Chebotarev and Cool Applications

Abstract. A small note on a really cool theorem and some sweet corollaries. The goal here will be to answer the following question: Given a prime p and an irreducible polynomial $f(x)$, how likely is it that there exists some $n \in \mathbb{N}$ s.t. $p|f(n)$?

1 Chebotarev

To start of this small note, we start with a quick look at one of the most famous theorems in number theory (whose fame stretches well outside of number theory):

Theorem 1 (Dirichlet's theorem on primes in arithmetic progression). *Given a, m with $\gcd(a, m) = 1$, the ratios*

$$\lim_{x\to\infty} \frac{|\{p \le x \mid p \text{ prime}, p \equiv a \pmod{m}\}|}{|\{p \le x \mid p \text{ prime}\}|} = \frac{1}{\phi(m)}$$

Here, its clear that if $\gcd a, m > 1$ then there is at most one prime in the set in the numerator. So another way to see the theorem above is that the representatives of all primes is normally distributed in in $(\mathbb{Z}/m\mathbb{Z})^\times$, ignoring those primes that divide m.

Chebotarev's density theorem is a celebrated generalization of Dirichlet's theorem. It is a bit complicated to state, so we will need some preliminaries. The theorem is related to Frobenius elements of primes, so we start by defining those.

From here on out, K is a Galois extension of $\mathbb{Q}$ (not just a numberfield!), p is a prime in $\mathbb{Q}$, and $\mathfrak{p}$ is a prime ideal K, with $\mathfrak{p}|(p)$ in $\mathcal{O}_K$. We know that in $\mathcal{O}_K$, $(p) = \prod_i \mathfrak{p}_i$, and that $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the primes dividing p, i.e. for any i, j, there exists some $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ with $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$. Given a prime $\mathfrak{p}$, we denote the subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ that fixes $\mathfrak{p}$ as

$$D_\mathfrak{p} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

Given a prime ideal $\mathfrak{p} \mid (p)$, we know that $\mathcal{O}_K/\mathfrak{p}$ is a finite field and infact a field extension of $\mathbb{Z}/(p)$. Since every automorphism of $D_\mathfrak{p}$ fixes $\mathfrak{p}$ by definition, it is clear that we can restrict $\sigma \in D_\mathfrak{p}$ to an automorphism of $\mathcal{O}_K/\mathfrak{p}$ as $\sigma(a + \mathfrak{p}) = \sigma(a) + \sigma(\mathfrak{p}) = \sigma(a) + \mathfrak{p}$. Further, any automorphism of $D_\mathfrak{p} < \mathrm{Gal}(K/\mathbb{Q})$ fixes $\mathbb{Z} \in \mathbb{Q}$, so the restriction above gives a homomorphism of galois groups:

$$D_\mathfrak{p} \to \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} \;/\; \mathbb{Z}/(p))$$

To define Frobenius elements of primes $\mathfrak{p}$, we need the following lemma:

Lemma 1. *The homomorphism $D_\mathfrak{p} \to \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} \;/\; \mathbb{Z}/(p))$ is surjective.*

Now, since $\mathcal{O}_K/\mathfrak{p} \supset \mathbb{Z}/(p)$ is a finite field extension, we know that $\mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} \;/\; \mathbb{Z}/(p))$ is generated by the p-power map, and because of the lemma above, we know that there are elements of $D_\mathfrak{p}$ which acts as the p-power map on $\mathcal{O}_K/\mathfrak{p}$. If we additionally require that p is unramified in K, which happens for all but a finite number of primes, this choice is unique[1]. We are finally ready to define frobenius elements:

[1] This is because the inertia group is trivial whenever p is unramified, where the inertia group is pretty much defined to be the kernel of the map $D_\mathfrak{p} \to \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} \;/\; \mathbb{Z}/(p))$

Definition 1 (Frobenius elements of $\mathfrak{p}$). *Given a prime $\mathfrak{p}|(p)$, where p is unramified in K, the frobenious element related to $\mathfrak{p}$ is the unique element of* $\mathrm{Gal}(K/\mathbb{Q})$ *satisfying*

$$\mathrm{Frob}_{\mathfrak{p}}(a) \equiv a^p \pmod{\mathfrak{p}}$$

for all $a \in \mathcal{O}_K$.

We are almost ready to state Chebotarev's density theorem. We have defined frobenius elements of primes $\mathfrak{p} \subset \mathcal{O}_K$, but to state the theorem, we need to define frobenius elements of $p \in \mathbb{Z}$. To do this we try to define $\mathrm{Frob}_p = \mathrm{Frob}_{\mathfrak{p}}$ for any $\mathfrak{p}|(p)$. This turns out to be a perfectly valid definition if $\mathrm{Gal}(K/\mathbb{Q})$ is abelian. And in the non-abelian case, its almost as good: While this element is no longer unique, it is unique up to conjugacy. To see this, notice that if $\mathfrak{p}_i, \mathfrak{p}_j$ are primes dividing (p), their frobenius elements are conjugates. This is because there exists some element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ with $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$. Then we get

$$\begin{aligned}
&\sigma \circ \mathrm{Frob}_{\mathfrak{p}_i} \circ \sigma^{-1}(a + \mathfrak{p}_j) = \\
&\sigma \circ \mathrm{Frob}_{\mathfrak{p}_i}(\sigma^{-1}(a) + \mathfrak{p}_i) = \\
&\sigma(\sigma^{-1}(a)^p + \mathfrak{p}_i) = \sigma(\sigma^{-1}(a))^p + \mathfrak{p}_j = a^p + \mathfrak{p}_j
\end{aligned}$$

Hence, we can create the following definition.

