C}_p) \backslash B(\infty,1)^-$.

By allowing more general sets at nonarchimedean places, one can construct algebraic numbers which satisfy prescribed conditions at finitely many places, and are integral at the remaining places.

# Fourth Example: Allowing more general sets

## Theorem

*Let $0 < R, L \in \mathbb{R}$, and take $E_\infty = D(0,R) \cup [R, R+L]$, a 'disc with a tail'. Fix a prime p, and let*

$$E_p = p\mathbb{Z}_p^\times \cup \mathbb{Z}_p^\times \cup p^{-1}\mathbb{Z}_p^\times = \mathbb{Q}_p \cap (D_p(0,p) \backslash D_p(0,1/p)^-) \ ,$$

*a p-adic annulus. For each prime $q \neq p$, put $E_q = D_q(0,1)$. Then if*

$$\left(\tfrac{3}{4}R + \tfrac{1}{4}\tfrac{R^2+RL+L^2}{R+L}\right) \cdot p^{1-\frac{1}{p-1}+\frac{1}{(p-1)^2(1+p^2+p^4)}} > 1 \ ,$$

*there are infinitely many algebraic numbers whose whose conjugates in $\mathbb{C}_v$ belong to $E_v$, for each place $v$.*

*If the reverse inequality holds, there are only finitely many.*

# Allowing more general sets

The sets in the theorem are finite unions of 'basic sets':

The set $E_\infty$ is a union of a set in $\mathbb{C}$ which is the closure of its complex interior, and a set in $\mathbb{R}$ which is the closure of its real interior. Note that these sets need not be disjoint.

The set $E_p$ is a union of affine translates of $\mathbb{Z}_p$:

$$E_p = \bigcup_{i=-1}^{1} \bigcup_{a=1}^{p-1} \left( a \cdot p^i + p^{i+1}\mathbb{Z}_p \right) .$$

The sets $E_q = D_q(0,1)$ for $q \neq p$ are 'trivial' with respect to $\infty$.

# Allowing more general sets

The sets in the theorem are finite unions of 'basic sets':

The set $E_\infty$ is a union of a set in $\mathbb{C}$ which is the closure of its complex interior, and a set in $\mathbb{R}$ which is the closure of its real interior. Note that these sets need not be disjoint.

The set $E_p$ is a union of affine translates of $\mathbb{Z}_p$:

$$E_p = \bigcup_{i=-1}^{1} \bigcup_{a=1}^{p-1} \left( a \cdot p^i + p^{i+1}\mathbb{Z}_p \right) .$$

The sets $E_q = D_q(0, 1)$ for $q \neq p$ are 'trivial' with respect to $\infty$.

# Allowing more general sets

The sets in the theorem are finite unions of 'basic sets':

The set $E_\infty$ is a union of a set in $\mathbb{C}$ which is the closure of its complex interior, and a set in $\mathbb{R}$ which is the closure of its real interior. Note that these sets need not be disjoint.

The set $E_p$ is a union of affine translates of $\mathbb{Z}_p$:

$$E_p = \bigcup_{i=-1}^{1} \bigcup_{a=1}^{p-1} \left( a \cdot p^i + p^{i+1}\mathbb{Z}_p \right) .$$

The sets $E_q = D_q(0,1)$ for $q \neq p$ are 'trivial' with respect to $\infty$.

# Allowing more general sets

The sets in the theorem are finite unions of 'basic sets':

The set $E_\infty$ is a union of a set in $\mathbb{C}$ which is the closure of its complex interior, and a set in $\mathbb{R}$ which is the closure of its real interior. Note that these sets need not be disjoint.

The set $E_p$ is a union of affine translates of $\mathbb{Z}_p$:

$$E_p \;=\; \bigcup_{i=-1}^{1} \bigcup_{a=1}^{p-1} \left(a \cdot p^i + p^{i+1}\mathbb{Z}_p\right) .$$

The sets $E_q = D_q(0,1)$ for $q \neq p$ are 'trivial' with respect to $\infty$.

