Artin's Conjecture: Unconditional Approach and Elliptic Curve Analogue

Sourav Sen Gupta

University of Washington

November 14, 2008

Artin's 'Primitive Root' Conjecture

Primitive Root

Primitive Root

Definition (Primitive Root)

An integer a is called the *primitive root* of a prime p if a generates the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$, i.e, the order of a modulo p is $p-1$.

Primitive Root

Definition (Primitive Root)

An integer a is called the *primitive root* of a prime p if a generates the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$, i.e, the order of a modulo p is $p-1$.

- Question 1
  "How many primitive roots are there for a fixed prime p?"

Primitive Root

Definition (Primitive Root)

An integer a is called the *primitive root* of a prime p if a generates the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$, i.e, the order of a modulo p is $p-1$.

- Question 1
  "How many primitive roots are there for a fixed prime p?"

- Answer 1
  "If we fix p, there are $\phi(p-1)$ primitive root modulo p, where ϕ is the Euler totient function."

Question Reversed

How about reversing the question?

Question Reversed

How about reversing the question?

What if we fix an integer a instead of fixing a prime p and ask a similar question?

Question Reversed

How about reversing the question?

What if we fix an integer *a* instead of fixing a prime *p* and ask a similar question?

- Question 2
  "If we fix an integer, 10 say, then for how many primes *p* will 10 be a primitive root?"

Question Reversed

How about reversing the question?

What if we fix an integer a instead of fixing a prime p and ask a similar question?

- Question 2
  "If we fix an integer, 10 say, then for how many primes p will 10 be a primitive root?"

- Answer 2
  "10 is probably a primitive root for infinitely many primes p."

Question Reversed

How about reversing the question?

What if we fix an integer a instead of fixing a prime p and ask a similar question?

- Question 2
  "If we fix an integer, 10 say, then for how many primes p will 10 be a primitive root?"

- Answer 2
  "10 is probably a primitive root for infinitely many primes p."

  \- Gauss

Artin's Conjecture

Conjecture (Emil Artin, 1927)

Artin's Conjecture

Conjecture (Emil Artin, 1927)

For any given integer a, if $a \neq 0, 1, -1$ and if a is not a perfect square, then there exist infinitely many primes p for which a is a primitive root modulo p.

Artin's Conjecture

Conjecture (Emil Artin, 1927)

For any given integer a, if $a \neq 0, 1, -1$ and if a is not a perfect square, then there exist infinitely many primes p for which a is a primitive root modulo p.

Conjecture (Stronger Form)

Artin's Conjecture

Conjecture (Emil Artin, 1927)

For any given integer a, if $a \neq 0, 1, -1$ and if a is not a perfect square, then there exist infinitely many primes p for which a is a primitive root modulo p.

Conjecture (Stronger Form)

If $a \neq 0, 1, -1$ and a is not a perfect square, then there exists a positive constant $A(a)$ depending on a

Artin's Conjecture

Conjecture (Emil Artin, 1927)

For any given integer a, if $a \neq 0, 1, -1$ and if a is not a perfect square, then there exist infinitely many primes p for which a is a primitive root modulo p.

Conjecture (Stronger Form)

If $a \neq 0, 1, -1$ and a is not a perfect square, then there exists a positive constant $A(a)$ depending on a such that for $x \to \infty$,

$$N_a(x) = \#\left\{p \leq x \ : \ \langle \overline{a} \rangle = (\mathbb{Z}/p\mathbb{Z})^*\right\} \sim A(a)\frac{x}{\log x}$$

where $\overline{a} = a \pmod{p}$.

Artin's Heuristic Idea

Artin's Heuristic Idea

The necessary and sufficient condition for a being a primitive root of p is

$$a^{(p-1)/q} \not\equiv 1 \pmod{p} \quad \forall \text{ prime } q|p-1$$

Artin's Heuristic Idea

The necessary and sufficient condition for a being a primitive root of p is

$$a^{(p-1)/q} \not\equiv 1 \pmod{p} \quad \forall \text{ prime } q | p-1$$

Heuristic Idea

$\langle \overline{a} \rangle = (\mathbb{Z}/p\mathbb{Z})^*$ if the following two events do not occur simultaneously for any prime q

Artin's Heuristic Idea

The necessary and sufficient condition for a being a primitive root of p is

$$a^{(p-1)/q} \not\equiv 1 \pmod{p} \quad \forall \text{ prime } q | p-1$$

Heuristic Idea

$\langle \overline{a} \rangle = (\mathbb{Z}/p\mathbb{Z})^*$ if the following two events do not occur simultaneously for any prime q

$$p \equiv 1 \pmod{q}$$

Artin's Heuristic Idea

The necessary and sufficient condition for a being a primitive root of p is

$$a^{(p-1)/q} \not\equiv 1 \pmod{p} \quad \forall \text{ prime } q|p-1$$

Heuristic Idea

$\langle \bar{a} \rangle = (\mathbb{Z}/p\mathbb{Z})^*$ if the following two events do not occur simultaneously for any prime q

$$p \equiv 1 \pmod{q}$$
$$a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$$

Artin's Heuristic Idea

Probabilities of the events:

Artin's Heuristic Idea

Probabilities of the events:

$$P_1 := \mathcal{P}\left(p \text{ prime } : \ p \equiv 1 \pmod{q}\right)$$

Artin's Heuristic Idea

Probabilities of the events:

$$\begin{aligned} P_1 := &\ \mathcal{P}\left(p \text{ prime } : \ p \equiv 1 \pmod{q}\right) \\ = &\ \mathcal{P}\left(p \text{ prime } : \ p \in \{aq+1\}_{a \in \mathbb{Z}}\right) \end{aligned}$$

Artin's Heuristic Idea

Probabilities of the events:

$$\begin{aligned} P_1 :&= \mathcal{P}\left(p \text{ prime } \;:\; p \equiv 1 \pmod{q}\right) \\ &= \mathcal{P}\left(p \text{ prime } \;:\; p \in \{aq+1\}_{a\in\mathbb{Z}}\right) \\ &= \frac{1}{\phi(q)} = \frac{1}{q-1} \end{aligned}$$

Artin's Heuristic Idea

Probabilities of the events:

$$\begin{aligned} P_1 &:= \mathcal{P}\left(p \text{ prime } : \ p \equiv 1 \pmod{q}\right) \\ &= \mathcal{P}\left(p \text{ prime } : \ p \in \{aq+1\}_{a \in \mathbb{Z}}\right) \\ &= \frac{1}{\phi(q)} = \frac{1}{q-1} \quad \text{by Dirichlet's Theorem} \end{aligned}$$

Artin's Heuristic Idea

Probabilities of the events:

$$\begin{aligned} P_1 := \mathcal{P}\,(p \text{ prime} \; : \; p \equiv 1 \pmod{q}) \\ = \mathcal{P}\,(p \text{ prime} \; : \; p \in \{aq+1\}_{a \in \mathbb{Z}}) \\ = \frac{1}{\phi(q)} = \frac{1}{q-1} \quad \text{by Dirichlet's Theorem} \end{aligned}$$

$$P_2 := \mathcal{P}\left(p \text{ prime} \; : \; a^{(p-1)/q} \equiv 1 \pmod{p}\right)$$

Artin's Heuristic Idea

Probabilities of the events:

$$\begin{aligned} P_1 :&= \mathcal{P}\left(p \text{ prime} \;:\; p \equiv 1 \pmod q\right) \\ &= \mathcal{P}\left(p \text{ prime} \;:\; p \in \{aq+1\}_{a\in\mathbb{Z}}\right) \\ &= \frac{1}{\phi(q)} = \frac{1}{q-1} \quad \text{by Dirichlet's Theorem} \end{aligned}$$

$$\begin{aligned} P_2 :&= \mathcal{P}\left(p \text{ prime} \;:\; a^{(p-1)/q} \equiv 1 \pmod p\right) \quad \text{for } a = b^k,\ 1 \le k \le p-1 \\ &= \mathcal{P}\left(p \text{ prime} \;:\; \frac{k(p-1)}{q} \equiv 0 \pmod{p-1}\right) \end{aligned}$$

Artin's Heuristic Idea

Probabilities of the events:

$$
\begin{aligned}
P_1 := {} & \mathcal{P}\left(p \text{ prime} \;:\; p \equiv 1 \pmod{q}\right) \\
= {} & \mathcal{P}\left(p \text{ prime} \;:\; p \in \{aq+1\}_{a\in\mathbb{Z}}\right) \\
= {} & \frac{1}{\phi(q)} = \frac{1}{q-1} \quad \text{by Dirichlet's Theorem}
\end{aligned}
$$

$$
\begin{aligned}
P_2 := {} & \mathcal{P}\left(p \text{ prime} \;:\; a^{(p-1)/q} \equiv 1 \pmod{p}\right) \quad \text{for } a = b^k,\ 1 \le k \le p-1 \\
= {} & \mathcal{P}\left(p \text{ prime} \;:\; \frac{k(p-1)}{q} \equiv 0 \pmod{p-1}\right) \quad \text{as } (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}
\end{aligned}
$$

Artin's Heuristic Idea

Probabilities of the events:

$$
\begin{aligned}
P_1 := & \ \mathcal{P}\left(p \text{ prime } : \ p \equiv 1 \pmod q\right) \\
= & \ \mathcal{P}\left(p \text{ prime } : \ p \in \{aq+1\}_{a \in \mathbb{Z}}\right) \\
= & \ \frac{1}{\phi(q)} = \frac{1}{q-1} \quad \text{by Dirichlet's Theorem}
\end{aligned}
$$

$$
\begin{aligned}
P_2 := & \ \mathcal{P}\left(p \text{ prime } : \ a^{(p-1)/q} \equiv 1 \pmod p\right) \quad \text{for } a = b^k,\ 1 \le k \le p-1 \\
= & \ \mathcal{P}\left(p \text{ prime } : \ \frac{k(p-1)}{q} \equiv 0 \pmod{p-1}\right) \quad \text{as } (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \\
= & \ \mathcal{P}\left(p \text{ prime } : \ q|k\right)
\end{aligned}
$$

