Counting irreducible divisors and irreducibles in progressions

Lee Troupe[1]
joint w/ Paul Pollack[2]

[1]University of British Columbia

[2]University of Georgia

Alberta Number Theory Days
2017

Let K be a number field with ring of integers $\mathbb{Z}_K$.

Every nonzero, nonunit $\alpha \in \mathbb{Z}_K$ is equal to a product of irreducible elements of $\mathbb{Z}_K$.

Question: Is this factorization unique?

Let K be a number field with ring of integers $\mathbb{Z}_K$.

Every nonzero, nonunit $\alpha \in \mathbb{Z}_K$ is equal to a product of irreducible elements of $\mathbb{Z}_K$.

Question: Is this factorization unique?

Example

- *Let $K = \mathbb{Q}$. Every $n \in \mathbb{Z}$ is equal to a unique product of prime numbers.*

Let K be a number field with ring of integers $\mathbb{Z}_K$.

Every nonzero, nonunit $\alpha \in \mathbb{Z}_K$ is equal to a product of irreducible elements of $\mathbb{Z}_K$.

Question: Is this factorization unique?

Example

- *Let $K = \mathbb{Q}$. Every $n \in \mathbb{Z}$ is equal to a unique product of prime numbers.*
- *Let $K = \mathbb{Q}(\sqrt{-5})$, with ring of integers $\mathbb{Z}_K$. In $\mathbb{Z}_K$,*

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Answer: No, not necessarily.

More questions: When is it unique? What can we say about it when it isn't unique?

Measuring the failure of unique factorization

Let

- $\mathcal{I}(K) = \{\text{fractional ideals of } K\}$
- $\operatorname{Prin}(K) = \{\text{principal fractional ideals of } K\}$.

$H(K) := \mathcal{I}(K)/\operatorname{Prin}(K)$ is called the *class group* of K.

Let $h_K := \#H(K)$ denote the class number of K.

Note: h_K is finite, for any number field K.

Measuring the failure of unique factorization

Let

- $\mathcal{I}(K) = \{\text{fractional ideals of } K\}$
- $\text{Prin}(K) = \{\text{principal fractional ideals of } K\}$.

$H(K) := \mathcal{I}(K)/\text{Prin}(K)$ is called the *class group* of K.

Let $h_K := \#H(K)$ denote the class number of K.

Note: h_K is finite, for any number field K.

Theorem

$h_K = 1 \iff \mathbb{Z}_K$ is a PID $\iff \mathbb{Z}_K$ is a UFD.

Measuring the failure of unique factorization

Theorem (Carlitz 1960)

$\mathbb{Z}_K$ is not a UFD, and every factorization of $\alpha \in \mathbb{Z}_K$ into irreducibles has the same length $\iff h_K = 2$.

Measuring the failure of unique factorization

For an principal ideal $I \subset \mathbb{Z}_K$, define

$$\mathcal{L}(I) := \{n \in \mathbb{N} : \begin{array}{c} I \text{ has a length } n \text{ factorization into} \\ \text{irreducible principal ideals} \end{array}\}.$$

$\mathcal{L}(I)$ is called the *length spectrum* of I.

Measuring the failure of unique factorization

For an principal ideal $I \subset \mathbb{Z}_K$, define

$$\mathcal{L}(I) := \{n \in \mathbb{N} : \begin{array}{c} I \text{ has a length } n \text{ factorization into} \\ \text{irreducible principal ideals} \end{array}\}.$$

$\mathcal{L}(I)$ is called the *length spectrum* of I.

Also, define

$$\rho_K := \sup_{\substack{I \in \mathrm{Prin}(\mathbb{Z}_K) \\ m,n \in \mathcal{L}(I)}} \frac{m}{n}.$$

ρ_K is called the *elasticity* of $\mathbb{Z}_K$.

Measuring the failure of unique factorization

The *Davenport constant* $D(G)$ of a finite abelian group G is smallest number such that every length $D(G)$ sequence of elements of G has a nonempty subsequence that sums to 0.

Example: $G = \mathbb{Z}/p\mathbb{Z}$. Then $D(G) = p$. (In general, $D(G) \leq \#G$.)

Fact: $D(G) \to \infty$ as $\#G \to \infty$.

Measuring the failure of unique factorization

The *Davenport constant* $D(G)$ of a finite abelian group G is smallest number such that every length $D(G)$ sequence of elements of G has a nonempty subsequence that sums to 0.

Example: $G = \mathbb{Z}/p\mathbb{Z}$. Then $D(G) = p$. (In general, $D(G) \leq \#G$.)

Fact: $D(G) \to \infty$ as $\#G \to \infty$.