# Fifth Example

**Theorem (Robinson, 1968)**

*Let* $0 < a < b \in \mathbb{R}$. *Then the interval* $[a, b]$ *contains infinitely many totally real algebraic units if and only if*

1. $\log(\frac{b-a}{4}) > 0$ *and*
2. $\log(\frac{b-a}{4}) \cdot \log(\frac{b-a}{4ab}) - \log(\frac{\sqrt{b}+\sqrt{a}}{\sqrt{b}-\sqrt{a}})^2 > 0$

*If either condition fails, there are only finitely many.*

# Discussion

An algebraic number is a unit if and only if its conjugates belong to

$$D_p(0,1)\backslash D_p(0,1)^- \;=\; \mathbb{P}^1(\mathbb{C}_p)\backslash(B(\infty,1)^- \cup B(0,1)^-)$$

for each $p$, that is, if it avoids $\infty$ and 0 at each finite place.

The conditions in the Theorem are equivalent to the negative definiteness of

$$\Gamma \;=\; \begin{pmatrix} -\log(\frac{b-a}{4}) & \log(\frac{\sqrt{b}+\sqrt{a}}{\sqrt{b}-\sqrt{a}}) \\ \log(\frac{\sqrt{b}+\sqrt{a}}{\sqrt{b}-\sqrt{a}}) & -\log(\frac{b-a}{4ab}) \end{pmatrix} .$$

There are Green's functions and Robin constants with respect any point not in $E$. Here

$$\Gamma \;=\; \Gamma(E,\{\infty,0\}) \;=\; \begin{pmatrix} V_\infty(E) & G(0,\infty;E) \\ G(\infty,0;E) & V_0(E) \end{pmatrix}$$

is the 'Green's matrix of $E$' with respect to $\infty$ and 0.

# Discussion

An algebraic number is a unit if and only if its conjugates belong to

$$D_p(0,1)\backslash D_p(0,1)^- \;=\; \mathbb{P}^1(\mathbb{C}_p)\backslash(B(\infty,1)^- \cup B(0,1)^-)$$

for each $p$, that is, if it avoids $\infty$ and 0 at each finite place.

The conditions in the Theorem are equivalent to the negative definiteness of

$$\Gamma \;=\; \begin{pmatrix} -\log(\frac{b-a}{4}) & \log(\frac{\sqrt{b}+\sqrt{a}}{\sqrt{b}-\sqrt{a}}) \\ \log(\frac{\sqrt{b}+\sqrt{a}}{\sqrt{b}-\sqrt{a}}) & -\log(\frac{b-a}{4ab})\,. \end{pmatrix}$$

There are Green's functions and Robin constants with respect any point not in $E$. Here

$$\Gamma \;=\; \Gamma(E,\{\infty,0\}) \;=\; \begin{pmatrix} V_\infty(E) & G(0,\infty;E) \\ G(\infty,0;E) & V_0(E) \end{pmatrix}$$

is the 'Green's matrix of $E$' with respect to $\infty$ and 0.

# Discussion

An algebraic number is a unit if and only if its conjugates belong to

$$D_p(0,1)\backslash D_p(0,1)^- \;=\; \mathbb{P}^1(\mathbb{C}_p)\backslash(B(\infty,1)^- \cup B(0,1)^-)$$

for each $p$, that is, if it avoids $\infty$ and 0 at each finite place.

The conditions in the Theorem are equivalent to the negative definiteness of

$$\Gamma \;=\; \begin{pmatrix} -\log(\frac{b-a}{4}) & \log(\frac{\sqrt{b}+\sqrt{a}}{\sqrt{b}-\sqrt{a}}) \\ \log(\frac{\sqrt{b}+\sqrt{a}}{\sqrt{b}-\sqrt{a}}) & -\log(\frac{b-a}{4ab}) \;. \end{pmatrix}$$

There are Green's functions and Robin constants with respect any point not in $E$. Here

$$\Gamma \;=\; \Gamma(E,\{\infty,0\}) \;=\; \begin{pmatrix} V_\infty(E) & G(0,\infty;E) \\ G(\infty,0;E) & V_0(E) \end{pmatrix}$$

is the 'Green's matrix of $E$' with respect to $\infty$ and 0.

