Arithmetic Beyond $\mathbb{Z}$

A fifteen-day course on quadratic number rings

Paul Pollack

Ross Program 2026

The course begins with a beautiful tragedy

Elements fail us.

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

Factorization into irreducibles need not be unique.

Ideals repair the damage.

$$(2) = P_2^2, \qquad (3) = P_3 \tilde{P}_3.$$

Their classes then measure what element factorization has lost.

Our narrative

Diophantine equations $\to$ failed factorization $\to$ ideals $\to$ prime ideals $\to$ units and class groups $\to$ factorization lengths.

DAY 1

Motivation

Why go beyond the integers to solve problems about integers?

How this course is meant to be learned

- The course follows the first-year number theory problem sets and is aimed primarily at returning students.
- Lectures supply the architecture; problems supply the understanding.
- The guiding habit is research-like: when an idea works beautifully, ask where else it works—and where it breaks.

The opening question

Why does algebraic number theory exist, and why are we studying it?

A warm-up stays entirely inside $\mathbb{Z}$

Problem

Find all integers x, y satisfying

$$y^2 = x^3 + x.$$

The obvious solution is $(x, y) = (0, 0)$. Rewrite:

$$y^2 = x(x^2 + 1).$$

If $d \mid x$ and $d \mid x^2 + 1$, then

$$d \mid (x^2 + 1) - x \cdot x = 1.$$

Thus the two factors on the right are coprime.

Coprime factors of a square are squares

From

$$y^2 = x(x^2+1), \qquad \gcd(x, x^2+1) = 1,$$

we obtain

$$x = \square, \qquad x^2+1 = \square,$$

using $x^2 + 1 > 0$.

So x^2 and x^2+1 are consecutive squares. The only consecutive squares are 0 and 1, because the gaps between squares are consecutive odd numbers.

$$x^2 = 0 \quad \Longrightarrow \quad x = 0,\ y = 0.$$

Well, that was too easy.

Fermat's sandwich theorem asks us to enlarge the ring

Problem

Find all integer solutions of

$$y^2 = x^3 - 2.$$

Rewrite the equation as

$$x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2})$$

inside

$$\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}.$$

The point is not to abandon $\mathbb{Z}$, but to factor an expression that refused to factor there.

The norm controls arithmetic in $\mathbb{Z}[\sqrt{-2}]$

For $\alpha = a + b\sqrt{-2}$, define the **norm**

$$\mathrm{N}(\alpha) = \alpha\tilde{\alpha} = a^2 + 2b^2.$$

Then:

- $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$;
- $\mathrm{N}(\alpha) \in \mathbb{Z}_{\geq 0}$, with $\mathrm{N}(\alpha) = 0 \iff \alpha = 0$;
- α is a unit iff $\mathrm{N}(\alpha) = 1$, hence iff $\alpha = \pm 1$.

Fermat's sandwich theorem

The only integer solutions of $x^3 = y^2 + 2$ are $x = 3$, $y = \pm 5$.

First squeeze: parity and coprimality

If x were even, then $8 \mid x^3 = y^2 + 2$, giving

$$y^2 \equiv 6 \pmod 8,$$

impossible. Hence x and y are odd.

Suppose δ divides both $y + \sqrt{-2}$ and $y - \sqrt{-2}$. Then

$$\mathrm{N}(\delta) \mid y^2 + 2,$$

so $\mathrm{N}(\delta)$ is odd. Also

$$\delta \mid 2\sqrt{-2} \quad \Longrightarrow \quad \mathrm{N}(\delta) \mid 8.$$

Therefore $\mathrm{N}(\delta) = 1$, so δ is a unit.

Coprime factors of a cube should be cubes

Since

$$(y+\sqrt{-2})(y-\sqrt{-2}) = x^3$$

and the factors are coprime, unique factorization in $\mathbb{Z}[\sqrt{-2}]$ gives

$$y+\sqrt{-2} = (a+b\sqrt{-2})^3.$$

The possible unit factor causes no trouble: ± 1 are cubes.

Expanding,

$$(a+b\sqrt{-2})^3 = (a^3-6ab^2)+(3a^2b-2b^3)\sqrt{-2}.$$

Comparing the $\sqrt{-2}$-coefficients yields

$$1 = b(3a^2-2b^2),$$

so $b = \pm 1$.

The coefficient comparison finishes the proof

If $b = 1$, then

$$3a^2 - 2 = 1,$$

so $a = \pm 1$. Thus

$$y + \sqrt{-2} = (\pm 1 + \sqrt{-2})^3 = \pm 5 + \sqrt{-2}.$$

Hence $y = \pm 5$, and then

$$x^3 = y^2 + 2 = 27,$$

so $x = 3$.

If $b = -1$, then $1 = -3a^2 + 2$, which has no integer solution.

The same idea appears to solve a harder equation

Now consider

$$x^3 = y^2 + 26 = (y + \sqrt{-26})(y - \sqrt{-26})$$

in $\mathbb{Z}[\sqrt{-26}]$.

Again x, y are odd. If δ divides both factors, then

$$\mathrm{N}(\delta) \mid y^2 + 26 \quad \text{and} \quad \mathrm{N}(\delta) \mid \mathrm{N}(2\sqrt{-26}) = 104.$$

Thus $\mathrm{N}(\delta) \mid 13$. But $\mathrm{N}(\delta) = 13$ would require

$$a^2 + 26b^2 = 13,$$

impossible. So the factors are coprime.

The copied argument produces $(35, \pm 207)$

Assuming the coprime-cube step,

$$y + \sqrt{-26} = (a + b\sqrt{-26})^3.$$

Comparing coefficients gives

$$1 = b(3a^2 - 26b^2),$$

so $b = \pm 1$. The case $b = -1$ is impossible; for $b = 1$,

$$3a^2 - 26 = 1 \quad \Longrightarrow \quad a = \pm 3.$$

Therefore

$$y + \sqrt{-26} = (\pm 3 + \sqrt{-26})^3 = \pm 207 + \sqrt{-26},$$

and apparently $y = \pm 207$, $x = 35$.

Wait a second

The equation

$$y^2 = x^3 - 26$$

also has the solution

$$x = 3, \qquad y = \pm 1.$$

So the preceding proof is wrong.

The suspicious step

If a, b are coprime and ab is a cube, must a and b be cubes up to units?

This coprime cube criterion is true in a unique factorization domain. It is false in $\mathbb{Z}[\sqrt{-26}]$.

The failed proof exposes the real subject

In $\mathbb{Z}[\sqrt{-26}]$,

$$3^3 = (1 + \sqrt{-26})(1 - \sqrt{-26}),$$

and the displayed factors are irreducible. The two sides even use different numbers of irreducible factors.

By contrast, in $\mathbb{Z}[\sqrt{-5}]$,

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

has two irreducible factors on each side.

The course goal

Build a class group that measures these failures. The coprime cube criterion will survive, in essence, whenever that group has no element of order 3.

DAY 2

What is unique factorization?

And is there just one meaning of “unique”?

The cube criterion is the culprit

Last time, we used:

Coprime cube criterion

If a, b are coprime and ab is a cube, then a and b are cubes up to unit factors.

It holds in $\mathbb{Z}$ by unique factorization, but fails in $\mathbb{Z}[\sqrt{-26}]$.

Two questions now separate:

- When does $\mathbb{Z}[\sqrt{n}]$ have unique factorization?
- Does the Diophantine method really require full unique factorization?

The eventual answer to the second question is no: "How far from a UFD?" is answered by a group, not merely yes or no.

Atoms are the pieces that cannot be split further

Let R be a domain.

Irreducible element, or atom

A nonzero nonunit $\pi \in R$ is irreducible if

$$\pi = \alpha\beta \quad \Longrightarrow \quad \alpha \text{ or } \beta \text{ is a unit.}$$

Atomic domain

R is atomic if every nonzero nonunit is a product of atoms.

Examples include $\mathbb{Z}$, $\mathbb{Z}[\sqrt{-2}]$, and every quadratic ring of integers $\mathcal{O}_D$; norms supply a well-ordering argument.