Theorem (Valenza 1980; Steffan 1986)

$\rho_K = \frac{1}{2} D(H(K))$.

Counting irreducible divisors

Let $\nu(\alpha)$ denote the number of pairwise nonassociate irreducible divisors of $\alpha \in \mathbb{Z}_K$.

For example, let $K = \mathbb{Q}(\sqrt{-5})$. Then $\nu(6) = 4$, since $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Counting irreducible divisors

Let $\nu(\alpha)$ denote the number of pairwise nonassociate irreducible divisors of $\alpha \in \mathbb{Z}_K$.

For example, let $K = \mathbb{Q}(\sqrt{-5})$. Then $\nu(6) = 4$, since $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Theorem (Pollack)

The quantity $\nu(\alpha)$ has a normal distribution with mean $A(\log\log|N(\alpha)|)^D$ and standard deviation $B(\log\log|N(\alpha)|)^{D-\frac{1}{2}}$, where A and B are positive constants depending on K and D is the Davenport constant of $H(K)$.

Maximal order of $\nu(\alpha)$

Theorem (Pollack, T)

We have

$$\max\{\nu(\alpha) : |N(\alpha)| \leq x\} = (M_K + o(1))\left(\frac{\log x}{h_K \log\log x}\right)^D,$$

where M_K is a positive constant depending only on K and D is the Davenport constant of the class group $H(K)$.

Counting irreducibles

Theorem (Rémond 1966)

Let $F(x)$ denote the number of pairwise nonassociate irreducible elements of $\mathbb{Z}_K$ with norm up to x in absolute value. Then

$$F(x) \sim C_K \frac{D}{h_K^D} \frac{x}{\log x} (\log \log x)^{D-1},$$

where D is the Davenport constant of $H(K)$, and C_K is a constant depending only on K.

Counting irreducibles

Theorem (Rémond 1966)

Let $F(x)$ denote the number of pairwise nonassociate irreducible elements of $\mathbb{Z}_K$ with norm up to x in absolute value. Then

$$F(x) \sim C_K \frac{D}{h_K^D} \frac{x}{\log x} (\log \log x)^{D-1},$$

where D is the Davenport constant of $H(K)$, and C_K is a constant depending only on K.

There is a formula for the constant C_K, in terms of the structure of the class groups of K. When $K = \mathbb{Q}$, we have $C_K = 1$, and we recover the prime number theorem:

$$\pi(x) \sim \frac{x}{\log x}.$$

Irreducibles in arithmetic progressions

Theorem (Pollack, T)

Let $\mathfrak{m}$ *be a nonzero ideal of* $\mathbb{Z}_K$*, and let* $\alpha \in \mathbb{Z}_K$ *be a nonzero element such that* (α) *and* $\mathfrak{m}$ *have no prime ideal factors in common. Then the number of irreducibles* $\pi \equiv \alpha \pmod{\mathfrak{m}}$*, with* $\pi/\alpha \gg 0$*, of norm at most* x *in absolute value is asymptotic to*

$$\frac{1}{\Phi(\mathfrak{m})} C_K \frac{D}{h_K^D} \frac{x}{\log x} (\log\log x)^{D-1},$$

where D *is the Davenport constant of* $H(K)$*,* $\Phi(\mathfrak{m})$ *is the analogue of Euler's totient function in this setting, and* C_K *is the same as in Rémond's theorem.*

Irreducibles in arithmetic progressions

Theorem (Pollack, T)

Let $\mathfrak{m}$ *be a nonzero ideal of* $\mathbb{Z}_K$*, and let* $\alpha \in \mathbb{Z}_K$ *be a nonzero element such that* (α) *and* $\mathfrak{m}$ *have no prime ideal factors in common. Then the number of irreducibles* $\pi \equiv \alpha \pmod{\mathfrak{m}}$*, with* $\pi/\alpha \gg 0$*, of norm at most* x *in absolute value is asymptotic to*

$$\frac{1}{\Phi(\mathfrak{m})} C_K \frac{D}{h_K^D} \frac{x}{\log x} (\log\log x)^{D-1},$$

where D *is the Davenport constant of* $H(K)$*,* $\Phi(\mathfrak{m})$ *is the analogue of Euler's totient function in this setting, and* C_K *is the same as in Rémond's theorem.*

Remark:

- Suppose $G := ((\alpha), \mathfrak{m})$ is a product of prime ideals with no principal subproduct. Then there are still infinitely many irreducibles $\pi \equiv \alpha \pmod{\mathfrak{m}}$, and we can count them!

Types of ideals and elements

Write $H(K) = \{C_1, \ldots, C_h\}$ (so $h = h_K$).

