A (not so) mean feat of Erdős

Paul Pollack

University of British Columbia/Simon Fraser University

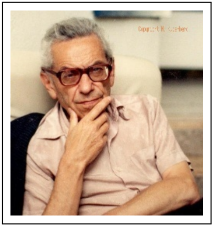
May 31, 2012

Definition

For each odd prime q, let $n_2(q)$ denote the least quadratic nonresidue modulo q. For example, $n_2(5) = 2$ and $n_2(7) = 3$. For completeness, put $n_2(2) = 0$.

Definition

For each odd prime q, let $n_2(q)$ denote the least quadratic nonresidue modulo q. For example, $n_2(5) = 2$ and $n_2(7) = 3$. For completeness, put $n_2(2) = 0$.



Theorem (Erdős, 1961)

We can determine the average value of the least quadratic nonresidue modulo primes q:

$$\lim_{x\to\infty}\left(\frac{1}{\pi(x)}\sum_{q\le x} n_2(q)\right) = A,$$

where

$$A := \sum_{k=1}^{\infty}\frac{p_k}{2^k},$$

and p_k denotes the kth prime.

Remark

Numerically,

$$A = 3.674643966011328778995676309084029411677797 5\ldots$$

Remark

Numerically,

$$A = 3.674643966011328778995676309084029411677797 5\ldots$$

Time muffles the original éclat of a theorem. In 1967, in a Nottingham seminar, I did not get past the value of Erdős's limit ... before Eduard Wirsing stopped me. "I don't believe it!", says he, looking at the expression for the constant, "I have never seen anything like it!"
– Peter Elliott

Known knowns and known unknowns

Erdős's theorem is about the *average order* of $n_2(q)$.
The study of the *maximal order* of $n_2(q)$ is older.

Known knowns and known unknowns

Erdős's theorem is about the *average order* of $n_2(q)$.
The study of the *maximal order* of $n_2(q)$ is older.

Theorem (Gauss)

If $q \equiv 1 \pmod 8$*, then there is a prime* $p < 2\sqrt{q} + 1$ *with* $\left(\frac{q}{p}\right) = -1$.

Corollary (post-QR)

If $q \equiv 1 \pmod 8$*, then* $n_2(q) < 2\sqrt{q} + 1$.

Known knowns and known unknowns

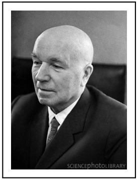
Erdős's theorem is about the *average order* of $n_2(q)$.
The study of the *maximal order* of $n_2(q)$ is older.

Theorem (Gauss)

If $q \equiv 1 \pmod 8$, *then there is a prime* $p < 2\sqrt{q} + 1$ *with* $\left(\frac{q}{p}\right) = -1$.

Corollary (post-QR)

If $q \equiv 1 \pmod 8$, *then* $n_2(q) < 2\sqrt{q} + 1$.



Conjecture (I.M. Vinogradov)

For each fixed $\epsilon > 0$ *and all* $q > q_0(\epsilon)$, *we have*

$$n_2(q) < q^{\epsilon}.$$

Theorem (Ankeny)

Assume the Riemann Hypothesis for Dirichlet L-functions. Then Vinogradov's conjecture is correct. In fact,

$$n_2(q) < C(\log q)^2$$

for all odd primes q.

Theorem (Bach)

We can take $C = 2$ in Ankeny's result.

Theorem (Ankeny)

Assume the Riemann Hypothesis for Dirichlet L-functions. Then Vinogradov's conjecture is correct. In fact,

$$n_2(q) < C(\log q)^2$$

for all odd primes q.

Theorem (Bach)

We can take $C = 2$ in Ankeny's result.

What about unconditionally?
In 1918, Pólya and Vinogradov showed (independently) that

$$\left| \sum_{n \le x} \left(\frac{n}{q} \right) \right| < \sqrt{q} \log q.$$

As an immediate consequence, $n_2(q) < 1 + \sqrt{q} \log q$.