A norm proves that $3 + \sqrt{2}$ is irreducible

In $\mathbb{Z}[\sqrt{2}]$,

$$\mathrm{N}(a + b\sqrt{2}) = a^2 - 2b^2,$$

which may be negative, and

$$\alpha \text{ is a unit} \iff \mathrm{N}(\alpha) = \pm 1.$$

Now $\mathrm{N}(3 + \sqrt{2}) = 7$, so $3 + \sqrt{2}$ is not a unit. If

$$3 + \sqrt{2} = \alpha\beta,$$

then

$$7 = \mathrm{N}(\alpha)\,\mathrm{N}(\beta).$$

One norm is ± 1, so one factor is a unit. Hence $3 + \sqrt{2}$ is an atom.

The integer 3 is also irreducible in $\mathbb{Z}[\sqrt{2}]$

If $3 = \alpha\beta$ with both factors nonunits, then

$$9 = \mathrm{N}(\alpha)\,\mathrm{N}(\beta),$$

forcing $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = \pm 3$.

Writing $\alpha = x + y\sqrt{2}$, this asks for

$$x^2 - 2y^2 = \pm 3.$$

Modulo 8, the right side would have to equal $x^2 + 6y^2$. Checking $y^2 \equiv 0, 1, 4 \pmod 8$ against the possible square residues $0, 1, 4$ gives no solution.

Therefore 3 is irreducible in $\mathbb{Z}[\sqrt{2}]$.

Units force us to weaken literal uniqueness

Even in $\mathbb{Z}$,

$$14 = 2 \cdot 7 = (-7)(-2).$$

In $\mathbb{Z}[\sqrt{2}]$, the phenomenon is much more dramatic:

$$7 = (3 + \sqrt{2})(3 - \sqrt{2}) = (181 + 128\sqrt{2})(-181 + 128\sqrt{2}).$$

But

$$181 + 128\sqrt{2} = (3 + \sqrt{2})(41 + 29\sqrt{2}),$$
$$-181 + 128\sqrt{2} = (3 - \sqrt{2})(-41 + 29\sqrt{2}),$$

and the extra factors are units. The two factorizations agree up to associates.

A UFD has existence and uniqueness

Two elements are **associates** if one is a unit multiple of the other.

Unique factorization domain

A domain R is a UFD if it is atomic and whenever

$$\pi_1 \cdots \pi_k = \rho_1 \cdots \rho_\ell$$

with all factors irreducible, then

1. $k = \ell$;
2. after a permutation, each π_i is associate to ρ_i.

This is the definition that the quotation marks around "unique factorization" were waiting for.

Three non-UFDs fail in three instructive ways

Quadratic examples

$$\mathbb{Z}[\sqrt{-5}]: \quad 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

with two atoms on each side, while

$$\mathbb{Z}[\sqrt{-26}]: \quad 3^3 = (1+\sqrt{-26})(1-\sqrt{-26})$$

has different lengths.

In both rings the only units are ± 1, and the displayed factors are atoms by norm arguments.

A polynomial subring has lengths 3 and 2

Let

$$R = \{f(x) \in \mathbb{Q}[x] : \text{the coefficient of } x \text{ vanishes}\}.$$

Then

$$x^6 = x^2x^2x^2 = x^3x^3.$$

The units are the nonzero rationals, and x^2, x^3 are irreducible in R.

Our challenge

Find a factorization in $\mathbb{Z}[\sqrt{-5}]$ whose two sides have different lengths.

I won't spoil this until the end of the course.

Factorization only needs multiplication

Commutative monoid

A (commutative) **monoid** is a nonempty set with an associative, commutative operation and an identity element 1.

Examples:

- every abelian group;
- a ring under multiplication, or the nonzero elements of a domain;
- $\mathbb{Z}_{\geq 0}$ under addition;
- $\{163x + 519y : x, y \geq 0\}$ under addition.

A monoid is **cancellative** if $\alpha\beta = \alpha\gamma$ implies $\beta = \gamma$.

Divisibility and atoms make sense in a monoid

Let M be a cancellative monoid.

- $\alpha \mid \beta$ if $\beta = \alpha\gamma$ for some $\gamma \in M$.
- A **unit** is an element that divides 1.
- α, β are **associates** if $\alpha = \beta u$ for a unit u.
- A nonunit π is an **atom** if $\pi = \alpha\beta$ forces α or β to be a unit.
- M is **atomic** if every nonunit is a product of atoms.

These are exactly the notions element factorization had been using all along.

Unique factorization monoids are the real abstraction

Unique factorization monoid

A cancellative monoid M is a UFM if it is atomic and every nonunit has a factorization into atoms that is unique up to order and associates.

If R is an integral domain and $M = R \setminus \{0\}$, then

$$R \text{ is a UFD} \iff R \setminus \{0\} \text{ is a UFM.}$$

This formulation will let us replace elements by ideals without changing the logic of factorization.

Primes turn atomicity into uniqueness

Prime element of a monoid

A nonunit $\pi \in M$ is prime if

$$\pi \mid \alpha\beta \quad \Longrightarrow \quad \pi \mid \alpha \text{ or } \pi \mid \beta.$$

Prime criterion

If a cancellative monoid M is atomic and every atom is prime, then M is a UFM.

This is the abstract form of the usual proof of unique factorization from Euclid's lemma.

Why the prime criterion gives uniqueness

Suppose

$$\pi_1 \cdots \pi_k = \rho_1 \cdots \rho_\ell$$

with all factors atoms. Since π_1 is prime, it divides some ρ_j. Irreducibility makes π_1 and ρ_j associates.

After reordering and cancelling these associates, repeat. Eventually

$$k = \ell$$

and the factors match up to associates.

The hard part in a new arithmetic system is therefore clear: prove atomicity, then prove a Euclid lemma.

DAY 3

The case of the missing numbers

Paradise lost, and a proposal for regaining it

Unique factorization explains every equality by refinement

In $\mathbb{Z}^+$, the identity

$$14 \cdot 15 = 21 \cdot 10$$

becomes unsurprising after refinement:

$$14 = 2 \cdot 7, \quad 15 = 3 \cdot 5, \quad 21 = 3 \cdot 7, \quad 10 = 2 \cdot 5.$$

Four Numbers Theorem

If M is a UFM and $ab = cd$, then there exist $r, s, t, u \in M$ such that

$$a = rs, \quad b = tu, \quad c = ru, \quad d = st.$$

We assign the general proof as homework.

In positive integers, fractions reveal the refinement

From $ab = cd$, write

$$\frac{a}{d} = \frac{c}{b} = \frac{r}{t}$$

in lowest terms. "Undoing" the reduction gives integers s, u such that

$$a = rs, \qquad d = ts,$$

$$c = ru, \qquad b = tu.$$

This beautifully short proof quietly uses the theory of fractions and the arithmetic of $\mathbb{Z}$. It is a productive exercise to formalize this argument starting from the Ross axioms for $\mathbb{Z}$.

The Four Numbers Theorem fails in $\mathbb{Z}[\sqrt{-5}]$

For

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

we would need

$$2 = rs, \quad 3 = tu, \quad 1 + \sqrt{-5} = ru, \quad 1 - \sqrt{-5} = st.$$

Since 2 is irreducible, one of r, s is a unit. If r is a unit, then $s = 2(\text{unit})$, forcing

$$2 \mid 1 - \sqrt{-5},$$

which is false. The case that s is a unit is similar.

The ring is missing the factors the refinement wants

For positive integers with $\gcd(a, b, c, d) = 1$, refinement can be written as

$$a = (a, c)(a, d), \quad c = (a, c)(b, c),$$
$$b = (b, c)(b, d), \quad d = (a, d)(b, d).$$

This suggests that our failed identity wants "numbers" such as

$$(2, 1 + \sqrt{-5}), \qquad (3, 1 - \sqrt{-5}).$$

The notation does not yet make sense as a gcd in $\mathbb{Z}[\sqrt{-5}]$. The challenge is to make it mean something else.