Let $A \subset \mathbb{Z}_K$ a nonzero ideal. We say A is *of type* $\tau = (t_1, \ldots, t_h)$ if the (unique) prime factorization of A into prime ideals has t_i factors from the ideal class C_i.

So a *type* is just an h-tuple of nonnegative integers.

Types of ideals and elements

Write $H(K) = \{C_1, \ldots, C_h\}$ (so $h = h_K$).

Let $A \subset \mathbb{Z}_K$ a nonzero ideal. We say A is *of type* $\tau = (t_1, \ldots, t_h)$ if the (unique) prime factorization of A into prime ideals has t_i factors from the ideal class C_i.

So a *type* is just an h-tuple of nonnegative integers.

An element $\alpha \in \mathbb{Z}_K$ is of type τ when (α) is of type τ.

The *length* of $\tau = (t_1, \ldots, t_h)$ is $t_1 + \cdots + t_h$, denoted $\ell(\tau)$.

Irreducible types

Let $\pi \in \mathbb{Z}_K$ be irreducible. Write

$$(\pi) = \mathfrak{p}_1 \cdots \mathfrak{p}_\ell.$$

π irreducible $\implies$ no subproduct of the $\mathfrak{p}_i$ is principal.

We say a type $\tau = (t_1, \ldots, t_h)$ is *irreducible* if, in the class group, $C_1^{t_1} \cdots C_h^{t_h}$ is trivial, while no proper subproduct of the C_is is trivial.

Irreducible types

Let $\pi \in \mathbb{Z}_K$ be irreducible. Write

$$(\pi) = \mathfrak{p}_1 \cdots \mathfrak{p}_\ell.$$

π irreducible $\implies$ no subproduct of the $\mathfrak{p}_i$ is principal.

We say a type $\tau = (t_1, \ldots, t_h)$ is *irreducible* if, in the class group, $C_1^{t_1} \cdots C_h^{t_h}$ is trivial, while no proper subproduct of the C_is is trivial.

Every irreducible $\pi \in \mathbb{Z}_K$ has an irreducible type. Conversely, every irreducible type is represented by an irreducible element, since (Landau) every ideal class contains a prime ideal.

Finally: A type τ is *maximal* if τ is irreducible and $\ell(\tau) = D(H(K))$.

Maximal order of $\nu(\alpha)$

Theorem (Pollack, T)

We have

$$\max\{\nu(\alpha) : |N(\alpha)| \leq x\} = (M_K + o(1))\left(\frac{\log x}{h_K \log\log x}\right)^D,$$

where M_K is a positive constant depending only on K and D is the Davenport constant of the class group $H(K)$.

Proof: What is M_K?

Define a polynomial

$$P(x_1, \ldots, x_h) = \sum_{\tau \text{ maximal}} \prod_{i=1}^{h} \frac{x^{t_i}}{t_i!}.$$

Proof: What is M_K?

Define a polynomial

$$P(x_1, \ldots, x_h) = \sum_{\tau \text{ maximal}} \prod_{i=1}^{h} \frac{x^{t_i}}{t_i!}.$$

Let M_K denote the maximum value achieved by this polynomial on the simplex

$$S = \{(x_1, \ldots, x_h) : x_i \geq 0, \sum_{i=1}^{h} x_i \leq h\}.$$

Proof: What is M_K?

Define a polynomial

$$P(x_1, \ldots, x_h) = \sum_{\tau \text{ maximal}} \prod_{i=1}^{h} \frac{x^{t_i}}{t_i!}.$$

Let M_K denote the maximum value achieved by this polynomial on the simplex

$$S = \{(x_1, \ldots, x_h) : x_i \geq 0, \sum_{i=1}^{h} x_i \leq h\}.$$

Let $(\gamma_1, \ldots, \gamma_h) \in S$ be a point at which P achieves the value M_K.

Proof: What is M_K?

Define a polynomial

$$P(x_1, \ldots, x_h) = \sum_{\tau \text{ maximal}} \prod_{i=1}^{h} \frac{x^{t_i}}{t_i!}.$$

Let M_K denote the maximum value achieved by this polynomial on the simplex

$$S = \{(x_1, \ldots, x_h) : x_i \geq 0, \sum_{i=1}^{h} x_i \leq h\}.$$

Let $(\gamma_1, \ldots, \gamma_h) \in S$ be a point at which P achieves the value M_K.