# The General Framework

Let $K$ be a global field, a number field or a finite extension of $\mathbb{F}_p(t)$ for some $p$. Fix an algebraic closure $\widetilde{K}$ of $K$.

Let $\mathcal{C}/K$ be a smooth, projective, geometrically integral curve.

Let $\mathfrak{X} = \{x_1, \ldots, x_m\} \subset \mathcal{C}(\widetilde{K})$ be a finite, galois-stable set of points: the points to *avoid*.

For each place $v$ of $K$, let $E_v \subset \mathcal{C}(\mathbb{C}_v)$ be a nonempty set disjoint from $\mathfrak{X}$. We will require that $E_v$ be galois-stable, and that it be a finite union of '$v$-basic sets' as defined below.

For all but finitely many places, we require that $E_v = \mathcal{C}(\mathbb{C}_v) \backslash (\bigcup_{i=1}^m B(x_i, 1)^-)$ be '$\mathfrak{X}$-trivial'.

# The General Framework

Let $K$ be a global field, a number field or a finite extension of $\mathbb{F}_p(t)$ for some $p$. Fix an algebraic closure $\widetilde{K}$ of $K$.

Let $\mathcal{C}/K$ be a smooth, projective, geometrically integral curve.

Let $\mathfrak{X} = \{x_1, \ldots, x_m\} \subset \mathcal{C}(\widetilde{K})$ be a finite, galois-stable set of points: the points to *avoid*.

For each place $v$ of $K$, let $E_v \subset \mathcal{C}(\mathbb{C}_v)$ be a nonempty set disjoint from $\mathfrak{X}$. We will require that $E_v$ be galois-stable, and that it be a finite union of '$v$-basic sets' as defined below.

For all but finitely many places, we require that $E_v = \mathcal{C}(\mathbb{C}_v) \backslash (\bigcup_{i=1}^m B(x_i, 1)^-)$ be '$\mathfrak{X}$-trivial'.

# The General Framework

Let $K$ be a global field, a number field or a finite extension of $\mathbb{F}_p(t)$ for some $p$. Fix an algebraic closure $\widetilde{K}$ of $K$.

Let $\mathcal{C}/K$ be a smooth, projective, geometrically integral curve.

Let $\mathfrak{X} = \{x_1, \ldots, x_m\} \subset \mathcal{C}(\widetilde{K})$ be a finite, galois-stable set of points: the points to *avoid*.

For each place $v$ of $K$, let $E_v \subset \mathcal{C}(\mathbb{C}_v)$ be a nonempty set disjoint from $\mathfrak{X}$. We will require that $E_v$ be galois-stable, and that it be a finite union of '$v$-basic sets' as defined below.

For all but finitely many places, we require that $E_v = \mathcal{C}(\mathbb{C}_v) \backslash (\bigcup_{i=1}^m B(x_i, 1)^-)$ be '$\mathfrak{X}$-trivial'.

# The General Framework

Let $K$ be a global field, a number field or a finite extension of $\mathbb{F}_p(t)$ for some $p$. Fix an algebraic closure $\widetilde{K}$ of $K$.

Let $\mathcal{C}/K$ be a smooth, projective, geometrically integral curve.

Let $\mathfrak{X} = \{x_1, \ldots, x_m\} \subset \mathcal{C}(\widetilde{K})$ be a finite, galois-stable set of points: the points to *avoid*.

For each place $v$ of $K$, let $E_v \subset \mathcal{C}(\mathbb{C}_v)$ be a nonempty set disjoint from $\mathfrak{X}$. We will require that $E_v$ be galois-stable, and that it be a finite union of '$v$-basic sets' as defined below.

For all but finitely many places, we require that $E_v = \mathcal{C}(\mathbb{C}_v) \backslash (\bigcup_{i=1}^{m} B(x_i, 1)^-)$ be '$\mathfrak{X}$-trivial'.

# The General Framework

Let $K$ be a global field, a number field or a finite extension of $\mathbb{F}_p(t)$ for some $p$. Fix an algebraic closure $\widetilde{K}$ of $K$.

Let $\mathcal{C}/K$ be a smooth, projective, geometrically integral curve.

