How nonunique . . .

is your factorization?

Paul Pollack, UGA

joint with Enrique Treviño and Kai (Steve) Fan

Unique factorization?

Let D be an integral domain. A nonzero, nonunit element $\pi \in D$ is **irreducible** if π cannot be written as a product of two nonunits.

A domain D is a **unique factorization domain (UFD)** if every nonzero nonunit is a product of irreducibles and this expression is unique $\underline{\text{up to order and up to unit factors}}$.

Unique factorization?

Let D be an integral domain. A nonzero, nonunit element $\pi \in D$ is **irreducible** if π cannot be written as a product of two nonunits.

A domain D is a **unique factorization domain (UFD)** if every nonzero nonunit is a product of irreducibles and this expression is unique $\underline{\text{up to order and up to unit factors}}$.

More precisely, we require that if $\pi_1 \cdots \pi_k = \rho_1 \ldots \rho_\ell$, with all the π_i and ρ_j irreducible, then

(a) $k = \ell$,

(b) after rearranging, π_i is a D-unit multiple of ρ_i for all $i = 1, 2, \ldots, k$.

Hits and misses

In a first algebra course, one sees many examples of UFDs. These can lull one into a false sense of security!

The following near-canonical example of non-unique factorization is helpful to keep students on their toes: In the ring $\mathbb{Z}[\sqrt{-5}]$,

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

This is a *genuine* example of non-unique factorization: all of $2, 3$, $1+\sqrt{-5}$ and $1-\sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. Furthermore, the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1, so there is no chance that the irreducibles on the left are unit multiples of those on the right.

Hits and misses

In a first algebra course, one sees many examples of UFDs. These can lull one into a false sense of security!

The following near-canonical example of non-unique factorization is helpful to keep students on their toes: In the ring $\mathbb{Z}[\sqrt{-5}]$,

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

This is a *genuine* example of non-unique factorization: all of $2, 3$, $1+\sqrt{-5}$ and $1-\sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. Furthermore, the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1, so there is no chance that the irreducibles on the left are unit multiples of those on the right.

Thus, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD!

Hits and misses

In a first algebra course, one sees many examples of UFDs. These can lull one into a false sense of security!

The following near-canonical example of non-unique factorization is helpful to keep students on their toes: In the ring $\mathbb{Z}[\sqrt{-5}]$,

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

This is a *genuine* example of non-unique factorization: all of $2, 3$, $1+\sqrt{-5}$ and $1-\sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. Furthermore, the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1, so there is no chance that the irreducibles on the left are unit multiples of those on the right.

Thus, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD! However, it's not that from being one. There are two irreducibles involved in both of our factorizations of 6. And this is the case for *all* counterexamples to uniqueness. We call $\mathbb{Z}[\sqrt{-5}]$ a **half-factorial domain** (HFD).

Stretching, the truth about unique factorization

Let D be a domain where every nonzero nonunit factors into irreducibles. For each nonzero nonunit $\alpha \in D$, we define the **length spectrum** of α by

$$\mathcal{L}(\alpha) = \{\text{all lengths } k \text{ of irreducible factorizations } \alpha = \pi_1 \cdots \pi_k\}.$$

We define the **elasticity** of α by

$$\rho(\alpha) = \frac{\sup \mathcal{L}(\alpha)}{\inf \mathcal{L}(\alpha)}.$$

Finally, we define the elasticity $\rho(D)$ of D by

$$\rho(D) = \sup_{\alpha} \rho(\alpha).$$

So $\rho(D) = 1$ if and only if D is an HFD.

Fun. Theorem of Stretchiness

When K be a number field (finite extension of $\mathbb{Q}$), it is known that the elasticity of the ring of integers $\mathcal{O}_K$ is a finite number expresible in terms of a certain combinatorial constant associated to the class group.

Definition

Let G be a finite abelian group. The **Davenport constant** of G is the smallest positive integer $D = D(G)$ with the following property:

> *Every sequence $g_1, g_2, \ldots, g_D$ of elements of G contains a nonempty subsequence multiplying to the identity.*

Fun. Theorem of Stretchiness, ctd.

Fun Theorem of Stretchiness (Narkiewicz, Steffan, Valenza)

Whenever $\mathcal{O}_K$ is not a unique factorization domain,

$$\rho(\mathcal{O}_K) = \frac{1}{2}D,$$

where $D = \mathrm{Dav}\ \mathrm{Cl}(\mathcal{O}_K)$.

