The First Prime in the Chebotarev Theorem

Andrew Fiori

University of Lethbridge

April 20, 2019

Talk Plan

1. Vague overview of the conjectures.
2. Vague overview of my results.
3. Vague overview of why they may be useful.
4. More explicit description of what all the words mean. I want you to see where the definitions are going before we explain them.
5. A more detailed description of my results.

The Chebotarev Theorem

The Chebotarev theorem roughly tells us that:

- if L/K is a degree n Galois extension with Galois group Γ.
- if $\sigma \in \Gamma$ is any element of the Galois group.
- That it we pick a random prime $\mathfrak{p}$ of K, (according to the natural density of K, among primes of size at most X).
- Then pick a random prime $\mathcal{P}|\mathfrak{p}$ of L.

Then the probability that

$$\mathrm{Frob}_{\mathcal{P}} = \sigma$$

is roughly $1/n$, and the roughly converges as $X \to \infty$.

The rate of convergence is controlled by L-functions and GRH-implies it is *fast*.

The way to think of this, is that picking a prime this way is like rolling an n-sided dice to see which σ comes.

The smallest prime

Most people don't actually believe that choosing the first prime is a random number, nor the second, nor the first hundred, nor the first thousand.

But if picking the first m primes is random, how large should the smallest prime such that

$$\mathrm{Frob}_{\mathcal{P}} = \sigma$$

be?

n

At what value m, would you expect to have seen each $\sigma \in \mathrm{Gal}(L/K)$?

$$m \sim n\log(n)$$

(asymptotically as $n \to \infty$, you can be far more precise.)

Of course there are infinitely many fields, and our expectations may not always be met, but still, if we have looked at D fields, how many exterme outliers can we have seen?

Conjectures (and theorems)

Vague Conjecture

For any Galois extension L/K of fields, and any element $\sigma \in \Gamma$, the **first** (unramified degree one) prime $\mathfrak{p}$ of K for which there is a prime $\mathcal{P}|\mathfrak{p}$ of L with $\mathrm{Frob}_{\mathcal{P}} = \sigma$ should be *small* relative to $|d_L|$, the absolute discriminant of L.

What does *small* mean:?

- if you believe GRH, then small should mean $\ll (\log |d_L|)^2$, this was proven by Lagarious and Odlyzko.
- if you don't believe GRH, then small perhaps means $< d_L^{16}$ for d_L sufficiently large (Kadiri, Ng, Wong), or $\ll |d_L|^{12577}$ for all L (Ahn and Kwon).

It is worth mentioning that $n \ll \log |d_L|$. More specifically, there are only finitely many fields with $n > \frac{1}{4\pi e^{\gamma} - \epsilon} \log(\mathrm{d_L})$. ($4\pi e^{\gamma} \sim 22$, if you believe GRH, this result can be improved by a factor of 2.)

As a consequence, other more precise conjectures are natural, for example $n \log |d_L|$, or even $|\Gamma| \log |d_L|$, (but not n^2!)

One way to think about the role of the discriminant is that it controls how many times you have repeated the experiment.

What have I been doing?

I have been doing calculations trying to find the truth, literally finding the smallest prime for all fields L with $|d_L| < 1.5 \cdot 10^6$ and looking at the formulas trying to figure out which one fits.

Why?

- There are a lot of conjectures, and no one has really checked if they are even reasonable.
- You can't use standard method to rule out unexpected luck for low discriminant fields.
- The best asymptotics may simply *not be true* for low degree fields as a non-asymptotic result.
- Even if they are true, it may not be for exactly the same reason, as proofs about asymptotics often involve ignoring terms. These may still be important for low discriminant fields.

A simple example to justify explicit checks for d_L small?

Consider $d_L = -3$ (which happens for exactly one field, $\mathbb{Q}(\sqrt{-3})$), it is simply not possible that for both automorphisms

$$\sqrt{-3} \mapsto \sqrt{-3} \qquad \sqrt{-3} \mapsto -\sqrt{-3}$$

we can find an unramified prime less than 3.

The smallest prime for which

$$\mathrm{Frob}_p \leftrightarrow \sqrt{-3} \mapsto \sqrt{-3}$$

turns out to be 7.

And 7 is fairly large relative to 3.

The larger problem is that asymptotic formulas like

$$d_L^{\epsilon} \qquad (\log |d_L|)^2 \qquad \left(\frac{\log |d_L| \log\log\log |d_L|}{\log\log |d_L|} \right)^2$$

are unreasonable to apply to fields with small discriminant, and the techniques that give them may involve terms which do not decay until d_L is large.