Let $\mathfrak{X} = \{x_1, \ldots, x_m\} \subset \mathcal{C}(\widetilde{K})$ be a finite, galois-stable set of points: the points to *avoid*.

For each place $v$ of $K$, let $E_v \subset \mathcal{C}(\mathbb{C}_v)$ be a nonempty set disjoint from $\mathfrak{X}$. We will require that $E_v$ be galois-stable, and that it be a finite union of '$v$-basic sets' as defined below.

For all but finitely many places, we require that $E_v = \mathcal{C}(\mathbb{C}_v) \backslash (\bigcup_{i=1}^m B(x_i, 1)^-)$ be '$\mathfrak{X}$-trivial'.

# Basic Sets

If $v$ is archimedean and $K_v \cong \mathbb{C}$, a set $F_v \subset \mathcal{C}(\mathbb{C})$ is $v$-basic if it is simply connected, has a piecewise smooth boundary, and is the closure of its interior.

If $v$ is archimedean and $K_v \cong \mathbb{R}$, a set $F_v \subset \mathcal{C}(\mathbb{C})$ is $v$-basic if either

- it is simply connected, has a piecewise smooth boundary, and is the closure of its $\mathbb{C}$-interior; or
- it is contained in $\mathcal{C}(\mathbb{R})$ and is homeomorphic to a segment $[a, b]$.

If $v$ is nonarchimedean, a set $F_v \subset \mathcal{C}(\mathbb{C}_v)$ is $v$-basic if

- it is an open ball $B(a, r)^-$ or a closed ball $B(a, r)$; or
- it is a closed affinoid in the sense of rigid analysis; or
- for some separable algebraic extension $L_w/K_v$ (finite or infinite), it is the intersection of $\mathcal{C}(L_w)$ with an open or closed ball or an affinoid.

# Basic Sets

If $v$ is archimedean and $K_v \cong \mathbb{C}$, a set $F_v \subset \mathcal{C}(\mathbb{C})$ is $v$-basic if it is simply connected, has a piecewise smooth boundary, and is the closure of its interior.

If $v$ is archimedean and $K_v \cong \mathbb{R}$, a set $F_v \subset \mathcal{C}(\mathbb{C})$ is $v$-basic if either

- it is simply connected, has a piecewise smooth boundary, and is the closure of its $\mathbb{C}$-interior; or
- it is contained in $\mathcal{C}(\mathbb{R})$ and is homeomorphic to a segment $[a, b]$.

If $v$ is nonarchimedean, a set $F_v \subset \mathcal{C}(\mathbb{C}_v)$ is $v$-basic if

- it is an open ball $B(a, r)^-$ or a closed ball $B(a, r)$; or
- it is a closed affinoid in the sense of rigid analysis; or
- for some separable algebraic extension $L_w/K_v$ (finite or infinite), it is the intersection of $\mathcal{C}(L_w)$ with an open or closed ball or an affinoid.

# Basic Sets

If $v$ is archimedean and $K_v \cong \mathbb{C}$, a set $F_v \subset \mathcal{C}(\mathbb{C})$ is $v$-basic if it is simply connected, has a piecewise smooth boundary, and is the closure of its interior.

If $v$ is archimedean and $K_v \cong \mathbb{R}$, a set $F_v \subset \mathcal{C}(\mathbb{C})$ is $v$-basic if either

- it is simply connected, has a piecewise smooth boundary, and is the closure of its $\mathbb{C}$-interior; or
- it is contained in $\mathcal{C}(\mathbb{R})$ and is homeomorphic to a segment $[a, b]$.

If $v$ is nonarchimedean, a set $F_v \subset \mathcal{C}(\mathbb{C}_v)$ is $v$-basic if

- it is an open ball $B(a, r)^-$ or a closed ball $B(a, r)$; or
- it is a closed affinoid in the sense of rigid analysis; or
- for some separable algebraic extension $L_w/K_v$ (finite or infinite), it is the intersection of $\mathcal{C}(L_w)$ with an open or closed ball or an affinoid.