Theorem (Vinogradov)

For each $\epsilon > 0$ and all primes $q > q_0(\epsilon)$, we have

$$n_2(q) < q^{\frac{1}{2\sqrt{e}}+\epsilon}.$$

Theorem (Burgess)

For each $\epsilon > 0$ and all primes $q > q_0(\epsilon)$, we have

$$n_2(q) < q^{\frac{1}{4\sqrt{e}}+\epsilon}.$$

Theorem (Linnik)

Fix $\epsilon > 0$. The number of primes $q \leq x$ with $n_2(q) > q^{\epsilon}$ is $\ll_{\epsilon} \log\log x$.

Interlude: A proof that $n_2(q) < q^{1/2}$

Given a fraction $\frac{a}{b}$ with $q \nmid b$, we identify $\frac{a}{b}$ with $ab^{-1} \pmod{q}$.
Notice that

$$\frac{a}{b} \equiv \frac{c}{d} \pmod{q} \Longleftrightarrow q \mid ad - bc.$$

Interlude: A proof that $n_2(q) < q^{1/2}$

Given a fraction $\frac{a}{b}$ with $q \nmid b$, we identify $\frac{a}{b}$ with $ab^{-1} \pmod{q}$. Notice that

$$\frac{a}{b} \equiv \frac{c}{d} \pmod{q} \iff q \mid ad - bc.$$

Now consider the following set of fractions:

$$\mathfrak{F} = \left\{ \frac{a}{b} : 1 \leq a, b \leq \sqrt{q} \text{ and } \gcd(a, b) = 1 \right\}.$$

Interlude: A proof that $n_2(q) < q^{1/2}$

Given a fraction $\frac{a}{b}$ with $q \nmid b$, we identify $\frac{a}{b}$ with $ab^{-1} \pmod{q}$. Notice that

$$\frac{a}{b} \equiv \frac{c}{d} \pmod{q} \Longleftrightarrow q \mid ad - bc.$$

Now consider the following set of fractions:

$$\mathfrak{F} = \left\{ \frac{a}{b} : 1 \le a, b \le \sqrt{q} \text{ and } \gcd(a, b) = 1 \right\}.$$

The probability two integers are relatively prime is $1/\zeta(2) = 6/\pi^2$, and so

$$\#\mathfrak{F} \sim \frac{6}{\pi^2} q, \quad \text{which gives} \quad \#\mathfrak{F} > \frac{q}{2}$$

for large q.

Lemma

No two elements of $\mathfrak{F}$ are congruent modulo q.

Proof.

If $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in \mathfrak{F}$ (and not the same), then $0 < |a_1 b_2 - a_2 b_1| < q$.

Lemma

No two elements of $\mathfrak{F}$ are congruent modulo q.

Proof.

If $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in \mathfrak{F}$ (and not the same), then $0 < |a_1 b_2 - a_2 b_1| < q$.

Since $\#\mathfrak{F} > q/2$ and there are only $\frac{q-1}{2}$ (nonzero) squares mod q, some $\frac{a}{b} \in \mathfrak{F}$ reduces to a nonsquare mod q. So either a is a nonsquare or b is a nonsquare. Hence,

$$n_2(q) \leq \sqrt{q}.$$

(Of course, equality is impossible here.)

The average least nonresidue, revisited

Theorem (Erdős, 1961)

We can determine the average value of the least quadratic nonresidue modulo primes q:

$$\lim_{x\to\infty}\left(\frac{1}{\pi(x)}\sum_{q\le x} n_2(q)\right) = A,$$

where

$$A := \sum_{k=1}^{\infty}\frac{p_k}{2^k},$$

and p_k denotes the kth prime in increasing order.