Luckily, there are only finitely many fields with any given discriminant, so we can rule out the bad behavior by just checking for all fields up to some bound, then use lower bounds on d_L in our asymptotic result proofs to obtain unconditional results.

Summary of the results:
There are three fields with $d_L < 1.5 \cdot 10^6$, where the smallest prime was larger than $|d_L|$, they are

$$\mathbb{Q}(\sqrt{-3}) \qquad \mathbb{Q}(\sqrt{-1}) \qquad \mathbb{Q}(\sqrt{5})$$

the unique fields of absolute discriminant $3, 4, 5$. (There are no fields with discriminant 2, only $\mathbb{Q}$ has discriminant 1).

I also found some hints about the true answer.

By GRH you can't expect the result to be much worse than $\log(d_L)^2$, however I have shown you can't expect it to be much better than $\log(d_L)^2$ either.

That is to say, I found the first traces of a large infinite family that gets close. (Then proved the family is an infinite family)

Theorem (F)
There exists an infinite family of fields L, Galois over $\mathbb{Q}$, such that the smallest unramified prime with

$$\mathrm{Frob}_p = \mathrm{Id}$$

is at least

$$(1 + o(1)) \left(\frac{3e^\gamma}{2\pi}\right)^2 \left(\frac{\log|d_L| \log(2 \log\log|d_L|)}{\log\log|d_L|}\right)^2$$

as $d_L \to \infty$.

I would like to emphasise that I never would have randomly guessed at the family that gave it if I hadn't noticed 3 exceptional fields in the data.

Concretely/computationally, what do these things mean?

- What are fields L/K?
  To specify L just give an irreducible rational polynomial $P(x) \in \mathbb{Q}[x]$, then $L = \mathbb{Q}[x]/(P(x))$.
- What is an element of the Galois group?
  To specify $\sigma \in \Gamma$, just give a polynomial $A(x) \in \mathbb{Q}[x]$ such that $P(A(x)) = 0 \pmod{P(x)}$.
- What is an ideal $\mathcal{P}$ of L over p?
  *To give an ideal is to give an irreducible factor of $P(x) \pmod{p}$, so if we write
  $$P(x) = P_1(x) \cdots P_r(x) \pmod{p}$$
  with P_i irreducible, then $\mathcal{P}|p \leftrightarrow P_i(x)$.
- What is Frobenius?
  Frobenius** at a prime $\mathcal{P}|\mathfrak{p}$ is the map: $x \mapsto x^p \pmod{\mathcal{P}}$.
- How do you check if $A(x) = \mathrm{Frob}_{P_i}$?
  We check if it is true that
  $$x^p = A(x) \pmod{p, P_i(x)}$$

*technicalities arise if p divides $Disc(P)$ or a denominator in P
** the Frobenius for a degree one prime $\mathfrak{p}$.

The above understanding basically tells us how do the check for all fields of small discriminant.

- We get a list of such fields (from Jones-Roberts database, or generate our own).
- We compute all the automorphisms by asking gp-pari.
- We search for the smallest prime satisfying the conditions on the previous slide*.

*with modifications to handle the case $p|\mathrm{Disc}(\mathrm{P})$ but $p \not| d_L$.
**we also need to explain why we are ignoring the role of K.
But basically by only considering $x \mapsto x^p$, we cover the subfields K of L^σ, which are those where primes $\mathfrak{p}$ between p and $\mathcal{P}$ will be degree 1, at the same time.

Some concrete examples

The irreducible polynomial

$$x^3 - x^2 - 2x + 1$$

describes a degree 3 field. The discriminant of the polynomial is 49.
anyone know which field this is, and why it is smallest example?
The polynomials

$$x \mapsto x \qquad x \mapsto -x^2 + 2 \qquad x \mapsto x^2 - x - 1$$

describe three automorphisms, of this field.
The polynomial $x^3 - x^2 - 2x + 1$ is irreducible mod 2 and 3 and notice

$$-x^2 + 2 = x^2 \pmod{2, x^3 - x^2 - 2x + 1}$$
$$x^2 - x - 1 = x^3 \pmod{3, x^3 - x^2 - 2x + 1}$$