A number can be viewed as its set of multiples

For a domain R,

$$a \mid b \quad \iff \quad b \in aR,$$

where

$$aR = \{ar : r \in R\}.$$

Moreover,

$$aR = bR \quad \iff \quad a = b(\text{unit}).$$

Define the **monoid of nonzero principal ideals**

$$\text{Prin}(R) = \{aR : a \neq 0\}, \qquad (aR)(bR) = abR.$$

Then

$$\text{Prin}(R) \text{ is a UFM} \iff R \text{ is a UFD}.$$

So principal ideals repackage the old problem. We still need to solve it!

Ideals are generalized sets of multiples

The sets aR all:

1. contain 0;
2. are closed under addition;
3. absorb multiplication by elements of R.

Ideal

An ideal $I \subseteq R$ is a subset with exactly these three properties.

Write

$$\mathrm{Id}(R) = \{I \subseteq R : I \text{ is a nonzero ideal}\}.$$

We have $\mathrm{Prin}(R) \subseteq \mathrm{Id}(R)$, with equality for $R = \mathbb{Z}$, but not generally.

Generated ideals make the old gcd notation useful again

For $a_1, \ldots, a_n \in R$, define the **ideal generated by** $a_1, \ldots, a_n$:

$$(a_1, \ldots, a_n) = a_1R + \cdots + a_nR = \left\{ \sum_{j=1}^{n} a_j r_j : r_j \in R \right\}.$$

Back in $\mathbb{Z}$,

$$a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z},$$

so the notation is not accidental.

For ideals I, J, define their **ideal product** IJ as the additive closure of pairwise products. In particular,

$$(a, b)(c, d) = (ac, ad, bc, bd).$$

The missing factors now exist

In $\mathrm{Id}(\mathbb{Z}[\sqrt{-5}])$,

$$\begin{aligned}
&(2, 1+\sqrt{-5})(2, 1-\sqrt{-5}) \\
&\quad = (4, 2-2\sqrt{-5}, 2+2\sqrt{-5}, 6) \\
&\quad = 2(2, 1-\sqrt{-5}, 1+\sqrt{-5}, 3) \\
&\quad = 2\mathbb{Z}[\sqrt{-5}] = (2).
\end{aligned}$$

The middle ideal is the unit ideal because it contains

$$3 - 2 = 1.$$

The whole factorization acquires a common refinement

Similarly,

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

Thus the equality of principal ideals

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

is explained by four ideal factors.

Paradise regained becomes a theorem to prove

Unique factorization of ideals

$\mathrm{Id}(\mathbb{Z}[\sqrt{-5}])$ is a UFM.

More generally, for every squarefree $D \neq 1$,

$$\mathrm{Id}(\mathcal{O}_D)$$

is a UFM.

Element factorization failed because the ring lacked the required elements. Ideal factorization succeeds because the ideal monoid supplies the missing numbers.

DAY 4

Purgatorio

We have made the claim; now we build the world we want to see.

Generalized multiples can also be set equal to zero

The first-year problem sets study quotients such as

$$\mathbb{Z}/(m), \qquad \mathbb{Z}[i]/(\alpha), \qquad \mathbb{F}_p[x]/(f(x)).$$

If I is an ideal of a ring R, define **congruence modulo** I by

$$a \equiv b \pmod{I} \iff a - b \in I.$$

The **quotient ring** is

$$R/I = \{a + I : a \in R\}$$

with operations

$$(a + I) + (b + I) = (a + b) + I, \qquad (a + I)(b + I) = ab + I.$$

Morally, R/I is R with every element of I set equal to zero.

The quotient map remembers exactly the ideal

The natural map

$$\phi : R \longrightarrow R/I, \qquad a \longmapsto a + I$$

is a ring homomorphism, and

$$\ker \phi = I.$$

When R/I is finite, define the **ideal norm**

$$\|I\| = \#(R/I).$$

Examples in $\mathbb{Z}$:

$$\|(7)\| = 7, \qquad \|(-13)\| = 13.$$

The name "norm" will soon turn out to be more than an analogy.

Principal ideal norms already hint at conjugation

In $\mathbb{Z}[i]$, lattice geometry gives

$$\|(2+i)\| = 5,$$

and more generally

$$\|(\alpha)\| = |\,\mathrm{N}(\alpha)|.$$

Throughout this class, we will let $D \neq 1$ be squarefree and write

$$\mathcal{O}_D = \mathbb{Z}[\tau] = \{a + b\tau : a, b \in \mathbb{Z}\},$$

where

$$\tau = \begin{cases} \sqrt{D}, & D \equiv 2, 3 \pmod 4, \\ \dfrac{1+\sqrt{D}}{2}, & D \equiv 1 \pmod 4. \end{cases}$$

Conjugation acts on elements and ideals

For $\alpha \in \mathcal{O}_D$, its **conjugate** is $\tilde{\alpha}$, and

$$(x - \alpha)(x - \tilde{\alpha}) = x^2 - \mathsf{Tr}(\alpha)x + \mathsf{N}(\alpha) \in \mathbb{Z}[x].$$

Thus its **trace** and **norm** are

$$\mathsf{Tr}(\alpha) = \alpha + \tilde{\alpha} \in \mathbb{Z}, \qquad \mathsf{N}(\alpha) = \alpha\tilde{\alpha} \in \mathbb{Z}.$$

For an ideal $I \subseteq \mathcal{O}_D$, define the **conjugate ideal**

$$\tilde{I} = \{\tilde{\alpha} : \alpha \in I\}.$$

The central norm identity

For every nonzero ideal $I \subseteq \mathcal{O}_D$,

$$I\tilde{I} = (\|I\|).$$

Friendly bases expose both the ideal and its norm

Friendly basis proposition

For every nonzero ideal $I \subseteq \mathcal{O}_D$, there are integers n, A, B, with $n, B > 0$, such that:

1. $n, A + B\tau$ is a $\mathbb{Z}$-basis of I;
2. $I \cap \mathbb{Z} = n\mathbb{Z}$;
3. $B \mid n$ and $B \mid A$;
4. $\|I\| = nB$.

We assign the proof as homework. We call such a basis **friendly**.

A friendly basis makes $I\tilde{I}$ explicit

Choose a friendly basis $n, A + B\tau$. Write

$$n = Bn', \qquad A = BA', \qquad \beta = A' + \tau.$$

Then

$$I = B(n', \beta), \qquad \tilde{I} = B(n', \tilde{\beta}).$$

Therefore

$$I\tilde{I} = B^2(n'^2, n'\tilde{\beta}, n'\beta, \beta\tilde{\beta}).$$

The last generator is divisible by n': indeed,

$$B\beta\tilde{\beta} = (A + B\tau)\tilde{\beta} \in I \cap \mathbb{Z} = n\mathbb{Z} = Bn'\mathbb{Z}.$$

The norm identity reduces to proving one ideal is (1)

Since $n' \mid \mathrm{N}(\beta)$, factor the preceding ideal as

$$I\tilde{I} = B^2 n' J,$$

where

$$J = (n', \beta, \tilde{\beta}, \mathrm{N}(\beta)/n').$$

Because $B^2 n' = Bn = \|I\|$, it remains to prove

$$J = (1).$$

Now J contains the integers

$$n', \qquad \mathrm{Tr}(\beta), \qquad \frac{\mathrm{N}(\beta)}{n'}.$$

If their gcd back in the ordinary integers is 1, then $1 \in J$ and we are done.

A common divisor would make β/g integral

Suppose instead that an integer $g > 1$ divides

$$n', \qquad \mathrm{Tr}(\beta), \qquad \mathrm{N}(\beta)/n'.$$

Then $g^2 \mid \mathrm{N}(\beta)$, and

$$f(x) = \left(x - \frac{\beta}{g}\right)\left(x - \frac{\tilde{\beta}}{g}\right) = x^2 - \frac{\mathrm{Tr}(\beta)}{g}x + \frac{\mathrm{N}(\beta)}{g^2}$$

belongs to $\mathbb{Z}[x]$.