Why you should believe Erdős

- multiplicativity of the Legendre symbol implies that $n_2(q)$ is always a prime,

Why you should believe Erdős

- multiplicativity of the Legendre symbol implies that $n_2(q)$ is always a prime,
- for a fixed prime p, we have a 50-50 chance that $\left(\frac{p}{q}\right) = -1$ for a randomly chosen prime q,

Why you should believe Erdős

- multiplicativity of the Legendre symbol implies that $n_2(q)$ is always a prime,
- for a fixed prime p, we have a 50-50 chance that $\left(\frac{p}{q}\right) = -1$ for a randomly chosen prime q,
- in order for $n_2(q)$ to equal p_k, it is necessary and sufficient that

$$\left(\frac{p_1}{q}\right) = \left(\frac{p_2}{q}\right) = \cdots = \left(\frac{p_{k-1}}{q}\right) = 1 \text{ and } \left(\frac{p_k}{q}\right) = -1.$$

Why you should believe Erdős

- multiplicativity of the Legendre symbol implies that $n_2(q)$ is always a prime,
- for a fixed prime p, we have a 50-50 chance that $\left(\frac{p}{q}\right) = -1$ for a randomly chosen prime q,
- in order for $n_2(q)$ to equal p_k, it is necessary and sufficient that

$$\left(\frac{p_1}{q}\right) = \left(\frac{p_2}{q}\right) = \cdots = \left(\frac{p_{k-1}}{q}\right) = 1 \text{ and } \left(\frac{p_k}{q}\right) = -1.$$

- Independence $\Rightarrow \mathbb{P}(n_2(q) = p_k) = \frac{1}{2^k}$.

Why you should believe Erdős

- multiplicativity of the Legendre symbol implies that $n_2(q)$ is always a prime,
- for a fixed prime p, we have a 50-50 chance that $\left(\frac{p}{q}\right) = -1$ for a randomly chosen prime q,
- in order for $n_2(q)$ to equal p_k, it is necessary and sufficient that

$$\left(\frac{p_1}{q}\right) = \left(\frac{p_2}{q}\right) = \cdots = \left(\frac{p_{k-1}}{q}\right) = 1 \text{ and } \left(\frac{p_k}{q}\right) = -1.$$

- Independence $\Rightarrow \mathbb{P}(n_2(q) = p_k) = \frac{1}{2^k}$.
- So we "should" have $\mathbb{E}(n_2) = \sum_{k=1}^{\infty} 2^{-k} p_k$.

Sketch of the proof

We want to understand

$$\frac{1}{\pi(x)}\sum_{q\le x} n_2(q) = \sum_k p_k \cdot \frac{\#\{q \le x : n_2(q) = p_k\}}{\#\{q \le x\}}.$$

Sketch of the proof

We want to understand

$$\frac{1}{\pi(x)} \sum_{q \le x} n_2(q) = \sum_k p_k \cdot \frac{\#\{q \le x : n_2(q) = p_k\}}{\#\{q \le x\}}.$$

Step #1: Treat small values of $n_2(q)$ with precision
By quadratic reciprocity, $n_2(q) = p_k$ if and only if q belongs to a certain set of coprime residue classes modulo $4p_1p_2\cdots p_k$. The fraction of OK residue classes is $1/2^k$. The PNT for APs gives:

Lemma

Assume $p_k \le \frac{1}{2}\log\log x$. The number of $q \le x$ for which $n_2(q) = p_k$ is $\frac{1}{2^k}\pi(x) + O(x\exp(-c\sqrt{\log x}))$.

Using this estimate, we get

$$\frac{1}{\pi(x)}\sum_{q\le x} n_2(q) = \sum_k p_k \cdot \frac{\#\{q \le x : n_2(q) = p_k\}}{\#\{q \le x\}}$$

$$= \sum_{p_k \le \frac{1}{2}\log\log x} \frac{p_k}{2^k} + o(1)$$

$$+ \sum_{p_k > \frac{1}{2}\log\log x} p_k \cdot \frac{\#\{q \le x : n_2(q) = p_k\}}{\#\{q \le x\}}$$

Using this estimate, we get

$$\frac{1}{\pi(x)} \sum_{q \le x} n_2(q) = \sum_k p_k \cdot \frac{\#\{q \le x : n_2(q) = p_k\}}{\#\{q \le x\}}$$

$$= \sum_{p_k \le \frac{1}{2} \log\log x} \frac{p_k}{2^k} + o(1)$$

$$+ \sum_{p_k > \frac{1}{2} \log\log x} p_k \cdot \frac{\#\{q \le x : n_2(q) = p_k\}}{\#\{q \le x\}}$$

So as $x \to \infty$,

$$\frac{1}{\pi(x)} \sum_{q \le x} n_2(q) = A + o(1)$$

$$+ \frac{1}{\pi(x)} \sum_{p_k > \frac{1}{2} \log\log x} p_k \cdot \#\{q \le x : n_2(q) = p_k\}.$$

We need to show that the last term goes to zero as x goes to infinity.