Fun. Theorem of Stretchiness, ctd.

Fun Theorem of Stretchiness (Narkiewicz, Steffan, Valenza)

Whenever $\mathcal{O}_K$ is not a unique factorization domain,

$$\rho(\mathcal{O}_K) = \frac{1}{2} D,$$

where $D = \mathrm{Dav}\ \mathrm{Cl}(\mathcal{O}_K)$.

This has some nice corollaries. For example, $\mathcal{O}_K$ is a HFD precisely when $\mathrm{Cl}(\mathcal{O}_K)$ has size 1 or 2 (Carlitz, 1960). In particular, $\mathbb{Z}[\sqrt{-5}]$ (of class number 2) is an HFD.

Fun. Theorem of Stretchiness, ctd.

Fun Theorem of Stretchiness (Narkiewicz, Steffan, Valenza)

Whenever $\mathcal{O}_K$ is not a unique factorization domain,

$$\rho(\mathcal{O}_K) = \frac{1}{2} D,$$

where $D = \mathrm{Dav}\ \mathrm{Cl}(\mathcal{O}_K)$.

This has some nice corollaries. For example, $\mathcal{O}_K$ is a HFD precisely when $\mathrm{Cl}(\mathcal{O}_K)$ has size 1 or 2 (Carlitz, 1960). In particular, $\mathbb{Z}[\sqrt{-5}]$ (of class number 2) is an HFD.

Davenport introduced these constants by means of the following observation, which is central to the proof of the Fun Stretchiness Theorem: The Davenport constant of the class group of K is the maximum number of prime ideals appearing (with multiplicity) in the prime ideal factorization of an irreducible element of $\mathcal{O}_K$.

Don't expect the worst

The Fun Elasticity Theorem tells us is that

$$\sup_{\alpha} \rho(\alpha) = \frac{1}{2} D,$$

where α here ranges over all nonzero nonunits.

Taking a sup means looking at the worst case. But we could also consider what we expect to happen!

That is: What is the *usual* size of $\rho(\alpha)$, for nonzero nonunits $\alpha \in \mathcal{O}_K$?

The answer is another constant $\tilde{\rho}(\mathcal{O}_K)$, strictly smaller than $\rho(\mathcal{O}_K)$ when $\mathcal{O}_K$ is not an HFD (Narkiewicz, Allen & Pleasants).

Don’t expect the worst, be Pleasant!

Theorem

For each number field K, there is a positive constant $\tilde{\rho}(\mathcal{O}_K)$ with the following property: For each $\epsilon > 0$, and asmyptotically 100% of $\alpha \in \mathcal{O}_K$,

$$1 - \epsilon < \frac{\rho(\alpha)}{\tilde{\rho}(\mathcal{O}_K)} < 1 + \epsilon.$$

Furthermore, $\tilde{\rho}(\mathcal{O}_K)$ depends only on the class group of K.

(For the fastidious: Asymptotically 100% is with respect to sampling principal ideals of $\mathcal{O}_K$, ordered by increasing norm.)

Which combinatorial invariant of $\mathrm{Cl}(\mathcal{O}_K)$ is $\tilde{\rho}$?

Playing solitaire, in a group!

To determine $\tilde{\rho}(\mathcal{O}_K)$ requires determining the optimal way to play a certain game on the class group of $\mathcal{O}_K$. I call this game "group solitaire."

Let G be a finite abelian group. (For the application to $\tilde{\rho}(\mathcal{O}_K)$, we will take G as a class group, but the setup of the game doesn't require that.) Observe that

$$\left(\prod_{g\in G} g\right)^2 = \prod_{g\in G} g \prod_{g\in G} g^{-1} = e.$$

This will be useful momentarily.

The rules of the game

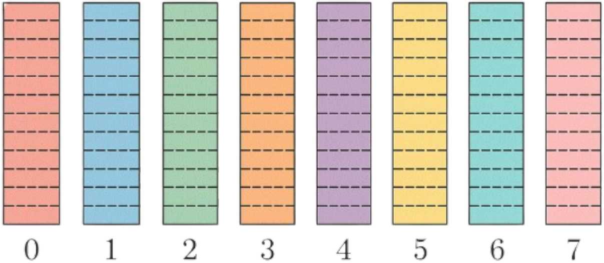
Let's suppose G has n elements. Take n stacks of poker chips, each of the same height X (height $=$ number of chips). We view each chip as representing an element of the group, with the different stacks corresponding to the different elements.