Thus β/g is an algebraic integer in $\mathbb{Q}(\sqrt{D})$, so

$$\frac{\beta}{g} \in \mathcal{O}_D.$$

The coefficient of τ supplies the contradiction

But

$$\frac{\beta}{g} = \frac{A'}{g} + \frac{1}{g}\tau.$$

Every element of $\mathcal{O}_D$ has a unique expression

$$a + b\tau, \qquad a, b \in \mathbb{Z}.$$

Since $g > 1$, the coefficient $1/g$ is not an integer. Contradiction.

Therefore the gcd is 1, so $J = (1)$, and hence

$$\boxed{I\tilde{I} = (\|I\|).}$$

A bit of a slog, but now the hits keep coming.

Principal ideals recover the familiar norm

Let $I = (\alpha)$, with $\alpha \neq 0$. Then

$$I\tilde{I} = (\alpha)(\tilde{\alpha}) = (\mathrm{N}(\alpha)),$$

while the norm identity gives

$$I\tilde{I} = (\|I\|).$$

Thus $\mathrm{N}(\alpha)/\|I\|$ and its reciprocal lie in

$$\mathbb{Q} \cap \mathcal{O}_D = \mathbb{Z}.$$

Their ratio is therefore ± 1, and positivity of ideal norm yields

$$\boxed{\|(\alpha)\| = |\,\mathrm{N}(\alpha)|.}$$

Ideal norm is multiplicative

For nonzero ideals $I, J \subseteq \mathcal{O}_D$,

$$\begin{aligned}(\|IJ\|) &= IJ(\tilde{I}\tilde{J}) \\ &= I J \tilde{I} \tilde{J} \\ &= (I\tilde{I})(J\tilde{J}) \\ &= (\|I\|)(\|J\|) \\ &= (\|I\|\|J\|).\end{aligned}$$

Both generators are positive integers, so

$$\boxed{\|IJ\| = \|I\|\|J\|.}$$

This multiplicativity will drive both atomicity and prime factorization.

DAY 5

Paradise regained

From one norm identity, civilization emerges.

Every ideal has a principal multiple

The identity

$$I\tilde{I} = (\|I\|)$$

immediately gives:

Principal Multiple Lemma

For every $I \in \mathrm{Id}(\mathcal{O}_D)$, there is $I' \in \mathrm{Id}(\mathcal{O}_D)$ such that II' is principal.

Indeed, take $I' = \tilde{I}$.

This result is the linchpin of (our way of developing) ideal theory.

The ideal monoid is cancellative

Suppose

$$IJ = IK.$$

Choose I' with $II' = (\alpha)$, $\alpha \neq 0$. Then

$$I'IJ = I'IK$$

becomes

$$(\alpha)J = (\alpha)K,$$

or

$$\alpha J = \alpha K.$$

Dilating both sides by α^{-1} gives $J = K$.

Thus $\mathrm{Id}(\mathcal{O}_D)$ is a cancellative monoid.

For ideals, to divide is to contain

Containment-divisibility theorem

For $I, J \in \mathrm{Id}(\mathcal{O}_D)$,

$$I \mid J \quad \iff \quad I \supseteq J.$$

If $J = IK$, then every finite sum of products from I and K lies in I, so $J \subseteq I$.

The converse is the interesting direction: if $I \supseteq J$, we must construct an ideal K with $J = IK$. Heuristically, $K = J/I$ (we don't know what this notation means, but let's not let that stop us). Now "$J/I = JI'/II'$", and we can choose I' to "rationalize the denominator."

A principal multiple makes the quotient ideal visible

Assume $I \supseteq J$. Choose I' with

$$II' = (\alpha), \qquad \alpha \neq 0,$$

and define

$$K = \alpha^{-1} JI' \subseteq \mathbb{Q}(\sqrt{D}).$$

Since $I \supseteq J$,

$$(\alpha) = II' \supseteq JI',$$

so

$$\mathcal{O}_D = (1) \supseteq \alpha^{-1} JI' = K.$$

Hence K is in fact an ideal of $\mathcal{O}_D$.

The constructed quotient really satisfies $J = IK$

Using the definition of K,

$$\begin{aligned} IK &= I(\alpha^{-1} J I') \\ &= \alpha^{-1}(II')J \\ &= \alpha^{-1}(\alpha)J \\ &= J. \end{aligned}$$

Therefore

$$I \supseteq J \quad \Longrightarrow \quad I \mid J,$$

which completes the proof that containment reverses divisibility.

The unit and atoms of $\mathrm{Id}(\mathcal{O}_D)$

The only unit of $\mathrm{Id}(\mathcal{O}_D)$ is the unit ideal $(1) = \mathcal{O}_D$.

Thus a nonzero ideal P is an atom precisely when

$$P \neq (1)$$

and

$$P = IJ \quad \Longrightarrow \quad I = (1) \text{ or } J = (1).$$

Hence, unique factorization here means that every nonzero ideal is a product of atoms, uniquely up to order. There is no need to worry about associates!

Norms make the ideal monoid atomic

Atomicity

Every nonzero ideal of $\mathcal{O}_D$ is a product of atoms.

We assign the well-ordering proof on $\|I\|$ as homework. The key input is

$$\|IJ\| = \|I\|\|J\|.$$

If a nonunit ideal is not an atom, split it into two nonunit ideals. Their positive integral norms are strictly smaller, so the process cannot descend forever.

It remains to prove the ideal version of Euclid's lemma.

The fundamental lemma is the last gate

Euclid's lemma for ideals

If P is an atom of $\mathrm{Id}(\mathcal{O}_D)$ and

$$P \mid IJ,$$

then

$$P \mid I \quad \text{or} \quad P \mid J.$$

Atomicity plus this statement will imply that $\mathrm{Id}(\mathcal{O}_D)$ is a UFM.

The proof uses the reversal

$$P \mid I \iff P \supseteq I$$

and the ideal sum $P + I$. We pick this up tomorrow.

DAY 6

Paradise regained, continued

Euclid's lemma returns in ideal form.

The ideal sum plays the role of a gcd

Let P be an atom and suppose

$$P \mid IJ.$$

If $P \mid I$, we are done, so assume $P \nmid I$.

Consider $P + I$. Since

$$P + I \supseteq P,$$

containment-divisibility gives

$$P + I \mid P.$$

Because P is an atom,

$$P + I = (1) \quad \text{or} \quad P + I = P.$$

The nontrivial case forces $P \mid J$

If $P + I = P$, then $I \subseteq P$, so $P \mid I$, contradicting our assumption. Therefore

$$P + I = (1).$$

Multiply by J:

$$PJ + IJ = J.$$

Since $P \mid IJ$, write $IJ = PS$. Then

$$P(J + S) = J,$$

so $P \mid J$.

Conclusion

Every atom in $\mathrm{Id}(\mathcal{O}_D)$ is prime; hence $\mathrm{Id}(\mathcal{O}_D)$ is a UFM.

This is the familiar Euclid lemma in new clothing

In $\mathbb{Z}$, a gcd can be encoded by an ideal sum:

$$(p) + (a) = (\gcd(p, a)).$$

If a prime $p \nmid a$, then

$$(p) + (a) = (1),$$

which is Bezout's identity. Multiplying by b and using $p \mid ab$ forces $p \mid b$.

The ideal proof is not merely analogous to the integer proof. It is the *same* proof, after replacing gcds by ideal sums and divisibility by reverse containment.

Atoms in the ideal monoid are prime ideals

For an atom $P \in \mathrm{Id}(\mathcal{O}_D)$, Euclid's lemma says

$$P \mid IJ \Longrightarrow P \mid I \text{ or } P \mid J.$$

Using divide $\leftrightarrow$ contain, this becomes

$$P \supseteq IJ \Longrightarrow P \supseteq I \text{ or } P \supseteq J.$$

Prime ideal

A proper ideal P of a ring R is prime if

$$P \supseteq IJ \Longrightarrow P \supseteq I \text{ or } P \supseteq J.$$

Thus every atom of $\mathrm{Id}(\mathcal{O}_D)$ is a prime ideal.