So the PNT for arithmetic progression handles the contribution from small primes ($p_k \leq \frac{1}{2} \log\log x$), which gives us the correct main term.

So the PNT for arithmetic progression handles the contribution from small primes ($p_k \leq \frac{1}{2} \log \log x$), which gives us the correct main term.

Step #2: Handle medium values of $n_2(q)$ using a crude upper bound

The Brun–Titchmarsh theorem says that as long as the modulus $m < x^{1/2}$ (for example), we have

$$\pi(x; m, a) \leq \frac{4}{\phi(m)} \frac{x}{\log x}.$$

So the PNT for arithmetic progression handles the contribution from small primes ($p_k \le \frac{1}{2}\log\log x$), which gives us the correct main term.

Step #2: Handle medium values of $n_2(q)$ using a crude upper bound

The Brun–Titchmarsh theorem says that as long as the modulus $m < x^{1/2}$ (for example), we have

$$\pi(x; m, a) \le \frac{4}{\phi(m)} \frac{x}{\log x}.$$

Using this, we can show that those values of $n_2(q) = p_k$ with $\frac{1}{2}\log\log x < p_k < (\log x)^{1000}$ make a negligible contribution:

$$\frac{1}{\pi(x)} \sum_{\frac{1}{2}\log\log x < p_k \le (\log x)^{1000}} p_k \cdot \#\{q \le x : n_2(q) = p_k\} \to 0.$$

Step #3: Handle values $n_2(q) > (\log x)^{1000}$, by hook or by crook

It remains to show that as $x \to \infty$,

$$\frac{1}{\pi(x)} \sum_{\substack{q \le x \\ n_2(q) > (\log x)^{1000}}} n_2(q) \to 0.$$

Step #3: Handle values $n_2(q) > (\log x)^{1000}$, by hook or by crook

It remains to show that as $x \to \infty$,

$$\frac{1}{\pi(x)} \sum_{\substack{q \le x \\ n_2(q) > (\log x)^{1000}}} n_2(q) \to 0.$$

Trivially,

$$\sum_{\substack{2 < q \le x \\ n_2(q) > (\log x)^{1000}}} n_2(q) \le AB,$$

where

$$A := \max_{q \le x} n_2(q) \quad \text{and} \quad B := \#\{q \le x : n_2(q) > (\log x)^{1000}\}.$$

We proved $A < x^{1/2}$ for large x.

To estimate B, we use a result of Erdős, proved using the large sieve ("GRH on average"):

Lemma (Erdős)

Fix $Z > 0$ and $\epsilon > 0$. The number of $q \leq x$ with $n_2(q) > (\log x)^Z$ is at most $x^{2/Z+\epsilon}$. In particular, the number of $q \leq x$ with $n_2(q) > (\log x)^{1000}$ is $\ll x^{1/499}$.

To estimate B, we use a result of Erdős, proved using the large sieve ("GRH on average"):

Lemma (Erdős)

Fix $Z > 0$ and $\epsilon > 0$. The number of $q \leq x$ with $n_2(q) > (\log x)^Z$ is at most $x^{2/Z+\epsilon}$. In particular, the number of $q \leq x$ with $n_2(q) > (\log x)^{1000}$ is $\ll x^{1/499}$.

Thus,

$$AB \ll x^{1/2} \cdot x^{1/499} < x^{2/3}.$$

So

$$\frac{1}{\pi(x)} \sum_{\substack{2<q\leq x \\ n_2(q)>(\log x)^{1000}}} n_2(q) \leq \frac{AB}{\pi(x)} \ll \frac{x^{2/3}}{\pi(x)},$$

which goes to zero.