Artin's Heuristic Idea

Probabilities of the events:

$$\begin{aligned} P_1 :&= \mathcal{P}\left(p \text{ prime} \ : \ p \equiv 1 \pmod{q}\right) \\ &= \mathcal{P}\left(p \text{ prime} \ : \ p \in \{aq+1\}_{a\in\mathbb{Z}}\right) \\ &= \frac{1}{\phi(q)} = \frac{1}{q-1} \quad \text{by Dirichlet's Theorem} \end{aligned}$$

$$\begin{aligned} P_2 :&= \mathcal{P}\left(p \text{ prime} \ : \ a^{(p-1)/q} \equiv 1 \pmod{p}\right) \quad \text{for } a = b^k,\ 1 \le k \le p-1 \\ &= \mathcal{P}\left(p \text{ prime} \ : \ \frac{k(p-1)}{q} \equiv 0 \pmod{p-1}\right) \quad \text{as } (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \\ &= \mathcal{P}\left(p \text{ prime} \ : \ q|k\right) = \frac{(p-1)/q}{p-1} = \frac{1}{q} \end{aligned}$$

Artin's Heuristic Idea

Heuristic estimate

$$N_a(x) \sim \left[\prod_{q \text{ prime}} (1 - P_1 P_2) \right] \frac{x}{\log x}$$

Artin's Heuristic Idea

Heuristic estimate

$$N_a(x) \sim \left[\prod_{q \text{ prime}} (1 - P_1 P_2)\right] \frac{x}{\log x} = \left[\prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right)\right] \frac{x}{\log x}$$

Artin's Heuristic Idea

Heuristic estimate

$$N_a(x) \sim \left[\prod_{q \text{ prime}} (1 - P_1 P_2) \right] \frac{x}{\log x} = \left[\prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)} \right) \right] \frac{x}{\log x}$$

Value of a	$N_a(x)$	$A(a) \cdot \text{li}(x)$	% of Error
2	18701	17175	8.16
3	18761	17175	8.45
5	19699	17175	12.81
7	18687	17175	8.09
8	11225	17175	53.01
11	18772	17175	8.51

Here x is chosen to be the 50000-th prime, i.e, 611953.

Artin's Heuristic Idea

Problem with the heuristic argument

Artin's Heuristic Idea

Problem with the heuristic argument : Incorrect Assumption

The event $a^{(p-1)/q} \equiv 1 \pmod{p}$ and P_2 are independent of a.

Artin's Heuristic Idea

Problem with the heuristic argument : Incorrect Assumption

The event $a^{(p-1)/q} \equiv 1 \pmod p$ and P_2 are independent of a.

Why is this not true?

Artin's Heuristic Idea

Problem with the heuristic argument : Incorrect Assumption

The event $a^{(p-1)/q} \equiv 1 \pmod{p}$ and P_2 are independent of a.

Why is this not true?

Not *always* true, because if we choose an a such that $a = b^k$ for b being a primitive root of p, then a is *not necessarily* a primitive root of p.

Artin's Heuristic Idea

Problem with the heuristic argument : Incorrect Assumption

The event $a^{(p-1)/q} \equiv 1 \pmod{p}$ and P_2 are independent of a.

Why is this not true?

Not *always* true, because if we choose an a such that $a = b^k$ for b being a primitive root of p, then a is *not necessarily* a primitive root of p.

Example: If $a = 2^5 = 32$ in $(\mathbb{Z}/11\mathbb{Z})^*$, then $a^{10/q} \equiv 1 \pmod{11}$ is always true for $q = 5$, i.e, $P_2 = 1$.

Artin's Heuristic Idea

Problem with the heuristic argument : Incorrect Assumption

The event $a^{(p-1)/q} \equiv 1 \pmod{p}$ and P_2 are independent of a.

Why is this not true?

Not *always* true, because if we choose an a such that $a = b^k$ for b being a primitive root of p, then a is *not necessarily* a primitive root of p.

Example: If $a = 2^5 = 32$ in $(\mathbb{Z}/11\mathbb{Z})^*$, then $a^{10/q} \equiv 1 \pmod{11}$ is always true for $q = 5$, i.e, $P_2 = 1$.

Intuition:

Artin's Heuristic Idea

Problem with the heuristic argument : Incorrect Assumption

The event $a^{(p-1)/q} \equiv 1 \pmod{p}$ and P_2 are independent of a.

Why is this not true?

Not *always* true, because if we choose an a such that $a = b^k$ for b being a primitive root of p, then a is *not necessarily* a primitive root of p.

Example: If $a = 2^5 = 32$ in $(\mathbb{Z}/11\mathbb{Z})^*$, then $a^{10/q} \equiv 1 \pmod{11}$ is always true for $q = 5$, i.e, $P_2 = 1$.

Intuition:

"The density $A(a)$ does depend on a"

Artin's Heuristic Idea

Problem with the heuristic argument : Incorrect Assumption

The event $a^{(p-1)/q} \equiv 1 \pmod{p}$ and P_2 are independent of a.

Why is this not true?

Not *always* true, because if we choose an a such that $a = b^k$ for b being a primitive root of p, then a is *not necessarily* a primitive root of p.

Example: If $a = 2^5 = 32$ in $(\mathbb{Z}/11\mathbb{Z})^*$, then $a^{10/q} \equiv 1 \pmod{11}$ is always true for $q = 5$, i.e, $P_2 = 1$.

Intuition:

"The density $A(a)$ does depend on a"- D.H. Lehmer

Hooley's Conditional Proof

Theorem (Christopher Hooley, 1967)

Hooley's Conditional Proof

Theorem (Christopher Hooley, 1967)

Let us denote by $\tilde{a}$ the square-free part of a and h the largest integer such that a is a perfect h-th power.

Hooley's Conditional Proof

Theorem (Christopher Hooley, 1967)

Let us denote by $\tilde{a}$ the square-free part of a and h the largest integer such that a is a perfect h-th power.

Then for $\tilde{a} \not\equiv 1 \pmod 4$,

Hooley's Conditional Proof

Theorem (Christopher Hooley, 1967)

Let us denote by $\tilde{a}$ the square-free part of a and h the largest integer such that a is a perfect h-th power.

Then for $\tilde{a} \not\equiv 1 \pmod 4$, we have

$$N_a(x) = C(h)\frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right)$$

Hooley's Conditional Proof

Theorem (Christopher Hooley, 1967)

Let us denote by $\tilde{a}$ the square-free part of a and h the largest integer such that a is a perfect h-th power.

Then for $\tilde{a} \not\equiv 1 \pmod 4$, we have

$$N_a(x) = C(h)\frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right)$$

and for $\tilde{a} \equiv 1 \pmod 4$,

Hooley's Conditional Proof

Theorem (Christopher Hooley, 1967)

Let us denote by $\tilde{a}$ the square-free part of a and h the largest integer such that a is a perfect h-th power.

Then for $\tilde{a} \not\equiv 1 \pmod 4$, *we have*

$$N_a(x) = C(h)\frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right)$$

and for $\tilde{a} \equiv 1 \pmod 4$, *we have*

$$N_a(x) = C(h)\left(1 - \mu(|\tilde{a}|)\prod_{\substack{q|h \\ q|\tilde{a}}}\left(\frac{1}{q-2}\right)\prod_{\substack{q\nmid h \\ q|\tilde{a}}}\left(\frac{1}{q^2-q-1}\right)\right)\frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right)$$

Hooley's Conditional Proof

Where

$$C(h) := \prod_{q \mid h} \left(1 - \frac{1}{q-1}\right) \prod_{q \nmid h} \left(1 - \frac{1}{q(q-1)}\right)$$

Hooley's Conditional Proof

Where

$$C(h) := \prod_{q|h}\left(1 - \frac{1}{q-1}\right)\prod_{q\nmid h}\left(1 - \frac{1}{q(q-1)}\right)$$

Value of a	$N_a(x)$	Hooley's Estimate	% of Error
2	18701	18724	0.12
3	18761	18724	0.20
5	19699	19709	0.05
7	18687	18724	0.20
8	11225	11235	0.10
11	18772	18724	0.26

Here x is chosen to be the 50000-th prime, i.e, 611953.

The Main Problem

The Main Problem

Condition

The generalized Riemann hypothesis holds for the class of Dedekind zeta functions over Galois extensions of the type $\mathbb{Q}(\sqrt[k_1]{b}, \sqrt[k]{1})$, where $b \in \mathbb{Z}$, k is a square-free integer and $k_1|k$.

The Main Problem

Condition

The generalized Riemann hypothesis holds for the class of Dedekind zeta functions over Galois extensions of the type $\mathbb{Q}(\sqrt[k_1]{b}, \sqrt[k]{1})$, where $b \in \mathbb{Z}$, k is a square-free integer and $k_1 | k$.

- What if generalized Riemann hypothesis is FALSE ??

The Main Problem

Condition

The generalized Riemann hypothesis holds for the class of Dedekind zeta functions over Galois extensions of the type $\mathbb{Q}(\sqrt[k_1]{b}, \sqrt[k]{1})$, where $b \in \mathbb{Z}$, k is a square-free integer and $k_1 | k$.

- What if generalized Riemann hypothesis is FALSE ??
- Hooley's proof does not work anymore !!

The Main Problem

Condition

The generalized Riemann hypothesis holds for the class of Dedekind zeta functions over Galois extensions of the type $\mathbb{Q}(\sqrt[k_1]{b}, \sqrt[k]{1})$, where $b \in \mathbb{Z}$, k is a square-free integer and $k_1 | k$.

- What if generalized Riemann hypothesis is FALSE ??
- Hooley's proof does not work anymore !!
- Is there something one can do about it ?

The Main Problem

Condition

The generalized Riemann hypothesis holds for the class of Dedekind zeta functions over Galois extensions of the type $\mathbb{Q}(\sqrt[k_1]{b}, \sqrt[k]{1})$, where $b \in \mathbb{Z}$, k is a square-free integer and $k_1 | k$.

- What if generalized Riemann hypothesis is FALSE ??
- Hooley's proof does not work anymore !!
- Is there something one can do about it ?
- Figure out an unconditional proof !