Definition 2 (Frobenius elements of p). *Given a prime $p \in \mathbb{Z}$, where p is unramified in K, the frobenious element related to p is*

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

where C is the conjugacy class of $\mathrm{Frob}_{\mathfrak{p}}$ *in* $\mathrm{Gal}(K/\mathbb{Q})$*, where $\mathfrak{p}$ is any prime in $\mathcal{O}_K$ dividng (p).*

Clearly the definition above is also dependent on K, but K will typically be clear from context.

Finally, we can state chebotarevs density theorem:

Theorem 2 (Chebotarev's denisty theorem). *Given a galois extension $K \supset \mathbb{Q}$, and a conjugacy class $C \subset \mathrm{Gal}(K/\mathbb{Q})$, the ratio*

$$\lim_{x \to \infty} \frac{|\{p \leq x \mid p \text{ prime}, \mathrm{Frob}_p = C\}|}{|\{p \leq x \mid p \text{ prime}\}|} = \frac{|C|}{|\mathrm{Gal}(K/\mathbb{Q})|}$$

If $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, then this theorem simplifies, since then as noted, Frob_p is actually unique, because all the conjugacy classes have size 1. If we additionally take $K = \mathbb{Q}(\omega)$, where $\omega^m = 1, \omega^n \neq 1, n < m$, then this exactly reduces to Dirichlet's theorem. This is not immidiately obvious, but comes from the isomorphism $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ given by

$$\begin{aligned}
\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) &\to (\mathbb{Z}/m\mathbb{Z})^\times \\
\sigma(\omega) = \omega^a &\to a
\end{aligned}$$

Finally, we note that everything written here can be changed to having some arbitrary number-field as a base field, and nothing really changes (only that all the results become more complicated to state).

2 Cool Consequences

Although Chebotarev seems like quite an abstract generalization of Dirichlet's theorem, we now take it show some much more "down to earth" consequences of this theorem. We can relate Chebotarev's density theorem to a closely related theorem by Dedekind, and get a pretty cool result that says something about how polynomials factors modulo primes.

Theorem 3 (Dedekind). *Let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial, K its splitting field and p some prime with $p \nmid \mathrm{disc}(f)$. Then $f \equiv \pi_1 \dots \pi_r \pmod{p}$ for distinct, irreducible π_i. Further, for some $\mathfrak{p}|(p)$ in $\mathcal{O}_K$,* $\mathrm{Frob}_{\mathfrak{p}}$ *acts on the roots of f with cycle type $d_1 + \dots + d_r$, where $d_i = \deg(\pi_i)$.*

Together with Chebotarev, which states that Frob_p across all primes p are normally distributed over the conjugacy classes of $\text{Gal}(K/\mathbb{Q})$, weighted by the size of the conjugacy class, we can related information about $\text{Gal}(K/\mathbb{Q})$ to how the polynomial factors modulo various primes! This even works both ways, i.e. if we know about $\text{Gal}(K/\mathbb{Q})$, we can say something about how f factors modulo various primes, or if we want to know about $\text{Gal}(K/\mathbb{Q})$, we can get this information by studying f modulo primes.

One cool example of this is that we can calculate the ratio

$$\lim_{x\to\infty} \frac{|\{p \leq x \mid p \text{ prime}, f \text{ splits completely modulo } p\}|}{|\{p \leq x \mid p \text{ prime}\}|}$$

By Dedekind, this corresponds to primes where Frob_p is the identity element (or equivalently, primes which split completely), and by Chebotarev, this ratio should be $\frac{1}{|\text{Gal}(K/\mathbb{Q})|}$. In other words, as $\lim x \to \infty$, we get a better and better approximation of the size of the galois group!

Another example going the other direction (answering the question raised in the abstract), i.e. using information about the galois group to say something about f modulo p, is the following: Suppose we want to answer the following question: What ratio of primes can divide $f(n)$? Here, we say that a prime p can divide $f(n)$ if $p \mid f(n)$ for some $n \in \mathbb{N}$. To answer this we start with the observation that p can divinde $f(n)$ if and only if f is reducible modulo p. By Dedekind, this corresponds to Frobenius elements that fixes at least one root. So to answer the question, Chebotarev tells us that the ratio of primes that can divide $f(n)$ is equal to

$$\frac{\sum_i |C_i|}{|\text{Gal}(K/\mathbb{Q})|},$$

where the sum is over all conjugacy classes fixing at least one element. Some of this is summarized in an example in Table 2.

$f(X))$	$X^3 - 3X + 1$	$X^3 + 2$
$\text{Gal}(K/\mathbb{Q})$	C_3	S_3
Conjugacy Classes	$\{()\}, \{(123), (132)\}$	$\{()\}, \{(123), (132)\}, \{(23), (12), (13)\}$
$\frac{\lvert\{p\leq 7928 \mid p \text{ prime}, f \text{ splits completely modulo } p\}\rvert}{\lvert\{p\leq 7928 \mid p \text{ prime}\}\rvert}$	$\frac{334}{1000}$	$\frac{156}{1000}$
Primes (out of the first 1000) dividing $f(n)$	334	665

Table 1. Some numerical examples

For $f(X) = X^3 - 3X + 1$, the primes dividing f coincide with the ones where f split completely, but this is clearly not true in general, see for instance $f(X) = X^3 + 2$.