To estimate B, we use a result of Erdős, proved using the large sieve ("GRH on average"):

Lemma (Erdős)

Fix $Z > 0$ and $\epsilon > 0$. The number of $q \leq x$ with $n_2(q) > (\log x)^Z$ is at most $x^{2/Z+\epsilon}$. In particular, the number of $q \leq x$ with $n_2(q) > (\log x)^{1000}$ is $\ll x^{1/499}$.

Thus,

$$AB \ll x^{1/2} \cdot x^{1/499} < x^{2/3}.$$

So

$$\frac{1}{\pi(x)} \sum_{\substack{2<q\leq x \\ n_2(q)>(\log x)^{1000}}} n_2(q) \leq \frac{AB}{\pi(x)} \ll \frac{x^{2/3}}{\pi(x)},$$

which goes to zero.

This completes the proof of Erdős's theorem.

Variations

For primes $q \equiv 1 \pmod{k}$, let $n_k(q)$ denote the least kth power nonresidue and $r_k(q)$ denote the least *prime* kth power residue. The following results are due to Peter Elliott:

Theorem
For each fixed k, the mean value of $n_k(q)$ exists.

Theorem
For each of $k = 2, 3, 4$, the mean value of $r_k(q)$ exists. When $k = 2$, the mean value of r_2 agrees with the mean value of n_2.

Variations

For primes $q \equiv 1 \pmod{k}$, let $n_k(q)$ denote the least kth power nonresidue and $r_k(q)$ denote the least *prime* kth power residue. The following results are due to Peter Elliott:

Theorem

For each fixed k, the mean value of $n_k(q)$ exists.

Theorem

For each of $k = 2, 3, 4$, the mean value of $r_k(q)$ exists. When $k = 2$, the mean value of r_2 agrees with the mean value of n_2.

Non-analogy: We have $n_k(q) \ll_\epsilon q^{1/4\sqrt{e}+\epsilon}$ (Burgess),
but we only know $r_k(q) \ll_\epsilon q^{\frac{1}{4}(k-1)+\epsilon}$ (Linnik–Vinogradov, Elliott).

Prime splitting in number fields

For each prime q, let K be the quadratic field of conductor q. So $K = \mathbb{Q}(\sqrt{q^*})$, where $q^* = (-1)^{\frac{q-1}{2}} q$. Then for any prime $p \neq q$,

$$p \text{ is inert in } K \Longleftrightarrow \left(\frac{p}{q}\right) = -1$$

and

$$p \text{ splits in } K \Longleftrightarrow \left(\frac{p}{q}\right) = 1.$$

So rephrasing the results of Erdős and Elliott:

Theorem

The average least inert prime in a quadratic field of prime conductor is $\sum_{k=1}^{\infty} 2^{-k} p_k$. The same holds for the average least split prime.

The quadratic field case

For each prime p, one can show that if one chooses a quadratic field uniformly at random,

$$\mathbb{P}(p \text{ inert}) = \frac{1/2}{1 + 1/p},$$

and similarly for $\mathbb{P}(p \text{ split})$.

In other words, as $x \to \infty$,

$$\frac{\sum_{|D| \leq x,\ \left(\frac{D}{p}\right) = -1} 1}{\sum_{|D| \leq x} 1} \to \frac{1/2}{1 + 1/p}.$$

and similarly with $\left(\frac{D}{p}\right) = 1$. Here D runs over fundamental discriminants.

The quadratic field case

For each prime p, one can show that if one chooses a quadratic field uniformly at random,

$$\mathbb{P}(p \text{ inert}) = \frac{1/2}{1 + 1/p},$$

and similarly for $\mathbb{P}(p \text{ split})$.

In other words, as $x \to \infty$,

$$\frac{\sum_{|D| \le x,\ \left(\frac{D}{p}\right) = -1} 1}{\sum_{|D| \le x} 1} \to \frac{1/2}{1 + 1/p}.$$

and similarly with $\left(\frac{D}{p}\right) = 1$. Here D runs over fundamental discriminants.