Let's assume X is even. Then the product of all the poker chips is the identity e. (It is $(\prod_{g\in G} g)^2$ raised to the power $X/2$.)

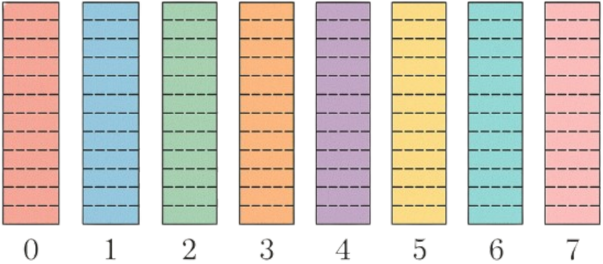
An allowable move consists of removing a collection of chips which multiply to the identity, where no proper subcollection also multiplies to the identity.

Objective: Clear all the stacks in as few moves as possible!

An example: $\mathbb{Z}/8\mathbb{Z}$ solitaire



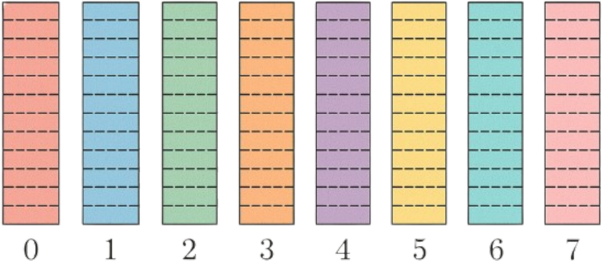
An example: $\mathbb{Z}/8\mathbb{Z}$ solitaire



Exercise

Take $G = \mathbb{Z}/8\mathbb{Z}$. Show that if each stack has height X, then any way of clearing the stacks requires at least $\sim \frac{5}{2}X$ moves.

An example: $\mathbb{Z}/8\mathbb{Z}$ solitaire



Exercise

Take $G = \mathbb{Z}/8\mathbb{Z}$. Show that if each stack has height X, then any way of clearing the stacks requires at least $\sim \frac{5}{2}X$ moves.

To determine $\tilde{\rho}(\mathcal{O}_K)$, we need the $\mathrm{Cl}(\mathcal{O}_K)$-analogue of the constant $\frac{5}{2}$. We know the G-analogue in only a few cases, e.g., $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ or $G = (\mathbb{Z}/p\mathbb{Z})^r$.

And now for something different

. . . but not completely different. . . .

So far we have been thinking about elasticities of rings of integers of number fields. For the rest of this talk, we will switch gears.

Rather than look at the full ring of integers of K, we will consider subrings. And rather than look at all K, we will restrict to quadratic fields K — fields one can write in the form $\mathbb{Q}(\sqrt{d})$, where d is a squarefree integers.

Orders in the court

Let K be a quadratic field. An **order** in K is a subring of $\mathcal{O}_K$ properly containing $\mathbb{Z}$. The ring $\mathcal{O}_K$ itself is referred to as the **maximal order**.

The orders in K are in one-to-one correspondence with positive integers f. Each order in K has finite index as a subgroup of $\mathcal{O}_K$, and for each $f \in \mathbb{Z}^+$, there is a unique order whose index is f. This is denoted $\mathcal{O}_f$, and f is called the **conductor** of the order.

It is easy to be (even more) explicit about the order of conductor f inside a given quadratic field. For example, in $\mathbb{Q}(i)$, it is just $\mathbb{Z}[fi]$, while in $\mathbb{Q}(\sqrt{5})$, it is $\mathbb{Z}[f\frac{1+\sqrt{5}}{2}]$.

Our problem: How do elasticities vary among orders in a fixed quadratic field?

There be dragons here. . .

Example

Let's think about the order of conductor 5 in $\mathbb{Z}[i]$, that is, $\mathbb{Z}[5i]$.

Exercise

(a) $5(2+i)^k$ is irreducible in $\mathbb{Z}[5i]$ for every k, as is $5(2-i)^k$.

(b) $5(2+i)^k \cdot 5(2-i)^k = \underbrace{5 \cdot 5 \cdot 5 \cdots 5}_{k+2 \text{ times}}$.