# The Fekete-Szegö Theorem with Local Rationality Conditions

**Theorem (R, 2012)**

*Let $K$ be a global field. Let $\mathcal{C}/K$ be a smooth, projective, geometrically integral curve. Let $\mathfrak{X} = \{x_1, \ldots, x_m\} \subset \mathcal{C}(\widetilde{K})$ be a finite set of points stable under* $\mathrm{Aut}(\widetilde{L}/K)$. *For each place $v$ of $K$, let $E_v \subset \mathcal{C}(\mathbb{C}_v) \backslash \mathfrak{X}$ be a nonempty set which is a finite union of $v$-basic sets and is stable under the group of continuous automorphisms* $\mathrm{Aut}^c(\mathbb{C}_v/K_v) \cong \mathrm{Aut}(\widetilde{K}^{\mathrm{sep}})/K_v$. *Assume that $E_v$ is $\mathfrak{X}$-trivial for all but finitely many $v$.*

*Put $\mathbb{E} = \prod_v E_v$. There is a measure of size $\gamma(\mathbb{E}, \mathfrak{X})$ called the* Cantor capacity *such that if $\gamma(\mathbb{E}, \mathfrak{X}) > 1$, there are infinitely many points of $\mathcal{C}(\widetilde{K})$ whose conjugates in $\mathcal{C}(\mathbb{C}_v)$ all belong to $E_v$, for each place $v$ of $K$. If $\gamma(\mathbb{E}, \mathfrak{X}) < 1$, there are only finitely many such points.*

# The Cantor Capacity

For each place $v$, define the local Green's matrix to be the $m \times m$ symmetric matrix

$$\Gamma(E_v, \mathfrak{X}) = \begin{pmatrix} V_{x_1}(E_v) & G(x_2, x_1; E_v) & \cdots & G(x_m, x_1; E_v) \\ G(x_1, x_2; E_v) & V_{x_2}(E_v) & \cdots & G(x_m, x_2; E_v) \\ \vdots & \vdots & \ddots & \vdots \\ G(x_1, x_m; E_v) & G(x_2, x_m; E_v) & \cdots & V_{x_m}(E_v) \end{pmatrix}$$

If $\mathfrak{X} \subset \mathcal{C}(K)$, put $\mathbb{E} = \prod_v E_v$. Define the global Green's matrix

$$\Gamma(\mathbb{E}, \mathfrak{X}) = \sum_v \Gamma(E_v, \mathfrak{X}) \log(Nv) ,$$

where $Nv$ is the order of the residue field at $v$, and $\log(Nv) = 1$ if $K_v \cong \mathbb{R}$ and $\log(Nv) = 2$ if $K_v \cong \mathbb{C}$.

If $\mathfrak{X} \not\subset \mathcal{C}(K)$, put $L = K(\mathfrak{X})$ and let $\Gamma(\mathbb{E}, \mathfrak{X}) = \frac{1}{[L:K]}\Gamma(\mathbb{E}_L, \mathfrak{X})$.

# The Cantor Capacity

For each place $v$, define the local Green's matrix to be the $m \times m$ symmetric matrix

$$\Gamma(E_v, \mathfrak{X}) = \begin{pmatrix} V_{x_1}(E_v) & G(x_2, x_1; E_v) & \cdots & G(x_m, x_1; E_v) \\ G(x_1, x_2; E_v) & V_{x_2}(E_v) & \cdots & G(x_m, x_2; E_v) \\ \vdots & \vdots & \ddots & \vdots \\ G(x_1, x_m; E_v) & G(x_2, x_m; E_v) & \cdots & V_{x_m}(E_v) \end{pmatrix}$$

If $\mathfrak{X} \subset \mathcal{C}(K)$, put $\mathbb{E} = \prod_v E_v$. Define the global Green's matrix

$$\Gamma(\mathbb{E}, \mathfrak{X}) = \sum_v \Gamma(E_v, \mathfrak{X}) \log(Nv) ,$$

where $Nv$ is the order of the residue field at $v$, and $\log(Nv) = 1$ if $K_v \cong \mathbb{R}$ and $\log(Nv) = 2$ if $K_v \cong \mathbb{C}$.