Unconditional Proof of Artin's Conjecture

Gupta and Murty's Result

Theorem (Rajiv Gupta and M. Ram Murty, 1984)

Gupta and Murty's Result

Theorem (Rajiv Gupta and M. Ram Murty, 1984)

Let q, r and s denote three distinct primes.

Gupta and Murty's Result

Theorem (Rajiv Gupta and M. Ram Murty, 1984)

Let q, r and s denote three distinct primes. If we define the following set

$$S = \left\{ qs^2, q^3r^2, q^2r, r^3s^2, r^2s, q^2s^3, qr^3, q^3rs^2, rs^3, q^2r^3s, q^3s, qr^2s^3, qrs \right\}$$

Gupta and Murty's Result

Theorem (Rajiv Gupta and M. Ram Murty, 1984)

Let q, r and s denote three distinct primes. If we define the following set

$$S = \left\{ qs^2, q^3r^2, q^2r, r^3s^2, r^2s, q^2s^3, qr^3, q^3rs^2, rs^3, q^2r^3s, q^3s, qr^2s^3, qrs \right\}$$

then for some $a \in S$, there exists a $\delta > 0$ such that

Gupta and Murty's Result

Theorem (Rajiv Gupta and M. Ram Murty, 1984)

Let q, r and s denote three distinct primes. If we define the following set

$$S = \left\{ qs^2, q^3r^2, q^2r, r^3s^2, r^2s, q^2s^3, qr^3, q^3rs^2, rs^3, q^2r^3s, q^3s, qr^2s^3, qrs \right\}$$

then for some $a \in S$, there exists a $\delta > 0$ such that

$$N_a(x) \geq \frac{\delta x}{\log^2 x}$$

Gupta and Murty's Result

Theorem (Rajiv Gupta and M. Ram Murty, 1984)

Let q, r and s denote three distinct primes. If we define the following set

$$S = \left\{ qs^2, q^3r^2, q^2r, r^3s^2, r^2s, q^2s^3, qr^3, q^3rs^2, rs^3, q^2r^3s, q^3s, qr^2s^3, qrs \right\}$$

then for some $a \in S$, there exists a $\delta > 0$ such that

$$N_a(x) \geq \frac{\delta x}{\log^2 x}$$

Here,

$$N_a(x) \ = \ \#\{p \leq x \ : \ a \text{ is a primitive root of } p\}$$

Sketch of the Proof

Sketch of the Proof

Notation: $(q, r, s)^u := q^{u_1} r^{u_2} s^{u_3}$ where $u := (u_1, u_2, u_3) \in \mathbb{Z}^3$ [non-negative].

Sketch of the Proof

Notation: $(q, r, s)^u := q^{u_1} r^{u_2} s^{u_3}$ where $u := (u_1, u_2, u_3) \in \mathbb{Z}^3$ [non-negative].

Vector Space Argument

Sketch of the Proof

Notation: $(q, r, s)^u := q^{u_1} r^{u_2} s^{u_3}$ where $u := (u_1, u_2, u_3) \in \mathbb{Z}^3$ [non-negative].

Vector Space Argument

Let us construct a set S_1 of 3-tuples u satisfying

Sketch of the Proof

Notation: $(q, r, s)^u := q^{u_1} r^{u_2} s^{u_3}$ where $u := (u_1, u_2, u_3) \in \mathbb{Z}^3$ [non-negative].

Vector Space Argument

Let us construct a set S_1 of 3-tuples u satisfying

1. For any $u \in S_1$, $u \not\equiv (0, 0, 0) \pmod 2$

Sketch of the Proof

Notation: $(q, r, s)^u := q^{u_1} r^{u_2} s^{u_3}$ where $u := (u_1, u_2, u_3) \in \mathbb{Z}^3$ [non-negative].

Vector Space Argument

Let us construct a set S_1 of 3-tuples u satisfying

1. For any $u \in S_1$, $u \not\equiv (0, 0, 0) \pmod 2$
2. For each $u \in S_1$, $\exists$ at most one $v \in S_1 \ : \ v \neq u$ and $v \equiv u \pmod 2$

Sketch of the Proof

Notation: $(q, r, s)^u := q^{u_1} r^{u_2} s^{u_3}$ where $u := (u_1, u_2, u_3) \in \mathbb{Z}^3$ [non-negative].

Vector Space Argument

Let us construct a set S_1 of 3-tuples u satisfying

1. For any $u \in S_1$, $u \not\equiv (0, 0, 0) \pmod 2$
2. For each $u \in S_1$, $\exists$ at most one $v \in S_1 \;:\; v \neq u$ and $v \equiv u \pmod 2$
3. For each 2-dimensional subspace $V \subset \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^3$, any three elements of $S_V = \{u \in S_1 \;:\; u \not\equiv v \pmod 2 \;\forall\, v \in V\}$ are linearly independent

Sketch of the Proof

Notation: $(q, r, s)^u := q^{u_1} r^{u_2} s^{u_3}$ where $u := (u_1, u_2, u_3) \in \mathbb{Z}^3$ [non-negative].

Vector Space Argument

Let us construct a set S_1 of 3-tuples u satisfying

1. For any $u \in S_1$, $u \not\equiv (0, 0, 0) \pmod 2$
2. For each $u \in S_1$, $\exists$ at most one $v \in S_1 \;:\; v \neq u$ and $v \equiv u \pmod 2$
3. For each 2-dimensional subspace $V \subset \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^3$, any three elements of $S_V = \{u \in S_1 \;:\; u \not\equiv v \pmod 2 \;\forall\, v \in V\}$ are linearly independent

The Set S_1

Sketch of the Proof

Notation: $(q, r, s)^u := q^{u_1} r^{u_2} s^{u_3}$ where $u := (u_1, u_2, u_3) \in \mathbb{Z}^3$ [non-negative].

Vector Space Argument

Let us construct a set S_1 of 3-tuples u satisfying

1. For any $u \in S_1$, $u \not\equiv (0,0,0) \pmod 2$
2. For each $u \in S_1$, $\exists$ at most one $v \in S_1 \;:\; v \neq u$ and $v \equiv u \pmod 2$
3. For each 2-dimensional subspace $V \subset \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^3$, any three elements of $S_V = \{u \in S_1 \;:\; u \not\equiv v \pmod 2 \; \forall \, v \in V\}$ are linearly independent

The Set S_1

$$S_1 = \{(1,0,2), (3,2,0), (2,1,0), (0,3,2), (0,2,1), (2,0,3), (1,3,0), (3,1,2), (0,1,3), (2,3,1), (3,0,1), (1,2,3), (1,1,1)\}$$

Sketch of the Proof

Lemma (Gupta and Murty)

If $\mathbb{F}_p^* = \langle q, r, s \rangle$, then for some $u \in S_1$, $(q, r, s)^u$ is a primitive root modulo p.

Sketch of the Proof

Lemma (Gupta and Murty)

If $\mathbb{F}_p^* = \langle q, r, s \rangle$, then for some $u \in S_1$, $(q, r, s)^u$ is a primitive root modulo p.

Lemma (Gupta and Murty)

There exists a $\delta > 0$ such that

$$\#\{p \leq x \ : \ \mathbb{F}_p^* = \langle q, r, s \rangle\} \ \geq \ \frac{\delta x}{\log^2 x}$$

Sketch of the Proof

Lemma (Gupta and Murty)

If $\mathbb{F}_p^* = \langle q, r, s \rangle$, then for some $u \in S_1$, $(q, r, s)^u$ is a primitive root modulo p.

Lemma (Gupta and Murty)

There exists a $\delta > 0$ such that

$$\#\{p \leq x \ : \ \mathbb{F}_p^* = \langle q, r, s \rangle\} \ \geq \ \frac{\delta x}{\log^2 x}$$

So, we have at least one element satisfying the result in $S = (q, r, s)^u$ for u in $S_1 = \{(1, 0, 2), (3, 2, 0), (2, 1, 0), (0, 3, 2), (0, 2, 1), (2, 0, 3), (1, 3, 0), (3, 1, 2), (0, 1, 3), (2, 3, 1), (3, 0, 1), (1, 2, 3), (1, 1, 1)\}$,

Sketch of the Proof

Lemma (Gupta and Murty)

If $\mathbb{F}_p^* = \langle q, r, s\rangle$, then for some $u \in S_1$, $(q, r, s)^u$ is a primitive root modulo p.

Lemma (Gupta and Murty)

There exists a $\delta > 0$ such that

$$\#\{p \le x \ : \ \mathbb{F}_p^* = \langle q, r, s\rangle\} \ \ge \ \frac{\delta x}{\log^2 x}$$

So, we have at least one element satisfying the result in $S = (q, r, s)^u$ for u in $S_1 = \{(1,0,2), (3,2,0), (2,1,0), (0,3,2), (0,2,1), (2,0,3), (1,3,0), (3,1,2), (0,1,3), (2,3,1), (3,0,1), (1,2,3), (1,1,1)\}$, i.e, in the set

$$S = \left\{qs^2, q^3r^2, q^2r, r^3s^2, r^2s, q^2s^3, qr^3, q^3rs^2, rs^3, q^2r^3s, q^3s, qr^2s^3, qrs\right\}$$

Sketch of the Proof

Lemma (Gupta and Murty)

If $\mathbb{F}_p^* = \langle q, r, s \rangle$, then for some $u \in S_1$, $(q, r, s)^u$ is a primitive root modulo p.

Lemma (Gupta and Murty)

There exists a $\delta > 0$ such that

$$\#\{p \leq x \ : \ \mathbb{F}_p^* = \langle q, r, s \rangle\} \ \geq \ \frac{\delta x}{\log^2 x}$$

So, we have at least one element satisfying the result in $S = (q, r, s)^u$ for u in $S_1 = \{(1,0,2), (3,2,0), (2,1,0), (0,3,2), (0,2,1), (2,0,3), (1,3,0), (3,1,2), (0,1,3), (2,3,1), (3,0,1), (1,2,3), (1,1,1)\}$, i.e, in the set

$$S = \left\{qs^2, q^3r^2, q^2r, r^3s^2, r^2s, q^2s^3, qr^3, q^3rs^2, rs^3, q^2r^3s, q^3s, qr^2s^3, qrs\right\}$$

Important: Both the lemmas are true provided that $(p-1)$ has at most 3 odd prime divisors, all sufficiently large.