Example: If $H(K) \simeq \mathbb{Z}/3\mathbb{Z}$, the maximal types are $(0, 3, 0)$ and $(0, 0, 3)$. So $P(x_1, x_2, x_3) = \frac{1}{3!}(x_2^3 + x_3^3)$, a choice of $(\gamma_1, \gamma_2, \gamma_3) = (0, 3, 0)$, and $M_K = \frac{1}{3!}3^3$.

Proof sketch

Key input:

Theorem (Landau 1907)

Let $C_i \in H(K)$*, and let* $\pi_i(x)$ *denote the count of prime ideals* $\mathfrak{p} \in C_i$ *with* $N(\mathfrak{p}) \leq x$*. Then*

$$\pi_i(x) = \left(\frac{1}{h} + o(1)\right)\frac{x}{\log x}.$$

Proof sketch

Key input:

Theorem (Landau 1907)

Let $C_i \in H(K)$, and let $\pi_i(x)$ denote the count of prime ideals $\mathfrak{p} \in C_i$ with $N(\mathfrak{p}) \leq x$. Then

$$\pi_i(x) = \left(\frac{1}{h} + o(1)\right) \frac{x}{\log x}.$$

Strategy: Mimic maximal order proof for $\omega(n)$.

(Let $n = p_1 \cdots p_m$. Then $\log(n) = \sum_{i=1}^{m} \log(p_m) = \psi(p_m) \sim p_m$ and

$$\omega(n) = \pi(p_m) \sim \frac{p_m}{\log p_m} \sim \frac{\log n}{\log \log n},$$

as $n \to \infty$ through primorials.)

Proof sketch

- Let $A = \prod_{i=1}^{h} \prod_{\substack{\mathfrak{p} \in C_i \\ N(\mathfrak{p}) \leq \gamma_i \log x}} \mathfrak{p}$, with γ_i as before
- $N(A) \approx x$

Proof sketch

- Let $A = \prod_{i=1}^{h} \prod_{\substack{\mathfrak{p} \in C_i \\ N(\mathfrak{p}) \le \gamma_i \log x}} \mathfrak{p}$, with γ_i as before
- $N(A) \approx x$
- The number of type $\tau = (t_1, \ldots, t_h)$ principal divisors of A is

$$\prod_{i=1}^{h} \binom{\omega_i(A)}{t_i} \approx \prod_{i=1}^{h} \frac{\omega_i(A)^{t_i}}{t_i!},$$

  where $\omega_i(A)$ is the number of prime ideal divisors of A from the ideal class C_i.

Proof sketch

- Let $A = \prod_{i=1}^{h} \prod_{\substack{\mathfrak{p} \in C_i \\ N(\mathfrak{p}) \le \gamma_i \log x}} \mathfrak{p}$, with γ_i as before
- $N(A) \approx x$
- The number of type $\tau = (t_1, \dots, t_h)$ principal divisors of A is

$$\prod_{i=1}^{h} \binom{\omega_i(A)}{t_i} \approx \prod_{i=1}^{h} \frac{\omega_i(A)^{t_i}}{t_i!},$$

  where $\omega_i(A)$ is the number of prime ideal divisors of A from the ideal class C_i.
- $\omega_i(A) \approx \gamma_i \dfrac{\log x}{h_K \log \log x}$; inserting this into the display above and summing over all maximal types τ, we see that the number of principal divisors of A of irreducible type is

$$\frac{1}{h_K^D} \sum_{\tau \text{ maximal}} \frac{\gamma_i^{t_i}}{t_i!} \left(\frac{\log x}{\log \log x} \right)^D.$$

Counting irreducibles

Theorem (Rémond 1966)

Let $F(x)$ denote the number of pairwise nonassociate irreducible elements of $\mathbb{Z}_K$ with norm up to x in absolute value. Then

$$F(x) \sim \frac{D}{h_K^D} \sum_{\tau \text{ maximal}} \frac{1}{t_1! \cdots t_h!} \frac{x(\log\log x)^{D-1}}{\log x},$$

where D is the Davenport constant of $H(K)$.

Counting irreducibles

Theorem (Rémond 1966)

Let $F(x)$ denote the number of pairwise nonassociate irreducible elements of $\mathbb{Z}_K$ with norm up to x in absolute value. Then

$$F(x) \sim \frac{D}{h_K^D} \sum_{\tau \text{ maximal}} \frac{1}{t_1! \cdots t_h!} \frac{x(\log \log x)^{D-1}}{\log x},$$

where D is the Davenport constant of $H(K)$.