The smallest prime where $x^3 - x^2 - 2x + 1$ is not irreducible is 13 and we have

$$x^3 - x^2 - 2x + 1 = (x - 3)(x - 5)(x - 6) \pmod{13}$$

and it isn't too surprising that

$$x^{13} = x \pmod{x - 3, 13}$$

All of $2, 3, 13$ are much smaller than 49. $(ln(49)^2 = 15.14...)$

The polynomial

$$x^4 - x^3 - x^2 + x + 1$$

defines a degree 4 field with discriminant 117, it has a quadratic subfield (which? $\mathbb{Q}(\sqrt{-3})$ of course).
We have automorphisms

$$x \mapsto x \qquad x \mapsto x^3 - x^2 - x + 1$$

The defining polynomial is irreducible mod 2 and 5 (so can't see Frobenius over any degree one primes!!), and is ramified at 3.
The smallest degree where we can find a degree one prime is 7, and we have

$$x^4 - x^3 - x^2 + x + 1 = (x+5)(x+4)(x^2+4x+6) \pmod 7$$

and we can *"see"* that

$$x^7 = x^3 - x^2 - x + 1 \pmod{7, x^2+4x+6}$$

and that

$$x^7 = x \pmod{7, x+5}$$

and 7 is small relative to 117 ($\log(117)^2 = 22.678...$).

The polynomial

$$x^2 - x - 41$$

defines a quadratic field with discriminant -163.
We have automorphisms

$$x \mapsto x \qquad x \mapsto 1 - x$$

The polynomial is irreducible for all primes up to 37, but at 41 we have:

$$x^2 - x - 41 = (x - 1)x \pmod{41}$$

41 is fairly large in comparison to 163 ($\log(163)^2 = 25.94...$). Why is this field special?
(By the way this is one of only a handfull of examples where we beat the $\log(d_L)^2$ bound).

Fun fact/answer/**Corollary** (F)
If p is prime, then p is the first split prime in the Hilbert class field of

$$\mathbb{Q}(\sqrt{1 - 4p}).$$

Low Degree Family

Theorem* (I have only written detailed proof for $K = \mathbb{Q}$)
For any field K, there are infinitely many quadratic extensions L/K, such that the smallest degree one prime of K which splits/is inert in K is at least $(1 - o(d_L)) \log |d_L|$.
The family is (with modifications if the product of primes below is not principal) for each value $N \in \mathbb{N}$

$$L_N = K\left(\sqrt{\prod_{\substack{N(\mathfrak{p})<N \\ \text{degree 1}}} \mathfrak{p}}\right)$$

we have that L/K is ramified at all degree one primes less than N, so these do not give Frobenius.

The discriminant of L_N satisfies

$$\log |D_{L_N}| < \log |D_K| + \sum_{N(\mathfrak{p})<N} \log |N(\mathfrak{p})| \sim N$$

This is both weaker/stronger than the other result which involved having the degree of the extensions go to ∞ but had a stronger lower bound.

It is worth pointing out that this construction can be modified, and one gets a Heuristic which suggests a slightly larger bound.

Heuristic*

You can build off this a heuristic which suggests that for quadratic fields L over a fixed K

$$\limsup_{d_L \to \infty} \text{ smallest } p = E \log |d_L|$$

for some E larger than 1.5.

* it is likely these results are already *"known"* in some contexts.

Higher Bound Family

Theorem (F)
Consider the family of Hilbert class fields $L = H_K$ for K a quadratic imaginary field. Then (unconditionally)

$$\limsup_{d_L \to \infty} (\text{smallest split } p) \geq \left(\frac{3e^\gamma}{2\pi}\right)^2 \left(\frac{\log|d_L| \log\log\log|d_L|}{\log\log|d_L|}\right)^2$$

and (if you believe GRH) then

$$\limsup_{d_L \to \infty} (\text{smallest split } p) \leq \left(\frac{3e^\gamma}{\pi}\right)^2 \left(\frac{\log|d_L| \log\log\log|d_L|}{\log\log|d_L|}\right)^2.$$

If p splits in H_K then

- p splits in K as $(p) = \mathfrak{p}_1\mathfrak{p}_2$ and hence $N_K(\mathfrak{p}_i) = p$.
- and $\mathfrak{p}_i$ splits in H_K, and hence $\mathrm{Frob}_{\mathfrak{p}_i} = 1$ and hence, $\mathfrak{p}_i$ is principal.
- if $\mathfrak{p}_i = (x + y\sqrt{d_K})$ is principal, then $p = N_K(x + y\sqrt{d_K}) = x^2 + y^2 d_K$, but then $p \geq d_K/4$.

Now because $\log|d_L| = h_K \log|d_K|$ being careless with $h_K \sim \sqrt{d_K}$ easily gives the bound $(\log|d_L|)^{2-\epsilon}$.
Being move careful gives the exact one above.

The End.