Backbone of the Proof

Backbone of the Proof

Lemma (Gupta and Murty)

Let us fix a prime q and a constant $\epsilon \in \left(0, \frac{1}{4}\right)$.

Backbone of the Proof

Lemma (Gupta and Murty)

Let us fix a prime q and a constant $\epsilon \in \left(0, \frac{1}{4}\right)$. *If* $\alpha = \frac{1}{4} + \epsilon$, *then there exists a constant* $c > 0$ *such that*

Backbone of the Proof

Lemma (Gupta and Murty)

Let us fix a prime q and a constant $\epsilon \in \left(0, \frac{1}{4}\right)$. If $\alpha = \frac{1}{4} + \epsilon$, then there exists a constant $c > 0$ such that

$$\#\left\{p \leq x \;:\; \left(\frac{q}{p}\right) = -1,\ t \text{ prime } \& \ t | (p-1) \Rightarrow t = 2 \text{ or } t > x^{\alpha}\right\} \geq \frac{cx}{\log^2 x}$$

Backbone of the Proof

Lemma (Gupta and Murty)

Let us fix a prime q and a constant $\epsilon \in \left(0, \frac{1}{4}\right)$. If $\alpha = \frac{1}{4} + \epsilon$, then there exists a constant $c > 0$ such that

$$\#\left\{p \leq x \,:\, \left(\frac{q}{p}\right) = -1,\ t \text{ prime } \&\ t|(p-1) \Rightarrow t = 2 \text{ or } t > x^{\alpha}\right\} \geq \frac{cx}{\log^2 x}$$

Stretching the Backbone

Backbone of the Proof

Lemma (Gupta and Murty)

Let us fix a prime q and a constant $\epsilon \in \left(0, \frac{1}{4}\right)$. If $\alpha = \frac{1}{4} + \epsilon$, then there exists a constant $c > 0$ such that

$$\#\left\{p \leq x \; : \; \left(\frac{q}{p}\right) = -1, \; t \text{ prime } \& \; t|(p-1) \Rightarrow t = 2 \text{ or } t > x^{\alpha}\right\} \geq \frac{cx}{\log^2 x}$$

Stretching the Backbone

- Lemma with $\alpha = \frac{1}{4} + \epsilon$: a result in Linear Sieve by H. Iwaniec.

Backbone of the Proof

Lemma (Gupta and Murty)

Let us fix a prime q and a constant $\epsilon \in \left(0, \frac{1}{4}\right)$. If $\alpha = \frac{1}{4} + \epsilon$, then there exists a constant $c > 0$ such that

$$\#\left\{p \leq x \;:\; \left(\frac{q}{p}\right) = -1,\ t \text{ prime } \&\ t|(p-1) \Rightarrow t = 2 \text{ or } t > x^{\alpha}\right\} \geq \frac{cx}{\log^2 x}$$

Stretching the Backbone

- Lemma with $\alpha = \frac{1}{4} + \epsilon$: a result in Linear Sieve by H. Iwaniec.
- Lemma with $\alpha = \frac{1}{4} - \epsilon$: another result by Iwaniec and the Bombieri-Vinogradov theorem.

Backbone of the Proof

Lemma (Gupta and Murty)

Let us fix a prime q and a constant $\epsilon \in \left(0, \frac{1}{4}\right)$. *If* $\alpha = \frac{1}{4} + \epsilon$, *then there exists a constant* $c > 0$ *such that*

$$\#\left\{p \leq x \;:\; \left(\frac{q}{p}\right) = -1,\ t \textit{ prime } \& \ t|(p-1) \Rightarrow t = 2 \textit{ or } t > x^{\alpha}\right\} \geq \frac{cx}{\log^2 x}$$

Stretching the Backbone

- Lemma with $\alpha = \frac{1}{4} + \epsilon$: a result in Linear Sieve by H. Iwaniec.
- Lemma with $\alpha = \frac{1}{4} - \epsilon$: another result by Iwaniec and the Bombieri-Vinogradov theorem.
- Lemma with $\alpha = \frac{1}{6} - \epsilon$: lower bound Selberg sieve along with the Bombieri-Vinogradov theorem.

Backbone of the Proof

Lemma (Gupta and Murty)

Let us fix a prime q and a constant $\epsilon \in \left(0, \frac{1}{4}\right)$. If $\alpha = \frac{1}{4} + \epsilon$, then there exists a constant $c > 0$ such that

$$\#\left\{p \leq x \ : \ \left(\frac{q}{p}\right) = -1,\ t \text{ prime } \&\ t|(p-1) \Rightarrow t = 2 \text{ or } t > x^{\alpha}\right\} \geq \frac{cx}{\log^2 x}$$

Stretching the Backbone

- Lemma with $\alpha = \frac{1}{4} + \epsilon$: a result in Linear Sieve by H. Iwaniec.
- Lemma with $\alpha = \frac{1}{4} - \epsilon$: another result by Iwaniec and the Bombieri-Vinogradov theorem.
- Lemma with $\alpha = \frac{1}{6} - \epsilon$: lower bound Selberg sieve along with the Bombieri-Vinogradov theorem.

Backbone of the Proof

Lemma (Gupta and Murty)

Let us fix a prime q and a constant $\epsilon \in \left(0, \frac{1}{4}\right)$. If $\alpha = \frac{1}{4} + \epsilon$, then there exists a constant $c > 0$ such that

$$\#\left\{p \leq x \ : \ \left(\frac{q}{p}\right) = -1, \ t \text{ prime } \& \ t|(p-1) \Rightarrow t = 2 \text{ or } t > x^{\alpha}\right\} \geq \frac{cx}{\log^2 x}$$

Stretching the Backbone

- Lemma with $\alpha = \frac{1}{4} + \epsilon$: a result in Linear Sieve by H. Iwaniec.
- Lemma with $\alpha = \frac{1}{4} - \epsilon$: another result by Iwaniec and the Bombieri-Vinogradov theorem.
- Lemma with $\alpha = \frac{1}{6} - \epsilon$: lower bound Selberg sieve along with the Bombieri-Vinogradov theorem.

Crucial Observation: The size of the set S in Gupta and Murty's theorem decreases if the previous lemma is strengthened by increasing the value of α.

Heath-Brown's (Improved) Result

Theorem (Heath-Brown, 1986)

Heath-Brown's (Improved) Result

Theorem (Heath-Brown, 1986)

Let us define the following set of multiplicatively independent non-zero integers

$$\tilde{S} = \{q, r, s \ : \ q^e r^f s^g = 1 \Rightarrow e = f = g = 0 \ \ \textit{for } e, f, g \in \mathbb{Z}\}$$

Heath-Brown's (Improved) Result

Theorem (Heath-Brown, 1986)

Let us define the following set of multiplicatively independent non-zero integers

$$\tilde{S} = \{q, r, s \ : \ q^e r^f s^g = 1 \Rightarrow e = f = g = 0 \ \ \textit{for } e, f, g \in \mathbb{Z}\}$$

Now, if we suppose that none of $q, r, s, -3qr, -3qs, -3rs, qrs$ *is a square*

Heath-Brown's (Improved) Result

Theorem (Heath-Brown, 1986)

Let us define the following set of multiplicatively independent non-zero integers

$$\tilde{S} = \{q, r, s \ : \ q^e r^f s^g = 1 \Rightarrow e = f = g = 0 \ \ \textit{for } e, f, g \in \mathbb{Z}\}$$

Now, if we suppose that none of $q, r, s, -3qr, -3qs, -3rs, qrs$ *is a square, then at least for one* $a \in \tilde{S}$

Heath-Brown's (Improved) Result

Theorem (Heath-Brown, 1986)

Let us define the following set of multiplicatively independent non-zero integers

$$\tilde{S} = \{q, r, s \ : \ q^e r^f s^g = 1 \Rightarrow e = f = g = 0 \ \text{ for } e, f, g \in \mathbb{Z}\}$$

Now, if we suppose that none of $q, r, s, -3qr, -3qs, -3rs, qrs$ *is a square, then at least for one* $a \in \tilde{S}$*, we have*

$$N_a(x) \gg \frac{x}{\log^2 x}$$

Heath-Brown's (Improved) Result

Theorem (Heath-Brown, 1986)

Let us define the following set of multiplicatively independent non-zero integers

$$\tilde{S} = \{q, r, s \ : \ q^e r^f s^g = 1 \Rightarrow e = f = g = 0 \ \text{ for } e, f, g \in \mathbb{Z}\}$$

Now, if we suppose that none of $q, r, s, -3qr, -3qs, -3rs, qrs$ *is a square, then at least for one* $a \in \tilde{S}$*, we have*

$$N_a(x) \gg \frac{x}{\log^2 x}$$

Corollary (Heath-Brown)

There are at most two primes for which Artin's conjecture does not hold.

Heath-Brown's (Improved) Result

Theorem (Heath-Brown, 1986)

Let us define the following set of multiplicatively independent non-zero integers

$$\tilde{S} = \{q, r, s \ : \ q^e r^f s^g = 1 \Rightarrow e = f = g = 0 \ \ \textit{for } e, f, g \in \mathbb{Z}\}$$

Now, if we suppose that none of $q, r, s, -3qr, -3qs, -3rs, qrs$ *is a square, then at least for one* $a \in \tilde{S}$*, we have*

$$N_a(x) \gg \frac{x}{\log^2 x}$$

Corollary (Heath-Brown)

There are at most two primes for which Artin's conjecture does not hold.

Corollary (Heath-Brown)

There are at most three square free integers greater than 1 for which Artin's conjecture does not hold.

A couple of open questions

A couple of open questions

Questions

For any problem in number theory

A couple of open questions

Questions

For any problem in number theory

- What if the problem is too hard in $\mathbb{Z}$? [That's frustrating !]