Prime ideals have three equivalent faces

For an ideal $P \subseteq R$, the following are equivalent:

1. P is a prime ideal;
2. $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in P$;
3. R/P is a domain.

In $\mathcal{O}_D$, the nonzero prime ideals are exactly the atoms of $\mathrm{Id}(\mathcal{O}_D)$.

The zero ideal is also prime because $\mathcal{O}_D$ is a domain, but it does not belong to our nonzero ideal monoid.

Unique factorization of ideals, in its standard form

Fundamental theorem for quadratic ideals

Every nonzero ideal of $\mathcal{O}_D$ factors as a product of nonzero prime ideals, uniquely up to order.

This is the form in which unique factorization of ideals usually appears in algebraic number theory textbooks.

The next problem is no longer whether factorization exists. It is to identify the prime ideals and understand how ordinary primes behave inside $\mathcal{O}_D$.

DAY 7

Factoring primes

Making Bill Gates proud

Every prime ideal lies over one rational prime

Proposition

Every nonzero prime ideal $P \subseteq \mathcal{O}_D$ divides (p) for a unique rational prime p.

Since ideal divisibility reverses containment, this is equivalent to saying

$$(p) \subseteq P$$

for a unique prime $p \in \mathbb{Z}$. When $(p) \subseteq P$, we say p **lies below** P, or P **lies above** p.

The proof studies the contraction

$$P \cap \mathbb{Z},$$

which is itself a prime ideal of $\mathbb{Z}$.

The contraction cannot be the zero ideal

The prime ideals of $\mathbb{Z}$ are

$$(0), (2), (3), (5), \ldots.$$

Choose $0 \neq \alpha \in P$. Since P is an ideal,

$$0 \neq \mathrm{N}(\alpha) = \alpha\tilde{\alpha} \in P \cap \mathbb{Z}.$$

Thus

$$P \cap \mathbb{Z} \neq (0),$$

so $P \cap \mathbb{Z} = (p)$ for some rational prime p. Hence $(p) \subseteq P$, or $P \mid (p)$.

The rational prime below P is unique

If P contained both (p) and (q) for distinct rational primes, then Bezout would give integers x, y with

$$px + qy = 1.$$

Therefore $1 \in P$, contradicting that P is proper.

So each nonzero prime ideal lies over exactly one rational prime.

Immediate consequence

There are infinitely many prime ideals of $\mathcal{O}_D$: factor $(2), (3), (5), \ldots$, and choose one prime ideal above each rational prime.

Norm leaves only three factorization patterns

Suppose

$$(p) = P_1 \cdots P_g.$$

Since

$$(\|(p)\|) = (p)(\tilde{p}) = (p^2),$$

we have $\|(p)\| = p^2$. Multiplicativity of ideal norm leaves three possibilities:

1. (p) is prime: p is **inert**;
2. $(p) = P_1 P_2$ with $P_1 \neq P_2$, both of norm p: p **splits**;
3. $(p) = P^2$ with $\|P\| = p$: p **ramifies**.

Gaussian integers reveal the pattern experimentally

In $\mathbb{Z}[i]$, where every ideal is principal,

$$2 = (1+i)(1-i), \qquad 5 = (2+i)(2-i),$$

$$13 = (2+3i)(2-3i),$$

while $3, 7, 11$ remain irreducible.

But $1 - i = (-i)(1+i)$, so the two prime ideals above 2 coincide. Thus

$$(2) = (1+i)^2$$

up to a unit: 2 ramifies, rather than splits.

The polynomial $x^2 + 1$ shows the same trichotomy

Modulo the corresponding primes,

p	$x^2 + 1 \pmod{p}$
2	$(x+1)^2$
3	irreducible
5	$(x-2)(x+2)$
7	irreducible
11	irreducible
13	$(x-5)(x+5)$

The polynomial factorization pattern matches ramification, inertia, and splitting in $\mathbb{Z}[i]$.

Every quadratic ring of integers has a defining polynomial

Let

$$m(x) = \begin{cases} x^2 - D, & D \equiv 2, 3 \pmod 4, \\ x^2 - x + \dfrac{1-D}{4}, & D \equiv 1 \pmod 4. \end{cases}$$

Then $m(\tau) = 0$, and

$$\mathcal{O}_D = \mathbb{Z}[\tau] \simeq \mathbb{Z}[x]/(m(x)),$$

with $\tau \leftrightarrow x$.

This identity explains why reducing $m(x)$ modulo p should control the ideal (p).

Prime factorization mirrors polynomial factorization

How to factor primes

If $m(x)$ is irreducible modulo p, then (p) is a prime ideal of $\mathcal{O}_D$.
If

$$m(x) \equiv (x-a)(x-b) \pmod{p},$$

then

$$(p) = (p, \tau - a)(p, \tau - b).$$

Both factors are prime ideals of norm p, and they coincide exactly when $a \equiv b \pmod{p}$.

The proof is the business of Day 8.

DAY 8

Factoring primes, continued

Quotient rings do some heavy lifting.

Irreducibility modulo p makes (p) prime

Suppose $m(x)$ is irreducible modulo p. Then

$$\mathbb{F}_p[x]/(m(x))$$

is a field, hence a domain. On the other hand,

$$\begin{aligned}\mathcal{O}_D/(p) &\simeq (\mathbb{Z}[x]/(m(x)))/(p)\\ &\simeq (\mathbb{Z}[x]/(p))/(m(x))\\ &\simeq \mathbb{F}_p[x]/(m(x)).\end{aligned}$$

Therefore $\mathcal{O}_D/(p)$ is a domain, so (p) is a prime ideal.

A root modulo p produces a prime ideal of norm p

Suppose

$$m(x) \equiv (x-a)(x-b) \pmod{p},$$

and define

$$P_1 = (p, \tau - a), \qquad P_2 = (p, \tau - b).$$

Then

$$\begin{aligned} \mathcal{O}_D/P_1 &\simeq \mathbb{F}_p[x]/(x-a, m(x)) \\ &\simeq \mathbb{F}_p[x]/(x-a) \\ &\simeq \mathbb{F}_p. \end{aligned}$$

Thus P_1 is prime and $\|P_1\| = p$. The same holds for P_2.

The two prime ideals multiply to (p)

Their product is

$$P_1P_2 = (p^2, p(\tau - a), p(\tau - b), (\tau - a)(\tau - b)).$$

Write

$$m(x) = (x - a)(x - b) + pg(x), \qquad g(x) \in \mathbb{Z}[x].$$

Since $m(\tau) = 0$,

$$(\tau - a)(\tau - b) = -pg(\tau).$$

Hence

$$P_1P_2 = (p)J, \qquad J = (p, \tau - a, \tau - b, -g(\tau)).$$

Norms finish the product calculation

Taking ideal norms in

$$P_1 P_2 = (p)J$$

gives

$$p^2 = p^2 \|J\|.$$

Therefore $\|J\| = 1$, so $J = (1)$. Thus

$$\boxed{(p) = P_1 P_2.}$$

This proof avoids a direct Bezout computation inside the four-generator ideal: the norm detects that the leftover factor must be the unit ideal.

The roots coincide exactly when the ideals coincide

If $a \equiv b \pmod{p}$, then $b = a + pk$ and

$$(p, \tau - a) = (p, \tau - b + pk) = (p, \tau - b).$$

Conversely, if $a \not\equiv b \pmod{p}$, then $P_1 + P_2$ contains both p and

$$(\tau - a) - (\tau - b) = b - a.$$

Since $\gcd(p, b - a) = 1$, we have $P_1 + P_2 = (1)$. Equal proper ideals could not have unit sum, so $P_1 \neq P_2$.

Example: factor small primes in $\mathbb{Z}[\sqrt{-5}]$

Here $m(x) = x^2 + 5$.

p	$m(x) \pmod p$	(p)
2	$(x+1)^2$	$(2, 1+\sqrt{-5})^2$
3	$(x+1)(x-1)$	$(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$
5	x^2	$(5, \sqrt{-5})^2 = (\sqrt{-5})^2$
7	irreducible	(7) prime

The factorization of elements from Day 3 has now become a systematic factorization of ideals.