Hence, $\rho(\mathbb{Z}[5i]) \geq \frac{k+2}{2}$.

But k is arbitrary! Hence, $\rho(\mathbb{Z}[5i]) = \infty$. Infinite elasticity cannot happen for a full ring of integers!

There be dragons here. . .

Example

Let's think about the order of conductor 5 in $\mathbb{Z}[i]$, that is, $\mathbb{Z}[5i]$.

Exercise

(a) $5(2+i)^k$ is irreducible in $\mathbb{Z}[5i]$ for every k, as is $5(2-i)^k$.

(b) $5(2+i)^k \cdot 5(2-i)^k = \underbrace{5 \cdot 5 \cdot 5 \cdots 5}_{k+2 \text{ times}}$.

Hence, $\rho(\mathbb{Z}[5i]) \geq \frac{k+2}{2}$.

But k is arbitrary! Hence, $\rho(\mathbb{Z}[5i]) = \infty$. Infinite elasticity cannot happen for a full ring of integers!

Halter-Koch: order of conductor f has finite elasticity $\iff$ f is not divisible by any prime split in K. (In $\mathbb{Q}(i)$: not divisible by any prime 1 mod 4.)

Half truths

An order of conductor > 1 cannot be a UFD. But it can be an HFD!

Theorem (Coykendall, 2001)

$\mathbb{Z}[\sqrt{-3}]$ *is the unique nonmaximal HFD order in an imaginary quadratic field.*

Conjecture (Coykendall, 2001)

(a) *There are infinitely many HFDs as you vary over all quadratic fields and all orders contained in those fields.*

(b) *There are infinitely many HFDs as you vary among the orders in the quadratic field* $\mathbb{Q}(\sqrt{2})$*.*

Half truths

Conjecture (Coykendall, 2001)

(a) *There are infinitely many HFDs as you vary over all quadratic fields and all orders contained in those fields.*

(b) *There are infinitely many HFDs as you vary among the orders in the quadratic field* $\mathbb{Q}(\sqrt{2})$.

Theorem (P., 2023)

(a) *is true, and* (b) *is true assuming GRH.*

By contrast, we do not know how to prove there are infinitely many number fields (quadratic or not) whose rings of integers are HFDs!

Why do I go to extremes?

We have seen examples where the elasticity is infinite and examples where the elasticity is 1.

What is the “typical” elasticity of an order in a fixed quadratic field K?

For most f, the elasticity is infinite. Asymptotically half the rational primes split in K. Most f are divisible by at least one of those primes.

Call an f not divisible by any prime that splits in K a **split-free integer**.

New question: Fix a quadratic field K. What is the “typical” size of $\rho(\mathcal{O}_f)$ as f varies among split-free positive integers?

Number theory → lumber theory

Theorem (Fan and P., 2024)

If K is real quadratic, then under GRH,

$$\rho(\mathcal{O}_f) \approx (\log f)^{1/2}$$

for almost all split-free f. If K is imaginary quadratic, then

$$\rho(\mathcal{O}_f) \approx f/(\log f)^{\frac{1}{2}\log\log\log f + C_K}$$

for almost all split-free f (unconditionally).

Approximately: Fix $\epsilon > 0$. Both estimates are accurate to within multiplicative factors of $(\log f)^{\epsilon}$.

Almost-all: The relative frequency of counterexamples among split-free f in $[1, x]$ tends to 0, as $x \to \infty$.

Extremal elasticities, split-free case

In a more recent paper, Steve and I study the extremal size of order elasticities. In the interests of time, I give our result only for the minimal size of elasticities in the imaginary quadratic case.

Theorem (minimal size, imaginary case)

Let K be a fixed imaginary quadratic field. There are absolute constants $c_1, c_2 > 0$ for which the following holds. For all sufficiently large split-free f,

$$\rho(\mathcal{O}_f) > (\log f)^{c_1 \log\log\log f}.$$

On the other hand, there is a sequence of split-free f tending to infinity along which

$$\rho(\mathcal{O}_f) < (\log f)^{c_2 \log\log\log f}.$$

Where does all this come from?

Perhaps surprisingly, the proofs builds on techniques used to study seemingly unrelated questions.

Observe that $1/7 = 0.\overline{142857}$ has period length $7-1$, and $1/19 = 0.\overline{052631578947368421}$ has period length $19-1 = 18$. On the other hand, $1/13 = 0.\overline{076923}$, so the period length is $\frac{13-1}{2}$.