A couple of open questions

Questions

For any problem in number theory

- What if the problem is too hard in $\mathbb{Z}$? [That's frustrating !]
- What if it is trivial in $\mathbb{Z}$? [Now, that's boring]

A couple of open questions

Questions

For any problem in number theory

- What if the problem is too hard in $\mathbb{Z}$? [That's frustrating !]
- What if it is trivial in $\mathbb{Z}$? [Now, that's boring]

A couple of open questions

Questions

For any problem in number theory

- What if the problem is too hard in $\mathbb{Z}$? [That's frustrating !]
- What if it is trivial in $\mathbb{Z}$? [Now, that's boring]

The most accepted solution

- Try to solve the problem in a different setting.

A couple of open questions

Questions

For any problem in number theory

- What if the problem is too hard in $\mathbb{Z}$? [That's frustrating !]
- What if it is trivial in $\mathbb{Z}$? [Now, that's boring]

The most accepted solution

- Try to solve the problem in a different setting.
- Try to formulate and solve an analogous case.

A couple of open questions

Questions

For any problem in number theory

- What if the problem is too hard in $\mathbb{Z}$? [That's frustrating !]
- What if it is trivial in $\mathbb{Z}$? [Now, that's boring]

The most accepted solution

- Try to solve the problem in a different setting.
- Try to formulate and solve an analogous case.
- And try to carry the information back to solve the original problem.

Elliptic Curve analogue of Artin's Conjecture

A brief introduction

An elliptic curve over a field $\mathbb{K}$ is a nonsingular cubic curve (genus 1) in two variables, having $\mathbb{K}$-rational points.

A brief introduction

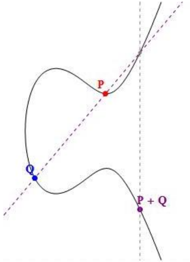
An elliptic curve over a field $\mathbb{K}$ is a nonsingular cubic curve (genus 1) in two variables, having $\mathbb{K}$-rational points.

A general elliptic curve over $\mathbb{K}$ with char $\mathbb{K} \neq 2, 3$ can be written in the Weierstrass form $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{K}$.

A brief introduction

An elliptic curve over a field $\mathbb{K}$ is a nonsingular cubic curve (genus 1) in two variables, having $\mathbb{K}$-rational points.

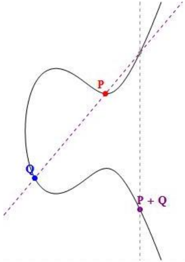
A general elliptic curve over $\mathbb{K}$ with char $\mathbb{K} \neq 2, 3$ can be written in the Weierstrass form $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{K}$.



A brief introduction

An elliptic curve over a field $\mathbb{K}$ is a nonsingular cubic curve (genus 1) in two variables, having $\mathbb{K}$-rational points.

A general elliptic curve over $\mathbb{K}$ with char $\mathbb{K} \neq 2, 3$ can be written in the Weierstrass form $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{K}$.



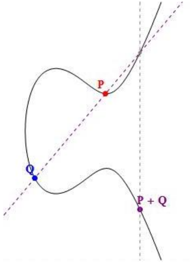
Some useful facts

- Discriminant of E: $\Delta_E = -16(4a^3 + 27b^2) \neq 0$ for nonsingular curve.

A brief introduction

An elliptic curve over a field $\mathbb{K}$ is a nonsingular cubic curve (genus 1) in two variables, having $\mathbb{K}$-rational points.

A general elliptic curve over $\mathbb{K}$ with char $\mathbb{K} \neq 2, 3$ can be written in the Weierstrass form $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{K}$.



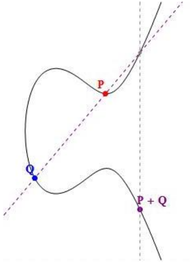
Some useful facts

- Discriminant of E: $\Delta_E = -16(4a^3 + 27b^2) \neq 0$ for nonsingular curve.
- We will choose $\mathbb{K} = \mathbb{Q}$, i.e, $E = E(\mathbb{Q})$ for this talk.

A brief introduction

An elliptic curve over a field $\mathbb{K}$ is a nonsingular cubic curve (genus 1) in two variables, having $\mathbb{K}$-rational points.

A general elliptic curve over $\mathbb{K}$ with char $\mathbb{K} \neq 2, 3$ can be written in the Weierstrass form $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{K}$.



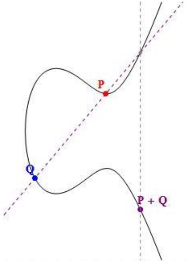
Some useful facts

- Discriminant of E: $\Delta_E = -16(4a^3 + 27b^2) \neq 0$ for nonsingular curve.
- We will choose $\mathbb{K} = \mathbb{Q}$, i.e, $E = E(\mathbb{Q})$ for this talk.
- $E(\mathbb{Q})$ is an additive group with the identity O, a projective point at infinity.

A brief introduction

An elliptic curve over a field $\mathbb{K}$ is a nonsingular cubic curve (genus 1) in two variables, having $\mathbb{K}$-rational points.

A general elliptic curve over $\mathbb{K}$ with char $\mathbb{K} \neq 2, 3$ can be written in the Weierstrass form $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{K}$.



Some useful facts

- Discriminant of E: $\Delta_E = -16(4a^3 + 27b^2) \neq 0$ for nonsingular curve.
- We will choose $\mathbb{K} = \mathbb{Q}$, i.e, $E = E(\mathbb{Q})$ for this talk.
- $E(\mathbb{Q})$ is an additive group with the identity O, a projective point at infinity.
- If a prime $p \nmid \Delta_E$, we can have a good (nonsingular) reduction of E modulo p to get $\overline{E}(\mathbb{F}_p)$ which also has an additive group structure.

Primitive Point

Primitive Point

Definition (Primitive Point)

Given an elliptic curve $E(\mathbb{Q})$ defined over the rationals and a prime p, let the reduction of the elliptic curve modulo p be denoted as $\overline{E}(\mathbb{F}_p)$.

Primitive Point

Definition (Primitive Point)

Given an elliptic curve $E(\mathbb{Q})$ defined over the rationals and a prime p, let the reduction of the elliptic curve modulo p be denoted as $\overline{E}(\mathbb{F}_p)$.

Then, a rational point $a \in E(\mathbb{Q})$ is said to be a *primitive point* of the curve modulo p

Primitive Point

Definition (Primitive Point)

Given an elliptic curve $E(\mathbb{Q})$ defined over the rationals and a prime p, let the reduction of the elliptic curve modulo p be denoted as $\overline{E}(\mathbb{F}_p)$.

Then, a rational point $a \in E(\mathbb{Q})$ is said to be a *primitive point* of the curve modulo p if $\overline{a}$, the reduction of a modulo p generates $\overline{E}(\mathbb{F}_p)$.

Primitive Point

Definition (Primitive Point)

Given an elliptic curve $E(\mathbb{Q})$ defined over the rationals and a prime p, let the reduction of the elliptic curve modulo p be denoted as $\overline{E}(\mathbb{F}_p)$.

Then, a rational point $a \in E(\mathbb{Q})$ is said to be a *primitive point* of the curve modulo p if $\overline{a}$, the reduction of a modulo p generates $\overline{E}(\mathbb{F}_p)$.

Put in mathematical notation, a rational point $a \in E(\mathbb{Q})$ is a *primitive point* of the curve modulo p if

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle$$

where $\overline{a}$ is the reduction of a modulo p.

The Analogous Conjecture

The Analogous Conjecture

The analogous question

If we fix a rational point a on an elliptic curve, then, for how many primes p will $\overline{a}$ generate $\overline{E}(\mathbb{F}_p)$?

The Analogous Conjecture

The analogous question

If we fix a rational point a on an elliptic curve, then, for how many primes p will $\overline{a}$ generate $\overline{E}(\mathbb{F}_p)$?

Conjecture (Lang and Trotter, 1977)

If we consider an elliptic curve $E(\mathbb{Q})$ defined over the rationals and a rational point $a \in E(\mathbb{Q})$ of infinite order

The Analogous Conjecture

The analogous question

If we fix a rational point a on an elliptic curve, then, for how many primes p will $\overline{a}$ generate $\overline{E}(\mathbb{F}_p)$?

Conjecture (Lang and Trotter, 1977)

If we consider an elliptic curve $E(\mathbb{Q})$ defined over the rationals and a rational point $a \in E(\mathbb{Q})$ of infinite order, then a will be a primitive point of $\overline{E}(\mathbb{F}_p)$ for infinitely many primes p.

Result 1 (Gupta and Murty)

Result 1 (Gupta and Murty)

Theorem (Gupta and Murty, 1986)

Let $E(\mathbb{Q})$ be an elliptic curve defined over the rationals with complex multiplication by $\mathcal{O}_{\mathbb{K}}$ (entire ring of integers in an imaginary quadratic extension $\mathbb{K}$ over $\mathbb{Q}$) and let a be a rational point of infinite order.