If $\mathfrak{X} \not\subset \mathcal{C}(K)$, put $L = K(\mathfrak{X})$ and let $\Gamma(\mathbb{E}, \mathfrak{X}) = \frac{1}{[L:K]}\Gamma(\mathbb{E}_L, \mathfrak{X})$.

# The Cantor Capacity

For each place $v$, define the local Green's matrix to be the $m \times m$ symmetric matrix

$$\Gamma(E_v, \mathfrak{X}) = \begin{pmatrix} V_{x_1}(E_v) & G(x_2, x_1; E_v) & \cdots & G(x_m, x_1; E_v) \\ G(x_1, x_2; E_v) & V_{x_2}(E_v) & \cdots & G(x_m, x_2; E_v) \\ \vdots & \vdots & \ddots & \vdots \\ G(x_1, x_m; E_v) & G(x_2, x_m; E_v) & \cdots & V_{x_m}(E_v) \end{pmatrix}$$

If $\mathfrak{X} \subset \mathcal{C}(K)$, put $\mathbb{E} = \prod_v E_v$. Define the global Green's matrix

$$\Gamma(\mathbb{E}, \mathfrak{X}) = \sum_v \Gamma(E_v, \mathfrak{X}) \log(Nv) ,$$

where $Nv$ is the order of the residue field at $v$, and $\log(Nv) = 1$ if $K_v \cong \mathbb{R}$ and $\log(Nv) = 2$ if $K_v \cong \mathbb{C}$.

If $\mathfrak{X} \not\subset \mathcal{C}(K)$, put $L = K(\mathfrak{X})$ and let $\Gamma(\mathbb{E}, \mathfrak{X}) = \frac{1}{[L:K]}\Gamma(\mathbb{E}_L, \mathfrak{X})$.

# The Cantor Capacity

Let
$\mathcal{P}_m = \{(s_1, \ldots, s_m) \in \mathbb{R}^m : s_1, \ldots, s_m \geq 0, s_1 + \cdots + s_m = 1\}$
denote the set of $m$-element *probability vectors*.

There is a simple criterion for a symmetric $m \times m$ matrix to be negative definite: The *value of* $\Gamma$ *as a matrix game* is

$$\mathrm{val}(\Gamma) \; = \; \max_{\vec{s} \in \mathcal{P}_m} \min_{\vec{r} \in \mathcal{P}_m} {}^t\vec{s}\,\Gamma\,\vec{r} \; ,$$

and $\Gamma$ is negative definite if and only if $\mathrm{val}(\Gamma) < 0$.

In general, for $\mathbb{E} = \prod_v E_v$ and $\mathfrak{X} = \{x_1, \ldots, x_m\}$, the Cantor capacity of $\mathbb{E}$ with respect to $\mathfrak{X}$ is defined to be

$$\gamma(\mathbb{E}, \mathfrak{X}) \; = \; e^{-\mathrm{val}(\Gamma(\mathbb{E}, \mathfrak{X}))} \; .$$

# The Cantor Capacity

Let
$\mathcal{P}_m = \{(s_1, \ldots, s_m) \in \mathbb{R}^m : s_1, \ldots, s_m \geq 0, s_1 + \cdots + s_m = 1\}$
denote the set of $m$-element *probability vectors*.

There is a simple criterion for a symmetric $m \times m$ matrix to be negative definite: The *value of* $\Gamma$ *as a matrix game* is

$$\mathrm{val}(\Gamma) \;=\; \max_{\vec{s} \in \mathcal{P}_m} \min_{\vec{r} \in \mathcal{P}_m} {}^t\vec{s}\Gamma\vec{r} \ ,$$

and $\Gamma$ is negative definite if and only if $\mathrm{val}(\Gamma) < 0$.

In general, for $\mathbb{E} = \prod_v E_v$ and $\mathfrak{X} = \{x_1, \ldots, x_m\}$, the Cantor capacity of $\mathbb{E}$ with respect to $\mathfrak{X}$ is defined to be

$$\gamma(\mathbb{E}, \mathfrak{X}) \;=\; e^{-\mathrm{val}(\Gamma(\mathbb{E}, \mathfrak{X}))} \ .$$

Let
$\mathcal{P}_m = \{(s_1, \ldots, s_m) \in \mathbb{R}^m : s_1, \ldots, s_m \geq 0, s_1 + \cdots + s_m = 1\}$
denote the set of $m$-element *probability vectors*.