We can prove this by hand, using that $\left(\frac{D}{p}\right) = 1$ is a congruence condition on D modulo $4p$.

Theorem (P.)

Let $n(D)$ be the least inert prime in the quadratic field of discriminant D and $r(D)$ the least split prime. Then as $x \to \infty$,

$$\frac{\sum_{|D| \le x} n(D)}{\sum_{|D| \le x} 1} \to \theta,$$

where

$$\theta = \sum_{k=1}^{\infty} p_k \cdot \left(\mathbb{P}(p_k \text{ inert}) \prod_{i=1}^{k-1} (1 - \mathbb{P}(p_{k-1} \text{ inert})) \right).$$

The constant θ satisfies $\theta \approx 4.98095$. The same result holds for $r(D)$.

Cubic fields

In a cubic field K, there are more splitting options, for example,

$$p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \quad \text{(split completely)}$$
$$p = \mathfrak{p}_1\mathfrak{p}_2 \quad \text{(partially split)}$$
$$p = \mathfrak{p}_1 \quad \text{(inert)}$$

We would like to be able compute the average least prime in each case (or not in each case).

Theorem (Martin, P.)

We can do any of these averages – assuming the Generalized Riemann Hypothesis.

Theorem (Martin, P.)

For a cubic number field K, let n_K denote the least rational prime that does not split completely in K. Define

$$\Delta = \sum_{\ell} \frac{5\ell^3 + 6\ell^2 + 6\ell}{6(\ell^2 + \ell + 1)} \prod_{p<\ell} \frac{p^2}{6(p^2 + p + 1)} \approx 2.1211027269,$$

*where the sum and product are taken over primes ℓ and p. Then (**unconditionally!**)*

$$\lim_{x\to\infty} \left(\sum_{|D_K|\leq x} 1 \right)^{-1} \left(\sum_{|D_K|\leq x} n_K \right) = \Delta,$$

where the sums on the left-hand side are taken over (all isomorphism classes of) cubic fields K for which $|D_K| \leq x$.

Why you should believe us

- We split the average up according to the value of n_K:

$$\frac{\sum_{|D_K|\leq x} n_K}{\sum_{|D_K|\leq x} 1} = \sum_k p_k \cdot \frac{\#\{|D_K| \leq x,\ p_k = n_K\}}{\sum_{|D_K|\leq x} 1}.$$

The ratio on the RHS is $\mathbb{P}(n_K = p_k : |D_K| \leq x)$.

- For the denominator in the averages, we have (Davenport–Heilbronn) that as $x \to \infty$,

$$\sum_{|D_K|\leq x} 1 \sim \frac{1}{3\zeta(3)} x.$$

- For each prime p, let $c_p = \frac{1/6}{1+1/p+1/p^2}$.
It is known that the limiting probability p_k is the least split completely prime is

$$\mathbb{P}(n_K = p_k) = (1 - c_{p_k}) \prod_{j=1}^{k-1} c_{p_j}.$$

Our claim for the "average value"

$$\Delta = \sum_k p_k \cdot \mathbb{P}(n_K = p_k).$$

- Work of Taniguchi–Thorne/Bhargava–Shankar–Tsimerman gives a *uniform estimate*. We get a main term of Δ from the primes $p_k \leq (\log x)^{1000}$.

It remains to show that

$$\frac{\sum_{\substack{|D_K|\le x \\ n_K > (\log x)^{1000}}} n_K}{\sum_{|D_K|\le x} 1} \to 0.$$

We bound

$$\sum_{\substack{K:\ |D_K|\le x \\ n_K > (\log x)^{1000}}} n_K$$

by AB, where A is the largest term and B is the number of terms.

The contribution to the average is obtained by dividing by the number of cubic fields with $|D_K| \le x$, which is $\sim \frac{1}{\zeta(3)}x$. So we want

$$AB = o(x).$$

Claim 1: each $n_K \ll_\epsilon |D_K|^{1/4\sqrt{e}+\epsilon}$, so that $A < x^{0.152}$ (say).