Result 1 (Gupta and Murty)

Theorem (Gupta and Murty, 1986)

Let $E(\mathbb{Q})$ be an elliptic curve defined over the rationals with complex multiplication by $\mathcal{O}_{\mathbb{K}}$ (entire ring of integers in an imaginary quadratic extension $\mathbb{K}$ over $\mathbb{Q}$) and let a be a rational point of infinite order. If we define

$$N_a^*(x) = \#\{p \leq x \ : \ p \nmid a,\ p \text{ splits completely in } \mathbb{K},\ \langle \overline{a} \rangle = \overline{E}(\mathbb{F}_p)\}$$

Result 1 (Gupta and Murty)

Theorem (Gupta and Murty, 1986)

Let $E(\mathbb{Q})$ be an elliptic curve defined over the rationals with complex multiplication by $\mathcal{O}_{\mathbb{K}}$ (entire ring of integers in an imaginary quadratic extension $\mathbb{K}$ over $\mathbb{Q}$) and let a be a rational point of infinite order. If we define

$$N_a^*(x) = \#\{p \leq x \ : \ p \nmid a, \ p \text{ splits completely in } \mathbb{K}, \ \langle \overline{a} \rangle = \overline{E}(\mathbb{F}_p)\}$$

then under the assumption of generalized Riemann hypothesis,

Result 1 (Gupta and Murty)

Theorem (Gupta and Murty, 1986)

Let $E(\mathbb{Q})$ be an elliptic curve defined over the rationals with complex multiplication by $\mathcal{O}_{\mathbb{K}}$ (entire ring of integers in an imaginary quadratic extension $\mathbb{K}$ over $\mathbb{Q}$) and let a be a rational point of infinite order. If we define

$$N_a^*(x) = \#\{p \leq x \ : \ p \nmid a, \ p \text{ splits completely in } \mathbb{K}, \ \langle \overline{a} \rangle = \overline{E}(\mathbb{F}_p)\}$$

then under the assumption of generalized Riemann hypothesis, we obtain the following as $x \to \infty$:

$$N_a^*(x) \ = \ C_E(a)\frac{x}{\log x} \ + \ O\left(\frac{x \log \log x}{\log^2 x}\right)$$

Main idea behind the proof

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle$$

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \;\Leftrightarrow\; i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle\right]$$

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \iff i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle \right] = 1$$

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \iff i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle \right] = 1 \iff q \nmid i(p) \ \forall \text{ primes } q$$

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \;\Leftrightarrow\; i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle\right] = 1 \;\Leftrightarrow\; q \nmid i(p) \;\forall \text{ primes } q$$

Define: $\mathbb{K}_q = \mathbb{K}(E[q])$

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \;\Leftrightarrow\; i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle\right] = 1 \;\Leftrightarrow\; q \nmid i(p)\ \forall \text{ primes } q$$

Define: $\mathbb{K}_q = \mathbb{K}(E[q])$ and $\mathbb{L}_\mathfrak{q} = \mathbb{K}(E[\mathfrak{q}], \mathfrak{q}^{-1}a)$

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \;\Leftrightarrow\; i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle\right] = 1 \;\Leftrightarrow\; q \nmid i(p) \;\forall \text{ primes } q$$

Define: $\mathbb{K}_q = \mathbb{K}(E[q])$ and $\mathbb{L}_{\mathfrak{q}} = \mathbb{K}(E[\mathfrak{q}], \mathfrak{q}^{-1}a)$, where $E[q]$: q-division points

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \bar{a} \rangle \iff i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \bar{a} \rangle\right] = 1 \iff q \nmid i(p) \; \forall \text{ primes } q$$

Define: $\mathbb{K}_q = \mathbb{K}(E[q])$ and $\mathbb{L}_\mathfrak{q} = \mathbb{K}(E[\mathfrak{q}], \mathfrak{q}^{-1}a)$, where $E[q]$: q-division points

Lemma (Modified Index Divisibility Criteria)

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \;\Leftrightarrow\; i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle\right] = 1 \;\Leftrightarrow\; q \nmid i(p) \;\forall \text{ primes } q$$

Define: $\mathbb{K}_q = \mathbb{K}(E[q])$ and $\mathbb{L}_{\mathfrak{q}} = \mathbb{K}(E[\mathfrak{q}], \mathfrak{q}^{-1}a)$, where $E[q]$: q-division points

Lemma (Modified Index Divisibility Criteria)

Suppose that p splits in $\mathbb{K}$ as $p = \pi_p \overline{\pi_p}$

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \Leftrightarrow i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle\right] = 1 \Leftrightarrow q \nmid i(p) \; \forall \text{ primes } q$$

Define: $\mathbb{K}_q = \mathbb{K}(E[q])$ and $\mathbb{L}_\mathfrak{q} = \mathbb{K}(E[\mathfrak{q}], \mathfrak{q}^{-1}a)$, where $E[q]$: q-division points

Lemma (Modified Index Divisibility Criteria)

Suppose that p splits in $\mathbb{K}$ as $p = \pi_p \overline{\pi_p}$ and $p \nmid q\Delta_E$.

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \;\Leftrightarrow\; i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle\right] = 1 \;\Leftrightarrow\; q \nmid i(p)\ \forall \text{ primes } q$$

Define: $\mathbb{K}_q = \mathbb{K}(E[q])$ and $\mathbb{L}_\mathfrak{q} = \mathbb{K}(E[\mathfrak{q}], \mathfrak{q}^{-1}a)$, where $E[q]$: q-division points

Lemma (Modified Index Divisibility Criteria)

Suppose that p splits in $\mathbb{K}$ as $p = \pi_p \overline{\pi_p}$ and $p \nmid q\Delta_E$. Then

1. *If q is inert in $\mathbb{K}$*

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \;\Leftrightarrow\; i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle\right] = 1 \;\Leftrightarrow\; q \nmid i(p) \;\forall \text{ primes } q$$

Define: $\mathbb{K}_q = \mathbb{K}(E[q])$ and $\mathbb{L}_\mathfrak{q} = \mathbb{K}(E[\mathfrak{q}], \mathfrak{q}^{-1}a)$, where $E[q]$: q-division points

Lemma (Modified Index Divisibility Criteria)

Suppose that p splits in $\mathbb{K}$ as $p = \pi_p \overline{\pi_p}$ and $p \nmid q\Delta_E$. Then

1. *If q is inert in $\mathbb{K}$, then $q | i(p)$ if and only if p splits completely in $\mathbb{K}_q$.*

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \;\Leftrightarrow\; i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle\right] = 1 \;\Leftrightarrow\; q \nmid i(p) \;\forall \text{ primes } q$$

Define: $\mathbb{K}_q = \mathbb{K}(E[q])$ and $\mathbb{L}_{\mathfrak{q}} = \mathbb{K}(E[\mathfrak{q}], \mathfrak{q}^{-1}a)$, where $E[q]$: q-division points

Lemma (Modified Index Divisibility Criteria)

Suppose that p splits in $\mathbb{K}$ as $p = \pi_p \overline{\pi_p}$ and $p \nmid q\Delta_E$. Then

1. *If q is inert in $\mathbb{K}$, then $q | i(p)$ if and only if p splits completely in $\mathbb{K}_q$.*
2. *If q ramifies or splits in $\mathbb{K}$ as $q = \mathfrak{q}_1\mathfrak{q}_2$*

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \;\Leftrightarrow\; i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle\right] = 1 \;\Leftrightarrow\; q \nmid i(p) \;\forall \text{ primes } q$$

Define: $\mathbb{K}_q = \mathbb{K}(E[q])$ and $\mathbb{L}_{\mathfrak{q}} = \mathbb{K}(E[\mathfrak{q}], \mathfrak{q}^{-1}a)$, where $E[q]$: q-division points

Lemma (Modified Index Divisibility Criteria)

Suppose that p splits in $\mathbb{K}$ as $p = \pi_p \overline{\pi_p}$ and $p \nmid q\Delta_E$. Then

1. *If q is inert in $\mathbb{K}$, then $q | i(p)$ if and only if p splits completely in $\mathbb{K}_q$.*
2. *If q ramifies or splits in $\mathbb{K}$ as $q = \mathfrak{q}_1\mathfrak{q}_2$, then $q | i(p)$ if and only if (π_p) splits completely in $\mathbb{L}_{\mathfrak{q}_1}$ or $\mathbb{L}_{\mathfrak{q}_2}$ or $\mathbb{K}_q$.*

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \Leftrightarrow i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle\right] = 1 \Leftrightarrow q \nmid i(p) \ \forall \text{ primes } q$$

Define: $\mathbb{K}_q = \mathbb{K}(E[q])$ and $\mathbb{L}_{\mathfrak{q}} = \mathbb{K}(E[\mathfrak{q}], \mathfrak{q}^{-1}a)$, where $E[q]$: q-division points

Lemma (Modified Index Divisibility Criteria)

Suppose that p splits in $\mathbb{K}$ as $p = \pi_p \overline{\pi_p}$ and $p \nmid q\Delta_E$. Then

1. *If q is inert in $\mathbb{K}$, then $q | i(p)$ if and only if p splits completely in $\mathbb{K}_q$.*
2. *If q ramifies or splits in $\mathbb{K}$ as $q = \mathfrak{q}_1\mathfrak{q}_2$, then $q | i(p)$ if and only if (π_p) splits completely in $\mathbb{L}_{\mathfrak{q}_1}$ or $\mathbb{L}_{\mathfrak{q}_2}$ or $\mathbb{K}_q$.*

Goal:

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \;\Leftrightarrow\; i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle\right] = 1 \;\Leftrightarrow\; q \nmid i(p)\ \forall \text{ primes } q$$

Define: $\mathbb{K}_q = \mathbb{K}(E[q])$ and $\mathbb{L}_{\mathfrak{q}} = \mathbb{K}(E[\mathfrak{q}], \mathfrak{q}^{-1}a)$, where $E[q]$: q-division points

Lemma (Modified Index Divisibility Criteria)

Suppose that p splits in $\mathbb{K}$ as $p = \pi_p \overline{\pi_p}$ and $p \nmid q\Delta_E$. Then

1. *If q is inert in $\mathbb{K}$, then $q | i(p)$ if and only if p splits completely in $\mathbb{K}_q$.*
2. *If q ramifies or splits in $\mathbb{K}$ as $q = \mathfrak{q}_1\mathfrak{q}_2$, then $q | i(p)$ if and only if (π_p) splits completely in $\mathbb{L}_{\mathfrak{q}_1}$ or $\mathbb{L}_{\mathfrak{q}_2}$ or $\mathbb{K}_q$.*

Goal: Find the number of primes p satisfying $q \nmid i(p)$ $\forall$ primes q.