Ramification is controlled by the discriminant

For

$$m(x) = x^2 + bx + c,$$

let the **discriminant** be $\Delta = b^2 - 4c$. In our quadratic rings,

$$\Delta = \begin{cases} 4D, & D \equiv 2, 3 \pmod 4, \\ D, & D \equiv 1 \pmod 4. \end{cases}$$

Ramification criterion

A rational prime p ramifies in $\mathcal{O}_D$ if and only if $p \mid \Delta$.

Consequently only finitely many primes ramify.

A repeated root forces $p \mid \Delta$

If p ramifies, then for some r,

$$m(x) \equiv (x - r)^2 = x^2 - 2rx + r^2 \pmod{p}.$$

Comparing coefficients gives

$$b \equiv -2r, \qquad c \equiv r^2 \pmod{p}.$$

Therefore

$$\Delta = b^2 - 4c \equiv (-2r)^2 - 4r^2 \equiv 0 \pmod{p}.$$

So ramification implies $p \mid \Delta$.

A discriminant divisor forces a repeated root

Assume $p \mid \Delta$.

If p is odd, then

$$c \equiv b^2/4 \pmod{p},$$

so

$$m(x) \equiv x^2 + bx + b^2/4 = (x + b/2)^2 \pmod{p}.$$

If $p = 2$, then necessarily $D \equiv 2, 3 \pmod 4$, and

$$m(x) = x^2 - D$$

is a square modulo 2. Thus p ramifies.

Only the primes dividing the discriminant can ramify; split and inert primes, by contrast, occur infinitely often.

A new arithmetic question: what are the units?

In $\mathbb{Z}[\sqrt{2}]$, let

$$\epsilon = 1 + \sqrt{2}.$$

Since $\mathrm{N}(\epsilon) = -1$, every power ϵ^n, $n \in \mathbb{Z}$, is again a unit. Thus the unit group is infinite.

We conjecture that

$$\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1+\sqrt{2})^n : n \in \mathbb{Z}\}.$$

Over the next two days, we explore this phenomenon for every real quadratic ring of integers.

DAY 9

Units

. . . and an equation having almost nothing to do with Pell.

Tiny powers give a proof of irrationality

An aside, motivated by the first-year lectures: Let

$$\eta = \sqrt{2} - 1, \qquad 0 < \eta < 1.$$

Then $\eta^n \in \mathbb{Z}[\sqrt{2}]$ and $\eta^n \to 0$.

If $\sqrt{2} = r/s \in \mathbb{Q}$ with $r, s > 0$, write

$$\eta^n = a_n + b_n\sqrt{2} = \frac{a_n s + b_n r}{s}.$$

The numerator is a positive integer, so

$$\eta^n \geq \frac{1}{s}$$

for every n, contradicting $\eta^n \to 0$. Thus $\sqrt{2} \notin \mathbb{Q}$.

The same argument detects rational algebraic integers

The same idea applies also to $\theta = 2^{1/3}$: if $\theta = r/s$, then powers of $\theta - 1$ lie in a fixed 1-dimensional lattice such as $s^{-2}\mathbb{Z}$, yet tend to zero.

The general conclusion is:

Rational algebraic integers

If a real number α is a root of a monic polynomial in $\mathbb{Z}[x]$, then

$$\alpha \in \mathbb{Q} \quad \Longrightarrow \quad \alpha \in \mathbb{Z}.$$

This is a different route to a familiar consequence of the rational root theorem.

Norm ± 1 characterizes units

Now back to business. For $\epsilon \in \mathcal{O}_D$,

$$\epsilon \in \mathcal{O}_D^\times \quad \iff \quad \mathrm{N}(\epsilon) = \pm 1.$$

If $D < 0$, the positive-definite norm makes the answer finite:

$$\mathcal{O}_D^\times = \begin{cases} \{\pm 1\}, & D \neq -1, -3, \\ \{\pm 1, \pm i\}, & D = -1, \\ \left\{ \pm 1, \dfrac{\pm 1 \pm \sqrt{-3}}{2} \right\}, & D = -3. \end{cases}$$

So the possibilities are the second roots of unity, the fourth roots of unity, and the sixth roots of unity.

Real quadratic rings have one fundamental unit

Target theorem

If $D > 1$ is squarefree, there is a smallest unit $\epsilon_0 > 1$. For this ϵ_0,

$$\mathcal{O}_D^\times = \{\pm\epsilon_0^m : m \in \mathbb{Z}\}.$$

Examples:

D	ϵ_0
2	$1+\sqrt{2}$
3	$2+\sqrt{3}$
5	$(1+\sqrt{5})/2$

The proof has three steps: existence, minimality, and generation.

Lagrange reduces existence to the so-called Pell equation

Lagrange's theorem

If $D > 0$ is not a square, then there are integers x, y, not $(\pm 1, 0)$, such that

$$x^2 - Dy^2 = 1.$$

Then

$$\epsilon = x + y\sqrt{D}$$

is a nontrivial unit.

We describe two methods of proof: one where we pull a rabbit out of a hat, and another utilizing Diophantine approximation plus arithmetic in $\mathbb{Z}[\sqrt{D}]$.

We run Euclid on $\sqrt{7}$ and 1

At each step, split off the integer part, invert the remainder, and continue:

$$\begin{aligned}
\sqrt{7} &= 2 + (\sqrt{7} - 2), \\
\frac{1}{\sqrt{7} - 2} &= \frac{\sqrt{7} + 2}{3} = 1 + \frac{\sqrt{7} - 1}{3}, \\
\frac{3}{\sqrt{7} - 1} &= \frac{\sqrt{7} + 1}{2} = 1 + \frac{\sqrt{7} - 1}{2}, \\
\frac{2}{\sqrt{7} - 1} &= \frac{\sqrt{7} + 1}{3} = 1 + \frac{\sqrt{7} - 2}{3}, \\
\frac{3}{\sqrt{7} - 2} &= 4 + (\sqrt{7} - 2).
\end{aligned}$$

The remainder has returned to $\sqrt{7} - 2$, so the process repeats. The quotients are

$$2, 1, 1, 1, 4, 1, 1, 1, 4, \ldots.$$

I believe in the power of magic

Write the quotients as $a_0, a_1, \cdots = 2, 1, 1, 1, 4, 1, 1, 1, \ldots$. Start with

$$P_{-2} = 0, \quad P_{-1} = 1, \qquad Q_{-2} = 1, \quad Q_{-1} = 0,$$

and recursively define

$$P_n = a_n P_{n-1} + P_{n-2}, \qquad Q_n = a_n Q_{n-1} + Q_{n-2}.$$

The recursion produces

n	-2	-1	0	1	2	3	4	5	6	7
a_n			2	1	1	1	4	1	1	1
P_n	0	1	2	3	5	8	37	45	82	127
Q_n	1	0	1	1	2	3	14	17	31	48
$P_n^2 - 7Q_n^2$			-3	2	-3	1	-3	2	-3	1

The Pell row picks out nontrivial units

The error row equals 1 at $n = 3$ and $n = 7$. Thus the (P_n, Q_n) are

$$(P_3, Q_3) = (8, 3) \qquad (P_7, Q_7) = (127, 48),$$

with

$$8^2 - 7 \cdot 3^2 = 1, \qquad 127^2 - 7 \cdot 48^2 = 1.$$

Therefore

$$8 + 3\sqrt{7}, \qquad 127 + 48\sqrt{7}$$

are nontrivial units in $\mathbb{Z}[\sqrt{7}]$.

Proving that this method succeeds for arbitrary $D > 0$ requires the theory of continued fractions. We'll sidestep this.

Distance modulo $\mathbb{Z}$ measures approximation

For $\alpha \in \mathbb{R}$, define the **distance modulo** $\mathbb{Z}$

$$\|\alpha\|_{\mathbb{R}/\mathbb{Z}} = \min_{n \in \mathbb{Z}} |n - \alpha|.$$

Dirichlet's approximation theorem

For every $Q \in \mathbb{Z}^+$, some integer q with $1 \leq q \leq Q$ satisfies

$$\|q\alpha\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{1}{Q+1}.$$

This is a pigeonhole theorem on the circle $\mathbb{R}/\mathbb{Z}$.