For non-Galois K, we use the *quadratic-resolvent of* K: The field $\mathbb{Q}(\sqrt{D_K})$ sits inside the normal closure of K. The least non-split prime in K is bounded above by the least non-split prime in $\mathbb{Q}(\sqrt{D_K})$, which is

$$\ll |D_K|^{1/4\sqrt{e}+\epsilon}.$$

If $K/\mathbb{Q}$ is Galois, then $K/\mathbb{Q}$ is abelian and $D_K = f^2$ is a square. In this case, the least non-split prime in K is the least prime p with $\chi(p) \notin \{0, 1\}$, where χ is a primitive cubic character modulo f. This implies (Burgess/Norton) an even better upper bound on n_K: namely,

$$\ll |D_K|^{1/8\sqrt{e}+\epsilon}.$$

Claim 2: $B < x^{0.84}$; in other words,
the number of K with $|D_K| \leq x$ and $n_K > (\log x)^{1000}$ is $< x^{0.84}$

[Assuming this: $0.152 + 0.84 < 0.995$, so $AB < x^{0.995} = o(X)$, and we are done!]

To prove the claim, we first throw away the Galois cubic fields. There are only $\ll x^{1/2}$ of those (Cohn), so this is OK. Each K that is left has a quadratic resolvent $\mathbb{Q}(\sqrt{D})$, where $D = D_K$. We can write

$$D = df^2,$$

where d is the discriminant of $\mathbb{Q}(\sqrt{D})$. Given d, there are at most $\sqrt{x/f} < \sqrt{x}$ possibilities for D.

We count the number of possibilities for d, then D, then K.

Since $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{D_K})$ is a subfield of the Galois closure of K, all primes $< (\log x)^{1000}$ are split.

We count the number of possibilities for d, then D, then K.

Since $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{D_K})$ is a subfield of the Galois closure of K, all primes $< (\log x)^{1000}$ are split.

We use the following lemma:

Lemma (proved using the large sieve)

The number of quadratic fields with discriminant bounded by x in absolute value for which all primes $\leq (\log x)^Z$ split completely is at most $x^{2/Z+o(1)}$, as $x \to \infty$.

So the number of possibilities for d is $\leq x^{1/500+o(1)}$.

We count the number of possibilities for d, then D, then K.

Since $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{D_K})$ is a subfield of the Galois closure of K, all primes $< (\log x)^{1000}$ are split.

We use the following lemma:

Lemma (proved using the large sieve)

The number of quadratic fields with discriminant bounded by x in absolute value for which all primes $\leq (\log x)^Z$ split completely is at most $x^{2/Z+o(1)}$, as $x \to \infty$.

So the number of possibilities for d is $\leq x^{1/500+o(1)}$.

So the number of possibilities for D is $< x^{1/2+1/500+o(1)}$.

Theorem (Ellenberg–Venkatesh)

Let $\epsilon > 0$. As $|D| \to \infty$, the number of cubic fields of discriminant D is $\leq |D|^{1/3+o(1)}$.

It follows that

$$B < x^{1/2+1/500+1/3+o(1)},$$

which is eventually smaller than $x^{0.84}$. This completes the proof of Claim #2 and so also the theorem.

Theorem (Ellenberg–Venkatesh)

Let $\epsilon > 0$. As $|D| \to \infty$, the number of cubic fields of discriminant D is $\leq |D|^{1/3+o(1)}$.

It follows that

$$B < x^{1/2+1/500+1/3+o(1)},$$

which is eventually smaller than $x^{0.84}$. This completes the proof of Claim #2 and so also the theorem.

- The GRH-conditional results are simpler. Indeed, under GRH, the least prime with a given splitting type is $\ll (\log |D_K|)^2$ (effective Chebotarev). So primes $> (\log x)^{1000}$ make **no contribution**. So we only need the Taniguchi–Thorne/Bhargava-Shankar-Tsimerman results.

Thank you!