There is a simple criterion for a symmetric $m \times m$ matrix to be negative definite: The *value of* $\Gamma$ *as a matrix game* is

$$\text{val}(\Gamma) \;=\; \max_{\vec{s} \in \mathcal{P}_m} \min_{\vec{r} \in \mathcal{P}_m} {}^t\vec{s}\,\Gamma\,\vec{r} \; ,$$

and $\Gamma$ is negative definite if and only if $\text{val}(\Gamma) < 0$.

In general, for $\mathbb{E} = \prod_v E_v$ and $\mathfrak{X} = \{x_1, \ldots, x_m\}$, the Cantor capacity of $\mathbb{E}$ with respect to $\mathfrak{X}$ is defined to be

$$\gamma(\mathbb{E}, \mathfrak{X}) \;=\; e^{-\text{val}(\Gamma(\mathbb{E}, \mathfrak{X}))} \; .$$

# An Elliptic Curve example

Let $\mathcal{E}/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 - 256x$.

The real locus $\mathcal{E}(\mathbb{R})$ has two components, with a bounded loop lying over the interval $[-16, 0]$.

**Theorem**

*There are infinitely many points $\alpha \in \mathcal{E}(\widetilde{\mathbb{Q}})$ whose archimedean conjugates all belong to the bounded real loop of $\mathcal{E}(\mathbb{R})$, whose 2-adic conjugates all belong to $\mathcal{E}(\mathbb{Z}_2)$, and whose p-adic conjugates all belong to $\mathcal{E}(\widehat{\mathcal{O}_p})$ where $\widehat{\mathcal{O}_p}$ is the ring of integers of $\mathbb{C}_p$*

Here $\mathfrak{X} = \{\overline{o}\}$ (the origin of $\mathcal{E}$), and $\gamma(\mathbb{E}, \mathfrak{X}) = \prod_v \gamma_{\overline{o}}(E_v)$ where

$$\gamma_{\overline{o}}(E_\infty) = 2, \quad \gamma_{\overline{o}}(E_2) = 2^{-106/107}, \text{ and } \quad \gamma_{\overline{o}}(E_p) = 1 \text{ for all odd } p.$$

# An Elliptic Curve example

Let $\mathcal{E}/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 - 256x$.

The real locus $\mathcal{E}(\mathbb{R})$ has two components, with a bounded loop lying over the interval $[-16, 0]$.

**Theorem**

*There are infinitely many points $\alpha \in \mathcal{E}(\widetilde{\mathbb{Q}})$ whose archimedean conjugates all belong to the bounded real loop of $\mathcal{E}(\mathbb{R})$, whose 2-adic conjugates all belong to $\mathcal{E}(\mathbb{Z}_2)$, and whose p-adic conjugates all belong to $\mathcal{E}(\widehat{\mathcal{O}}_p)$ where $\widehat{\mathcal{O}}_p$ is the ring of integers of $\mathbb{C}_p$*

Here $\mathfrak{X} = \{\overline{o}\}$ (the origin of $\mathcal{E}$), and $\gamma(\mathbb{E}, \mathfrak{X}) = \prod_v \gamma_{\overline{o}}(E_v)$ where

$$\gamma_{\overline{o}}(E_\infty) = 2, \quad \gamma_{\overline{o}}(E_2) = 2^{-106/107}, \text{ and } \quad \gamma_{\overline{o}}(E_p) = 1 \text{ for all odd } p.$$

# A Fermat Curve example

Take $K = \mathbb{Q}$ and consider the Fermat Curve $\mathcal{F}$ with affine equation $x^p + y^p = 1$.

It has $p$ points at $\infty$; let $\mathfrak{X}$ be that set of points.

Take $0 < R \in \mathbb{R}$ and put $E_\infty = \{(x, y) \in \mathcal{F}(\mathbb{C}) : |x| \leq R\}$.
At the prime $p$, let $L_w/\mathbb{Q}_p$ be the extension $L_w = \mathbb{Q}_p(\zeta_p)$.
Put $E_p = \mathcal{F}(\mathcal{O}_{L_w})$.
For all other primes $q$, let $E_q$ be the $\mathfrak{X}$-trivial set.