Pigeonhole proof of Dirichlet's theorem

Place

$$0, \alpha, 2\alpha, \ldots, Q\alpha$$

on the circle $\mathbb{R}/\mathbb{Z}$. Two points, say $q_0\alpha$ and $q_1\alpha$ with $q_0 < q_1$, are within $1/(Q+1)$. Taking $q = q_1 - q_0$, we have $1 \leq q \leq Q$ and

$$\|q\alpha\|_{\mathbb{R}/\mathbb{Z}} = \|(q_1 - q_0)\alpha\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{1}{Q+1}.$$

Approximate $\sqrt{D}$, then measure the Pell error

Choose $1 \le q \le Q$ with

$$\|q\sqrt{D}\|_{\mathbb{R}/\mathbb{Z}} \le \frac{1}{Q+1},$$

and let p be the nearest integer to $q\sqrt{D}$. Then

$$|p - q\sqrt{D}| \le \frac{1}{Q+1}.$$

Also

$$|p + q\sqrt{D}| \le |p - q\sqrt{D}| + 2q\sqrt{D} < 1 + 2Q\sqrt{D}.$$

Every approximation is a bounded Pell near-miss

Multiplying the two conjugate errors gives

$$\begin{aligned} |p^2 - Dq^2| &= |p - q\sqrt{D}|\,|p + q\sqrt{D}| \\ &< \frac{1 + 2Q\sqrt{D}}{Q+1} \\ &\le 2\sqrt{D}. \end{aligned}$$

Thus for every Q we produce positive integers p, q satisfying

$$|p^2 - Dq^2| < 2\sqrt{D}.$$

This is not yet Pell's equation, but the error belongs to a fixed finite set of integers.

There are infinitely many near-misses

A fixed pair (p, q) can arise for only finitely many Q, because

$$Q + 1 \leq \frac{1}{\|q\sqrt{D}\|_{\mathbb{R}/\mathbb{Z}}},$$

and $\sqrt{D} \notin \mathbb{Q}$.

Therefore infinitely many positive pairs (p, q) satisfy

$$|p^2 - Dq^2| < 2\sqrt{D}.$$

By pigeonhole, there is a fixed nonzero integer k, with $|k| \leq 2\sqrt{D}$, such that

$$S = \{p + q\sqrt{D} : p, q > 0,\ \mathrm{N}(p + q\sqrt{D}) = k\}$$

is infinite.

A quotient has norm 1, but may not be integral

For $\alpha, \alpha' \in S$,

$$\mathsf{N}\left(\frac{\alpha}{\alpha'}\right) = 1.$$

This looks like a unit. But

$$\frac{\alpha}{\alpha'} = \frac{\alpha\tilde{\alpha'}}{\alpha'\tilde{\alpha'}} = \frac{\alpha\tilde{\alpha'}}{k}$$

lies a priori only in $\mathbb{Q}[\sqrt{D}]$, not in $\mathbb{Z}[\sqrt{D}]$.

The remaining issue

Choose α, α' so that $k \mid \alpha\tilde{\alpha'}$.

Day 10 uses pigeonhole one more time.

DAY 10

Units, continued

Pigeonhole: A strategy so nice, we use it twice.

Pigeonhole again, now modulo k

The quotient ring

$$\mathbb{Z}[\sqrt{D}]/(k)$$

has k^2 elements. Since S is infinite, choose distinct $\alpha, \alpha' \in S$ in the same residue class modulo k, with $\alpha > \alpha'$.

Then

$$\tilde{\alpha} \equiv \tilde{\alpha'} \pmod{k},$$

and hence

$$\alpha\tilde{\alpha'} \equiv \alpha\tilde{\alpha} = k \equiv 0 \pmod{k}.$$

Thus $\alpha\tilde{\alpha'}/k \in \mathbb{Z}[\sqrt{D}]$.

The quotient is finally a nontrivial unit

Set

$$\eta = \frac{\alpha}{\alpha'} = \frac{\alpha\tilde{\alpha'}}{k}.$$

Then $\eta \in \mathbb{Z}[\sqrt{D}]$ and

$$\mathsf{N}(\eta) = \frac{\mathsf{N}(\alpha)}{\mathsf{N}(\alpha')} = 1.$$

Because $\alpha > \alpha' > 0$, we also have $\eta > 1$. Writing

$$\eta = x + y\sqrt{D}$$

gives a nontrivial solution

$$x^2 - Dy^2 = 1.$$

This proves Lagrange's theorem.

A unit bigger than 1 has positive coordinates

Lemma

If $\eta = a + b\sqrt{D} \in \mathcal{O}_D^\times$ and $\eta > 1$, then $a, b > 0$.

Since $\mathrm{N}(\eta) = \pm 1$,

$$\tilde{\eta} = \pm \eta^{-1},$$

so $|\tilde{\eta}| < 1 < \eta$. Therefore

$$2a = \eta + \tilde{\eta} > 0, \qquad 2b\sqrt{D} = \eta - \tilde{\eta} > 0.$$

Hence $a, b > 0$. (Note that this argument applies equally well whether a, b are integers or half-integers.)

There is a smallest unit greater than 1

Let $\epsilon > 1$ be any unit furnished by Pell's equation. Consider units

$$1 < \eta \leq \epsilon, \qquad \eta = a + b\sqrt{D}.$$

The lemma gives $a, b > 0$, and therefore

$$0 < a < \eta \leq \epsilon, \qquad 0 < b\sqrt{D} < \eta \leq \epsilon.$$

Only finitely many allowed integer or half-integer pairs (a, b) satisfy these bounds. Thus the interval $(1, \epsilon]$ contains finitely many units, and one of them is smallest. Call it ϵ_0.

Minimality forces every positive unit to be a power

Let $\eta > 0$ be a unit. Choose $m \in \mathbb{Z}$ such that

$$\epsilon_0^m \leq \eta < \epsilon_0^{m+1}.$$

If $\eta \neq \epsilon_0^m$, then

$$1 < \eta \epsilon_0^{-m} < \epsilon_0.$$

But $\eta \epsilon_0^{-m}$ is a unit, contradicting the minimality of ϵ_0.

Hence every positive unit equals ϵ_0^m. Allowing a sign,

$$\boxed{\mathcal{O}_D^\times = \{\pm \epsilon_0^m : m \in \mathbb{Z}\}.}$$

Pigeons prove $\mathbb{Z}[i]$ is a PID

Let $(0) \neq I \subseteq \mathbb{Z}[i]$ and put $m = \|I\|$. Consider Gaussian integers $a + bi$ satisfying

$$0 \leq a \leq \sqrt{m}, \qquad 0 \leq b < \sqrt{m}.$$

There are

$$(1 + \lfloor \sqrt{m} \rfloor)\lceil \sqrt{m} \rceil > m$$

of these but only m residue classes modulo I. Hence, two are congruent modulo I.

The small difference generates the ideal

Subtract the two congruent values to obtain

$$0 \neq \alpha = A + Bi \in I,$$

with

$$|A| \leq \sqrt{m}, \qquad |B| < \sqrt{m}.$$

Since $(\alpha) \subseteq I$, write

$$(\alpha) = IJ.$$

Taking norms,

$$m\|J\| = \|(\alpha)\| = A^2 + B^2 < 2m.$$

Thus $\|J\| < 2$, so $\|J\| = 1$, $J = (1)$, and

$$I = (\alpha).$$

Every ideal is principal; hence $\mathbb{Z}[i]$ is a UFD.

Look, ma, no division algorithm!

The standard first-year proof that $\mathbb{Z}[i]$ is a UFD proceeds through Euclidean division. Our route is different:

$$\text{finite quotient} \longrightarrow \text{small nonzero element of } I \longrightarrow \text{norm comparison} \longrightarrow I \text{ principal.}$$

This geometry-of-numbers pattern proves principality in rings where no obvious division algorithm is available.