It's not so hard to prove that for a prime $p \neq 2, 5$, the period length is always a divisor of $p-1$ — in fact, it's nothing other than the order of 10 in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^{\times}$. Is it equal to $p-1$ infinitely often?

Artin conjectured YES. He gave a heuristic argument that this should happen $\approx 37.4\%$ of the time.

Hooley, Gupta, and Murty, oh my!

Artin's conjecture is still open. However, in 1967 Hooley proved that Artin's conjecture follows from the Generalized Riemann Hypothesis.

In 1984, Gupta and Murty found a clever proof that there is some base $b \geq 2$ for which infinitely many primes p have repeating period $p-1$. In fact, their method produces many such bases; Heath-Brown has shown that one of the bases $2, 3$, or 5 works (though the method does not allow one to decide which).

Quadratic Artin to the rescue

The theorem about HFDs (towards Coykendall's conjectures) is proved by similar methods but in the quadratic field setting. Here the connection is provided by the order class number formula, and the role of the base is played by the "fundamental unit" of the quadratic field.

To make this all explicit. It turns out that proving conjecture (b) — that $\mathbb{Z}[\sqrt{2}]$ has infinitely many half-factorial orders — is equivalent to showing there are infinitely many primes p inert in $\mathbb{Z}[\sqrt{2}]$ for which $\ell = p+1$ is the least positive integer ℓ with

$$(1+\sqrt{2})^{\ell} \equiv (\text{some rational integer}) \pmod{p}.$$

This can be shown under GRH (almost implicit in work of Chen and Roskam).

Typical and extremal elasticites?

The other elasticity results are consequences of new theorems on the distribution of Davenport constants of class groups of quadratic orders.

These Davenport constants do not tell all of the story — unlike in the case of the maximal order, the elasticity of an order is not a function of the isomorphism class of the class group! But (we are able to show) they tell most of the story.

For our purposes: When K is imaginary quadratic, one can model the family of class groups of the orders $\mathcal{O}_f$ by the unit groups $(\mathbb{Z}/f\mathbb{Z})^\times$.

When K is real quadratic, one can model the family of class groups of the orders $\mathcal{O}_f$ by the unit groups $(\mathbb{Z}/f\mathbb{Z})^\times/\langle 2\rangle$, where f ranges only over odd integers.

On the shoulders of a giant

The Davenport constant of a finite abelian group is usually not too far off from the exponent of that group (the largest order of any element) — by a theorem of van Emde Boas/Kruyswijk.

Quite a lot is known about the distribution of orders of elements in $(\mathbb{Z}/f\mathbb{Z})^\times$.

Many mathematicians have worked on these problems. There is one mathematician whose work has been paticularly influential in formulating, and establishing, our class group results: Carl Pomerance.

On the shoulders of a giant

In a 1991 paper, Erdős, Pomerance, and Schmutz show that 'typically' the group $(\mathbb{Z}/f\mathbb{Z})^{\times}$ has exponent

$$\approx f/(\log f)^{\log\log\log f + C}.$$

This looks an awful lot like the result we claimed for the typical elasticity of an imaginary quadratic order!

On the shoulders of a giant

In a 1991 paper, Erdős, Pomerance, and Schmutz show that 'typically' the group $(\mathbb{Z}/f\mathbb{Z})^{\times}$ has exponent

$$\approx f/(\log f)^{\log\log\log f + C}.$$

This looks an awful lot like the result we claimed for the typical elasticity of an imaginary quadratic order!

In that same article, Carl and his coauthors show that

$$\mathrm{Exp}\,(\mathbb{Z}/f\mathbb{Z})^{\times} > (\log f)^{c\log\log\log f}$$

for all large f, and that this result is best possible up to the choice of c. Look familiar?

Giants, ctd.

Where does GRH enter the picture? Recall that when K is real quadratic, our model suggests the class groups are “similar” to the quotiented unit groups $(\mathbb{Z}/f\mathbb{Z})^\times/\langle 2\rangle$.

Understanding the size of this group requires coming to terms with the order of 2 modulo f. GRH implies that the order of 2 modulo f is usually ‘close’ in size to the exponent of the group $(\mathbb{Z}/f\mathbb{Z})^\times$ (Li and Pomerance). These ideas play a crucial role in our handling of the real quadratic case.

Thank You!