McCallum has determined a regular model for $\mathcal{F}$ over $\mathcal{O}_{L_w}$; it has $n_p$ components of a certain type, corresponding to the number of nontrivial linear $\mathbb{F}_p$-rational factors of the equation $((x - y)^p - (x^p - y^p))/p \equiv 0 \pmod{p}$.

# A Fermat Curve example

Take $K = \mathbb{Q}$ and consider the Fermat Curve $\mathcal{F}$ with affine equation $x^p + y^p = 1$.

It has $p$ points at $\infty$; let $\mathfrak{X}$ be that set of points.

Take $0 < R \in \mathbb{R}$ and put $E_\infty = \{(x, y) \in \mathcal{F}(\mathbb{C}) : |x| \leq R\}$.
At the prime $p$, let $L_w/\mathbb{Q}_p$ be the extension $L_w = \mathbb{Q}_p(\zeta_p)$.
Put $E_p = \mathcal{F}(\mathcal{O}_{L_w})$.
For all other primes $q$, let $E_q$ be the $\mathfrak{X}$-trivial set.

McCallum has determined a regular model for $\mathcal{F}$ over $\mathcal{O}_{L_w}$; it has $n_p$ components of a certain type, corresponding to the number of nontrivial linear $\mathbb{F}_p$-rational factors of the equation $((x - y)^p - (x^p - y^p))/p \equiv 0 \pmod{p}$.

# A Fermat Curve example

Take $K = \mathbb{Q}$ and consider the Fermat Curve $\mathcal{F}$ with affine equation $x^p + y^p = 1$.

It has $p$ points at $\infty$; let $\mathfrak{X}$ be that set of points.

Take $0 < R \in \mathbb{R}$ and put $E_\infty = \{(x, y) \in \mathcal{F}(\mathbb{C}) : |x| \leq R\}$.
At the prime $p$, let $L_w/\mathbb{Q}_p$ be the extension $L_w = \mathbb{Q}_p(\zeta_p)$.
Put $E_p = \mathcal{F}(\mathcal{O}_{L_w})$.
For all other primes $q$, let $E_q$ be the $\mathfrak{X}$-trivial set.

McCallum has determined a regular model for $\mathcal{F}$ over $\mathcal{O}_{L_w}$; it has $n_p$ components of a certain type, corresponding to the number of nontrivial linear $\mathbb{F}_p$-rational factors of the equation $((x - y)^p - (x^p - y^p))/p \equiv 0 \pmod{p}$.

# A Fermat Curve example

Take $K = \mathbb{Q}$ and consider the Fermat Curve $\mathcal{F}$ with affine equation $x^p + y^p = 1$.

It has $p$ points at $\infty$; let $\mathfrak{X}$ be that set of points.

Take $0 < R \in \mathbb{R}$ and put $E_\infty = \{(x, y) \in \mathcal{F}(\mathbb{C}) : |x| \leq R\}$.
At the prime $p$, let $L_w/\mathbb{Q}_p$ be the extension $L_w = \mathbb{Q}_p(\zeta_p)$.
Put $E_p = \mathcal{F}(\mathcal{O}_{L_w})$.
For all other primes $q$, let $E_q$ be the $\mathfrak{X}$-trivial set.

McCallum has determined a regular model for $\mathcal{F}$ over $\mathcal{O}_{L_w}$; it has $n_p$ components of a certain type, corresponding to the number of nontrivial linear $\mathbb{F}_p$-rational factors of the equation $((x - y)^p - (x^p - y^p))/p \equiv 0 \pmod{p}$.

# A Fermat Curve example

**Theorem**

*There are infinitely many points of $\mathcal{F}(\widetilde{\mathbb{Q}})$ which have all their conjugates in $E_v$ for each $v$ if*

$$R \cdot p^{-\frac{p(2p-1)}{(p-1)^2((2n_p+2)p-n_p)}} > 1,$$

*and only finitely many if the opposite inequality holds.*