When $K = \mathbb{Q}$, we recover the prime number theorem:

$$\pi(x) \sim \frac{x}{\log x}.$$

Irreducibles in arithmetic progressions

Theorem (Pollack, T)

Let $\mathfrak{m}$ be a nonzero ideal of $\mathbb{Z}_K$, and let $\alpha \in \mathbb{Z}_K$ be a nonzero element such that (α) and $\mathfrak{m}$ have no prime ideal factors in common. Then there are infinitely many irreducible elements π of $\mathbb{Z}_K$ with $\pi \equiv \alpha \pmod{\mathfrak{m}}$, and $\pi/\alpha \gg 0$.

More precisely: The number of principal ideals of norm at most x admitting a generator $\pi \equiv \alpha \pmod{\mathfrak{m}}$ is asymptotic to

$$\frac{1}{\Phi(\mathfrak{m})} \frac{D}{h^D} \sum_{\tau \text{ maximal}} \frac{1}{t_1! \cdots t_h!} \frac{x}{\log x} (\log \log x)^{D-1},$$

where we have written each $\tau = (t_1, \ldots, t_h)$.

Proof sketch: Upper Bound

Suppose π is of type $\tau = (t_1, \ldots, t_h)$. Write $(\pi) = \mathfrak{p}_1 \cdots \mathfrak{p}_D$, and assume $N\mathfrak{p}_D > x^{1-1/\log\log x}$. This discards a negligible number of ideals (π).

Proof sketch: Upper Bound

Suppose π is of type $\tau = (t_1, \ldots, t_h)$. Write $(\pi) = \mathfrak{p}_1 \cdots \mathfrak{p}_D$, and assume $N\mathfrak{p}_D > x^{1-1/\log\log x}$. This discards a negligible number of ideals (π).

Since $\pi \equiv \alpha \pmod{\mathfrak{m}}$, (π) and (α) are equivalent modulo $\mathrm{Prin}^+_{\mathfrak{m}}(K)$, and so represent the same element in $H^+_{\mathfrak{m}}(K)$, the *strict ray class group modulo* $\mathfrak{m}$.

Given $\mathfrak{p}_1 \cdots \mathfrak{p}_{D-1}$, the ray class of $\mathfrak{p}_D$ is that of (α) times the inverse of the class of $\mathfrak{p}_1 \cdots \mathfrak{p}_{D-1}$.

Proof sketch: Upper Bound

Theorem (Landau 1918)

The number of prime ideals of $\mathbb{Z}_K$ of norm up to x belonging to a particular strict ray class modulo $\mathfrak{m}$ is asymptotic to

$$\frac{1}{h_{\mathfrak{m}}^{+}(K)} \frac{x}{\log x}.$$

Proof sketch: Upper Bound

Theorem (Landau 1918)

The number of prime ideals of $\mathbb{Z}_K$ of norm up to x belonging to a particular strict ray class modulo $\mathfrak{m}$ is asymptotic to

$$\frac{1}{h_{\mathfrak{m}}^{+}(K)} \frac{x}{\log x}.$$

The number of possibilities for $\mathfrak{p}_D$ is

$$\sim \frac{1}{h_{\mathfrak{m}}^{+}(K)} \frac{x/N\mathfrak{p}_1 \cdots \mathfrak{p}_{D-1}}{\log(x/N\mathfrak{p}_1 \cdots \mathfrak{p}_{D-1})} \sim \frac{1}{h_{\mathfrak{m}}^{+}(K)} \frac{x/N\mathfrak{p}_1 \cdots \mathfrak{p}_{D-1}}{\log(x)}.$$

- Sum on $\mathfrak{p}_1, \ldots, \mathfrak{p}_{D-1}$
- Estimate this sum with a Mertens-type theorem for strict ray classes, which follows from Landau's theorem and partial summation

But wait, there's more

We say a type τ is maximal with respect to τ' if $\tau' \leq \tau$, τ is irreducible and τ has maximal length among the irreducible types which have τ' as a subtype.

Theorem (Pollack, T)

Let $\alpha \in \mathbb{Z}_K$ such that (α) and $\mathfrak{m}$ have no common principal ideal factor. Let $G = ((\alpha), \mathfrak{m})$, and let τ' be the type of G. Then the number of principal ideals of norm at most x admitting a generator $\pi \equiv \alpha \pmod{\mathfrak{m}}$ is asymptotic to

$$\frac{1}{N(G)\Phi(\mathfrak{m}G^{-1})} \frac{L}{h^L} \sum_{\substack{\tau' \leq \tau \\ \tau \text{ irred.} \\ \tau \text{ max'l w.r.t.} \tau'}} \frac{1}{n_1! \cdots n_h!} \frac{x}{\log x} (\log \log x)^{L-1},$$

where we have written each $\tau - \tau' = (n_1, \ldots, n_h)$, and where L is the length of these types $\tau - \tau'$.

Thanks!