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \Leftrightarrow i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle\right] = 1 \Leftrightarrow q \nmid i(p) \; \forall \text{ primes } q$$

Define: $\mathbb{K}_q = \mathbb{K}(E[q])$ and $\mathbb{L}_{\mathfrak{q}} = \mathbb{K}(E[\mathfrak{q}], \mathfrak{q}^{-1}a)$, where $E[q]$: q-division points

Lemma (Modified Index Divisibility Criteria)

Suppose that p splits in $\mathbb{K}$ as $p = \pi_p \overline{\pi_p}$ and $p \nmid q\Delta_E$. Then

1. *If q is inert in $\mathbb{K}$, then $q | i(p)$ if and only if p splits completely in $\mathbb{K}_q$.*
2. *If q ramifies or splits in $\mathbb{K}$ as $q = \mathfrak{q}_1\mathfrak{q}_2$, then $q | i(p)$ if and only if (π_p) splits completely in $\mathbb{L}_{\mathfrak{q}_1}$ or $\mathbb{L}_{\mathfrak{q}_2}$ or $\mathbb{K}_q$.*

Goal: Find the number of primes p satisfying $q \nmid i(p)$ $\forall$ primes q.
General approach:

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \;\Leftrightarrow\; i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle\right] = 1 \;\Leftrightarrow\; q \nmid i(p) \;\forall \text{ primes } q$$

Define: $\mathbb{K}_q = \mathbb{K}(E[q])$ and $\mathbb{L}_\mathfrak{q} = \mathbb{K}(E[\mathfrak{q}], \mathfrak{q}^{-1}a)$, where $E[q]$: q-division points

Lemma (Modified Index Divisibility Criteria)

Suppose that p splits in $\mathbb{K}$ as $p = \pi_p \overline{\pi_p}$ and $p \nmid q\Delta_E$. Then

1. *If q is inert in $\mathbb{K}$, then $q | i(p)$ if and only if p splits completely in $\mathbb{K}_q$.*
2. *If q ramifies or splits in $\mathbb{K}$ as $q = \mathfrak{q}_1\mathfrak{q}_2$, then $q | i(p)$ if and only if (π_p) splits completely in $\mathbb{L}_{\mathfrak{q}_1}$ or $\mathbb{L}_{\mathfrak{q}_2}$ or $\mathbb{K}_q$.*

Goal: Find the number of primes p satisfying $q \nmid i(p)$ $\forall$ primes q.
General approach: Sieve through the primes p in $\mathbb{Q}$ by the set of primes $q | i(p)$.

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \;\Leftrightarrow\; i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle\right] = 1 \;\Leftrightarrow\; q \nmid i(p) \;\forall \text{ primes } q$$

Define: $\mathbb{K}_q = \mathbb{K}(E[q])$ and $\mathbb{L}_{\mathfrak{q}} = \mathbb{K}(E[\mathfrak{q}], \mathfrak{q}^{-1}a)$, where $E[q]$: q-division points

Lemma (Modified Index Divisibility Criteria)

Suppose that p splits in $\mathbb{K}$ as $p = \pi_p \overline{\pi_p}$ and $p \nmid q\Delta_E$. Then

1. *If q is inert in $\mathbb{K}$, then $q | i(p)$ if and only if p splits completely in $\mathbb{K}_q$.*
2. *If q ramifies or splits in $\mathbb{K}$ as $q = \mathfrak{q}_1\mathfrak{q}_2$, then $q | i(p)$ if and only if (π_p) splits completely in $\mathbb{L}_{\mathfrak{q}_1}$ or $\mathbb{L}_{\mathfrak{q}_2}$ or $\mathbb{K}_q$.*

Goal: Find the number of primes p satisfying $q \nmid i(p)$ $\forall$ primes q.
General approach: Sieve through the primes p in $\mathbb{Q}$ by the set of primes $q | i(p)$.
Modified approach:

Main idea behind the proof

Index Divisibility Criteria:

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle \;\Leftrightarrow\; i(p) := \left[\overline{E}(\mathbb{F}_p) : \langle \overline{a} \rangle\right] = 1 \;\Leftrightarrow\; q \nmid i(p) \; \forall \text{ primes } q$$

Define: $\mathbb{K}_q = \mathbb{K}(E[q])$ and $\mathbb{L}_{\mathfrak{q}} = \mathbb{K}(E[\mathfrak{q}], \mathfrak{q}^{-1}a)$, where $E[q]$: q-division points

Lemma (Modified Index Divisibility Criteria)

Suppose that p splits in $\mathbb{K}$ as $p = \pi_p \overline{\pi_p}$ and $p \nmid q\Delta_E$. Then

1. *If q is inert in $\mathbb{K}$, then $q | i(p)$ if and only if p splits completely in $\mathbb{K}_q$.*
2. *If q ramifies or splits in $\mathbb{K}$ as $q = \mathfrak{q}_1 \mathfrak{q}_2$, then $q | i(p)$ if and only if (π_p) splits completely in $\mathbb{L}_{\mathfrak{q}_1}$ or $\mathbb{L}_{\mathfrak{q}_2}$ or $\mathbb{K}_q$.*

Goal: Find the number of primes p satisfying $q \nmid i(p)$ $\forall$ primes q.
General approach: Sieve through the primes p in $\mathbb{Q}$ by the set of primes $q | i(p)$.
Modified approach: Sieve through the ideals (π_p) in $\mathbb{K}$ by the primes $q | i(p)$.

Result 2 (Gupta and Murty)

We obtain the asymptotic expression for $N_a^*(x)$ by sieving.

Result 2 (Gupta and Murty)

We obtain the asymptotic expression for $N_a^*(x)$ by sieving.
But, what can we say about the density $C_E(a)$?

Result 2 (Gupta and Murty)

We obtain the asymptotic expression for $N_a^*(x)$ by sieving.
But, what can we say about the density $C_E(a)$?

Theorem (Gupta and Murty, 1986)

If 2 *and* 3 *are inert in* $\mathbb{K}$ *or if* $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$, *then* $C_E(a) > 0$.

Result 2 (Gupta and Murty)

We obtain the asymptotic expression for $N_a^*(x)$ by sieving.
But, what can we say about the density $C_E(a)$?

Theorem (Gupta and Murty, 1986)

If 2 and 3 are inert in $\mathbb{K}$ or if $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$, then $C_E(a) > 0$. Hence, assuming GRH in these cases, we obtain

$$N_a^*(x) \gg \frac{x}{\log x}$$

Result 2 (Gupta and Murty)

We obtain the asymptotic expression for $N_a^*(x)$ by sieving.
But, what can we say about the density $C_E(a)$?

Theorem (Gupta and Murty, 1986)

If 2 and 3 are inert in $\mathbb{K}$ or if $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$, then $C_E(a) > 0$. Hence, assuming GRH in these cases, we obtain

$$N_a^*(x) \gg \frac{x}{\log x}$$

Case Studies

- 2 and 3 are inert in $\mathbb{K}$: $C_E(a) > 0$ ($\mathbb{K} = \mathbb{Q}(\sqrt{-D})$, $D = 19, 43, 67, 163$)

Result 2 (Gupta and Murty)

We obtain the asymptotic expression for $N_a^*(x)$ by sieving.
But, what can we say about the density $C_E(a)$?

Theorem (Gupta and Murty, 1986)

If 2 and 3 are inert in $\mathbb{K}$ or if $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$, then $C_E(a) > 0$. Hence, assuming GRH in these cases, we obtain

$$N_a^*(x) \gg \frac{x}{\log x}$$

Case Studies

- 2 and 3 are inert in $\mathbb{K}$: $C_E(a) > 0$ ($\mathbb{K} = \mathbb{Q}(\sqrt{-D})$, $D = 19, 43, 67, 163$)
- $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$: $C_E(a) > 0$

Result 2 (Gupta and Murty)

We obtain the asymptotic expression for $N_a^*(x)$ by sieving.
But, what can we say about the density $C_E(a)$?

Theorem (Gupta and Murty, 1986)

If 2 and 3 are inert in $\mathbb{K}$ or if $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$, then $C_E(a) > 0$. Hence, assuming GRH in these cases, we obtain

$$N_a^*(x) \gg \frac{x}{\log x}$$

Case Studies

- 2 and 3 are inert in $\mathbb{K}$: $C_E(a) > 0$ ($\mathbb{K} = \mathbb{Q}(\sqrt{-D})$, $D = 19, 43, 67, 163$)
- $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$: $C_E(a) > 0$
- $\mathbb{K} = \mathbb{Q}(\sqrt{-7})$: $C_E(a) = 0$ (2 splits in $\mathbb{Q}(\sqrt{-7})$)

Result 2 (Gupta and Murty)

We obtain the asymptotic expression for $N_a^*(x)$ by sieving.
But, what can we say about the density $C_E(a)$?

Theorem (Gupta and Murty, 1986)

If 2 and 3 are inert in $\mathbb{K}$ or if $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$, then $C_E(a) > 0$. Hence, assuming GRH in these cases, we obtain

$$N_a^*(x) \gg \frac{x}{\log x}$$

Case Studies

- 2 and 3 are inert in $\mathbb{K}$: $C_E(a) > 0$ ($\mathbb{K} = \mathbb{Q}(\sqrt{-D})$, $D = 19, 43, 67, 163$)
- $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$: $C_E(a) > 0$
- $\mathbb{K} = \mathbb{Q}(\sqrt{-7})$: $C_E(a) = 0$ (2 splits in $\mathbb{Q}(\sqrt{-7})$)
- $\mathbb{K} = \mathbb{Q}(\sqrt{-2})$: $C_E(a) > 0$ most of the time

Result 2 (Gupta and Murty)

We obtain the asymptotic expression for $N_a^*(x)$ by sieving.
But, what can we say about the density $C_E(a)$?

Theorem (Gupta and Murty, 1986)

If 2 and 3 are inert in $\mathbb{K}$ or if $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$, then $C_E(a) > 0$. Hence, assuming GRH in these cases, we obtain

$$N_a^*(x) \gg \frac{x}{\log x}$$

Case Studies

- 2 and 3 are inert in $\mathbb{K}$: $C_E(a) > 0$ ($\mathbb{K} = \mathbb{Q}(\sqrt{-D})$, $D = 19, 43, 67, 163$)
- $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$: $C_E(a) > 0$
- $\mathbb{K} = \mathbb{Q}(\sqrt{-7})$: $C_E(a) = 0$ (2 splits in $\mathbb{Q}(\sqrt{-7})$)
- $\mathbb{K} = \mathbb{Q}(\sqrt{-2})$: $C_E(a) > 0$ most of the time

Result 2 (Gupta and Murty)

We obtain the asymptotic expression for $N_a^*(x)$ by sieving.
But, what can we say about the density $C_E(a)$?

Theorem (Gupta and Murty, 1986)

If 2 and 3 are inert in $\mathbb{K}$ or if $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$, then $C_E(a) > 0$. Hence, assuming GRH in these cases, we obtain

$$N_a^*(x) \gg \frac{x}{\log x}$$

Case Studies

- 2 and 3 are inert in $\mathbb{K}$: $C_E(a) > 0$ ($\mathbb{K} = \mathbb{Q}(\sqrt{-D})$, $D = 19, 43, 67, 163$)
- $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$: $C_E(a) > 0$
- $\mathbb{K} = \mathbb{Q}(\sqrt{-7})$: $C_E(a) = 0$ (2 splits in $\mathbb{Q}(\sqrt{-7})$)
- $\mathbb{K} = \mathbb{Q}(\sqrt{-2})$: $C_E(a) > 0$ most of the time

Hence we have a positive density in most of the cases.

Higher Rank Analogue

Higher Rank Analogue

Let us suppose that Γ is a free subgroup of rational points of the elliptic curve.

Higher Rank Analogue

Let us suppose that Γ is a free subgroup of rational points of the elliptic curve.

Analogous problem of Artin's conjecture

Higher Rank Analogue

Let us suppose that Γ is a free subgroup of rational points of the elliptic curve.

Analogous problem of Artin's conjecture

Compute the density of the primes p for which the elliptic curve group reduced modulo p is generated by Γ_p, the reduction of the free subgroup modulo p.

Higher Rank Analogue

Let us suppose that Γ is a free subgroup of rational points of the elliptic curve.

Analogous problem of Artin's conjecture

Compute the density of the primes p for which the elliptic curve group reduced modulo p is generated by Γ_p, the reduction of the free subgroup modulo p.

Higher Rank Results: Gupta and Murty (1986)

Higher Rank Analogue

Let us suppose that Γ is a free subgroup of rational points of the elliptic curve.

Analogous problem of Artin's conjecture

Compute the density of the primes p for which the elliptic curve group reduced modulo p is generated by Γ_p, the reduction of the free subgroup modulo p.

Higher Rank Results: Gupta and Murty (1986)

The conjecture is true assuming generalized Riemann Hypothesis for

Higher Rank Analogue

Let us suppose that Γ is a free subgroup of rational points of the elliptic curve.

Analogous problem of Artin's conjecture

Compute the density of the primes p for which the elliptic curve group reduced modulo p is generated by Γ_p, the reduction of the free subgroup modulo p.

Higher Rank Results: Gupta and Murty (1986)

The conjecture is true assuming generalized Riemann Hypothesis for

- $\mathrm{rank}(\Gamma) \geq 18$ for E with no complex multiplication.

Higher Rank Analogue

Let us suppose that Γ is a free subgroup of rational points of the elliptic curve.

Analogous problem of Artin's conjecture

Compute the density of the primes p for which the elliptic curve group reduced modulo p is generated by Γ_p, the reduction of the free subgroup modulo p.

Higher Rank Results: Gupta and Murty (1986)

The conjecture is true assuming generalized Riemann Hypothesis for

- $\text{rank}(\Gamma) \geq 18$ for E with no complex multiplication.
- $\text{rank}(\Gamma) \geq 10$ for E with CM over a quadratic extension of $\mathbb{Q}$.

Higher Rank Analogue

Let us suppose that Γ is a free subgroup of rational points of the elliptic curve.

Analogous problem of Artin's conjecture

Compute the density of the primes p for which the elliptic curve group reduced modulo p is generated by Γ_p, the reduction of the free subgroup modulo p.

Higher Rank Results: Gupta and Murty (1986)

The conjecture is true assuming generalized Riemann Hypothesis for

- $\mathrm{rank}(\Gamma) \geq 18$ for E with no complex multiplication.
- $\mathrm{rank}(\Gamma) \geq 10$ for E with CM over a quadratic extension of $\mathbb{Q}$.

Higher Rank Analogue

Let us suppose that Γ is a free subgroup of rational points of the elliptic curve.

Analogous problem of Artin's conjecture

Compute the density of the primes p for which the elliptic curve group reduced modulo p is generated by Γ_p, the reduction of the free subgroup modulo p.

Higher Rank Results: Gupta and Murty (1986)

The conjecture is true assuming generalized Riemann Hypothesis for

- $\text{rank}(\Gamma) \geq 18$ for E with no complex multiplication.
- $\text{rank}(\Gamma) \geq 10$ for E with CM over a quadratic extension of $\mathbb{Q}$.

The assumption of GRH can be somewhat relaxed for higher rank case with E having complex multiplication.

Concluding remarks

The Bigger Picture

The Bigger Picture

Original Conjecture

The Bigger Picture

Original Conjecture

- Conditional Proof - Christopher Hooley (1967)

The Bigger Picture

Original Conjecture

- Conditional Proof - Christopher Hooley (1967)
- Unconditional Proof

The Bigger Picture

Original Conjecture

- Conditional Proof - Christopher Hooley (1967)
- Unconditional Proof
  - Rajiv Gupta and M. Ram Murty (1983)

The Bigger Picture

Original Conjecture

- Conditional Proof - Christopher Hooley (1967)
- Unconditional Proof
  - Rajiv Gupta and M. Ram Murty (1983)
  - D. Roger Heath-Brown (1986)

The Bigger Picture

Original Conjecture

- Conditional Proof - Christopher Hooley (1967)
- Unconditional Proof
    - Rajiv Gupta and M. Ram Murty (1983)
    - D. Roger Heath-Brown (1986)
- Average Case - P.J. Stephens (1969)

The Bigger Picture

Original Conjecture

- Conditional Proof - Christopher Hooley (1967)
- Unconditional Proof
  - Rajiv Gupta and M. Ram Murty (1983)
  - D. Roger Heath-Brown (1986)
- Average Case - P.J. Stephens (1969)

Analogous Conjectures

The Bigger Picture

Original Conjecture

- Conditional Proof - Christopher Hooley (1967)
- Unconditional Proof
  - Rajiv Gupta and M. Ram Murty (1983)
  - D. Roger Heath-Brown (1986)
- Average Case - P.J. Stephens (1969)

Analogous Conjectures

- Elliptic Curve Analogue

The Bigger Picture

Original Conjecture

- Conditional Proof - Christopher Hooley (1967)
- Unconditional Proof
  - Rajiv Gupta and M. Ram Murty (1983)
  - D. Roger Heath-Brown (1986)
- Average Case - P.J. Stephens (1969)

Analogous Conjectures

- Elliptic Curve Analogue
  - S. Lang and H. Trotter (1977)

The Bigger Picture

Original Conjecture

- Conditional Proof - Christopher Hooley (1967)
- Unconditional Proof
  - Rajiv Gupta and M. Ram Murty (1983)
  - D. Roger Heath-Brown (1986)
- Average Case - P.J. Stephens (1969)

Analogous Conjectures

- Elliptic Curve Analogue
  - S. Lang and H. Trotter (1977)
  - Rajiv Gupta and M. Ram Murty (1986)

The Bigger Picture

Original Conjecture

- Conditional Proof - Christopher Hooley (1967)
- Unconditional Proof
  - Rajiv Gupta and M. Ram Murty (1983)
  - D. Roger Heath-Brown (1986)
- Average Case - P.J. Stephens (1969)

Analogous Conjectures

- Elliptic Curve Analogue
  - S. Lang and H. Trotter (1977)
  - Rajiv Gupta and M. Ram Murty (1986)
- Composite Moduli Analogue - S. Li and Carl Pomerance (2000)

The Bigger Picture

Original Conjecture

- Conditional Proof - Christopher Hooley (1967)
- Unconditional Proof
  - Rajiv Gupta and M. Ram Murty (1983)
  - D. Roger Heath-Brown (1986)
- Average Case - P.J. Stephens (1969)

Analogous Conjectures

- Elliptic Curve Analogue
  - S. Lang and H. Trotter (1977)
  - Rajiv Gupta and M. Ram Murty (1986)
- Composite Moduli Analogue - S. Li and Carl Pomerance (2000)
- Drinfeld Module Analogue - Chih-Nung Hsu and Jing Yu (2001)

Open Questions: Unconditional Proof

Open Questions: Unconditional Proof

- The conjecture has been proven for almost all integers.

Open Questions: Unconditional Proof

- The conjecture has been proven for almost all integers.
- It has not been proven completely without the assumption of the generalized Riemann hypothesis.

Open Questions: Unconditional Proof

- The conjecture has been proven for almost all integers.
- It has not been proven completely without the assumption of the generalized Riemann hypothesis.
- We know that there exist at most 2 exceptional primes for which the conjecture might fail.

Open Questions: Unconditional Proof

- The conjecture has been proven for almost all integers.
- It has not been proven completely without the assumption of the generalized Riemann hypothesis.

- We know that there exist at most 2 exceptional primes for which the conjecture might fail.
- Which 2 ? - We can not explicitly point those two out.

Open Questions: Unconditional Proof

- The conjecture has been proven for almost all integers.
- It has not been proven completely without the assumption of the generalized Riemann hypothesis.

- We know that there exist at most 2 exceptional primes for which the conjecture might fail.
- Which 2 ? - We can not explicitly point those two out.

Open Question: Unconditional Proof of Artin's Conjecture

Open Questions: Elliptic Curve Analogue

Open Questions: Elliptic Curve Analogue

- Is the analogous conjecture true unconditionally for all curves?

Open Questions: Elliptic Curve Analogue

- Is the analogous conjecture true unconditionally for all curves?
- Can we formulate the proof without the assumption of complex multiplication of the curve?

Open Questions: Elliptic Curve Analogue

- Is the analogous conjecture true unconditionally for all curves?
- Can we formulate the proof without the assumption of complex multiplication of the curve?
- Is the analogue in case of higher rank elliptic curves true without the assumption of GRH?

Questions ?

Thank you for your attention !