DAY 11

A touch of class

Let the ideal theory do the work for us!

Recycling our $\mathbb{Z}[i]$ proof

For a nonzero ideal I of norm m, our method is:

1. place more than m algebraic integers in a carefully shaped region;
2. subtract two that are congruent modulo I;
3. obtain $0 \neq \alpha \in I$ with small norm;
4. write $(\alpha) = IJ$ and bound $\|J\|$;
5. classify the few ideals whose norms survive the bound.

For $\mathbb{Z}[i]$, the last bound forced $J = (1)$. Other rings may leave a short list of small possibilities.

Apply the machine to $\mathbb{Z}[\sqrt{6}]$

Let $(0) \neq I \subseteq \mathbb{Z}[\sqrt{6}]$ and $m = \|I\|$. Consider $a + b\sqrt{6}$ with

$$0 \leq a \leq 6^{1/4} m^{1/2}, \qquad 0 \leq b < m^{1/2}/6^{1/4}.$$

There are more than m choices, so two are congruent modulo I. Their difference gives

$$0 \neq \alpha = A + B\sqrt{6} \in I$$

with

$$|A| \leq 6^{1/4} m^{1/2}, \qquad |B| < m^{1/2}/6^{1/4}.$$

Only norms 1 and 2 can remain

Write

$$(\alpha) = IJ.$$

Then

$$\|J\| = \frac{|A^2 - 6B^2|}{m} < \sqrt{6} < 3.$$

Thus

$$\|J\| = 1 \quad \text{or} \quad 2.$$

If $\|J\| = 1$, then $J = (1)$ and $I = (\alpha)$ is principal.

The only obstruction could be an ideal of norm 2.

The norm-two obstruction is itself principal

If $\|J\| = 2$, then J is an atom, hence a prime ideal above 2.

But pure thought gives

$$(2) = (\sqrt{6}+2)(\sqrt{6}-2),$$

and each factor has ideal norm 2. Therefore

$$J = (\sqrt{6}+2) \quad \text{or} \quad J = (\sqrt{6}-2).$$

So $J = (\beta)$ is principal. From

$$(\alpha) = IJ = I(\beta) = \beta I$$

we obtain

$$I = (\alpha/\beta).$$

Hence $\mathbb{Z}[\sqrt{6}]$ is a UFD.

A more delicate example: $\mathcal{O}_{-19}$

Let

$$\tau = \frac{1+\sqrt{-19}}{2}, \qquad \mathcal{O}_{-19} = \mathbb{Z}[\tau].$$

For $(0) \neq I \subseteq \mathcal{O}_{-19}$ with $\|I\| = m$, use points $a + b\tau$ in the rectangle

$$0 \leq a \leq 5^{1/4} m^{1/2}, \qquad 0 \leq b < m^{1/2}/5^{1/4}.$$

Pigeonhole again gives

$$0 \neq \alpha = A + B\tau \in I$$

with the corresponding bounds on A, B.

The leftover ideal has norm at most 5

Write $(\alpha) = IJ$. Since

$$\mathrm{N}(A + B\tau) = A^2 + AB + 5B^2,$$

the chosen bounds yield

$$\|J\| = \frac{A^2 + AB + 5B^2}{m} < 1 + 2\sqrt{5} < 6.$$

Thus

$$\|J\| \in \{1, 2, 3, 4, 5\}.$$

The problem of proving every ideal principal has been reduced to understanding ideals of five small norms. If $\|J\| = 1$, then $J = (1)$.

Norms 2 and 3 are impossible

The minimal polynomial of τ is

$$m(x) = x^2 - x + 5.$$

Modulo 2,

$$m(x) \equiv x^2 + x + 1$$

is irreducible, so (2) is prime of norm 4. There is no ideal of norm 2.

Modulo 3,

$$m(x) \equiv x^2 + 2x + 2$$

is irreducible, so (3) is prime of norm 9. There is no ideal of norm 3.

Norm 4 leaves only the principal ideal (2)

If $\|J\| = 4$, factor J into prime ideals. Every prime factor must have norm a power of 2, hence lie above 2.

But (2) is the unique prime ideal above 2, and it already has norm 4. Therefore

$$J = (2),$$

which is principal.

The cases $\|J\| = 1, 2, 3, 4$ are settled. Only the possibility $\|J\| = 5$ remains.

Norm 5 also gives a principal leftover

Modulo 5,

$$m(x) = x^2 - x + 5 \equiv x(x-1).$$

Thus

$$(5) = (5, \tau)(5, \tau - 1) = (\tau)(\tilde{\tau}),$$

and both prime factors have norm 5.

Hence an ideal J of norm 5 is (τ) or $(\tilde{\tau})$, in either case principal.

Every possible leftover J is principal, so every ideal I is principal. Therefore

$$\boxed{\mathcal{O}_{-19} \text{ is a UFD.}}$$

DAY 12

Class consciousness

What flavors are your ideals?

Run the same machine in $\mathbb{Z}[\sqrt{-5}]$

Let $(0) \neq I \subseteq \mathbb{Z}[\sqrt{-5}]$, $m = \|I\|$. The same rectangle argument produces

$$0 \neq \alpha = A + B\sqrt{-5} \in I$$

with

$$|A| \leq 5^{1/4} m^{1/2}, \qquad |B| < m^{1/2}/5^{1/4}.$$

Writing $(\alpha) = IJ$,

$$\|J\| = \frac{A^2 + 5B^2}{m} < 2\sqrt{5} < 5.$$

So only norms $1, 2, 3, 4$ can occur.

Three small prime ideals control every class

Set

$$P_2 = (2, 1 + \sqrt{-5}),$$

$$P_3 = (3, 1 + \sqrt{-5}), \qquad \tilde{P}_3 = (3, 1 - \sqrt{-5}).$$

We know

$$(2) = P_2^2, \qquad (3) = P_3 \tilde{P}_3,$$

and

$$(1 + \sqrt{-5}) = P_2 P_3, \qquad (1 - \sqrt{-5}) = P_2 \tilde{P}_3.$$

These identities turn each possible small J into one of two ideal shapes.

Norms 1 and 2 give the two shapes

If $\|J\| = 1$, then $J = (1)$, so

$$I = (\alpha) = \lambda(1).$$

If $\|J\| = 2$, then $J = P_2$, and

$$(\alpha) = IP_2.$$

Multiplying by P_2,

$$(\alpha)P_2 = IP_2^2 = I(2) = 2I.$$

Hence

$$I = \frac{\alpha}{2}P_2 = \lambda P_2.$$

Norms 3 and 4 give the same two shapes

If $\|J\| = 3$, then $J = P_3$ or $\tilde{P_3}$. For example, if $J = P_3$,

$$(\alpha) = IP_3.$$

Multiplying by P_2 and using $P_2P_3 = (1 + \sqrt{-5})$,

$$\alpha P_2 = (1 + \sqrt{-5})I,$$

so $I = \lambda P_2$. The conjugate case is identical.

If $\|J\| = 4$, then $J = (2)$, so $I = \lambda(1)$.

Every ideal has one of two flavors

Every nonzero ideal of $\mathbb{Z}[\sqrt{-5}]$ is a dilation of exactly one of

$$(1) \qquad \text{or} \qquad P_2 = (2, 1 + \sqrt{-5}).$$

We name these two flavors:

$\lambda(1)$	λP_2
vanilla	chocolate

The vanilla ideals are principal. The chocolate ideals are nonprincipal.

The flavor profile is not merely a set: multiplying ideals multiplies flavors! For instance, vanilla $\times$ chocolate $=$ chocolate, while chocolate $\times$ chocolate $=$ vanilla.

The ideal flavors of $\mathbb{Z}[\sqrt{-5}]$ form a group (OK, the group) of order 2.

Dilation equivalence defines the class group

Let $K = \mathbb{Q}(\sqrt{D})$. For $I, J \in \mathrm{Id}(\mathcal{O}_D)$, say that I and J are **dilation equivalent**, and write

$$I \sim J$$

if $I = \lambda J$ for some $\lambda \in K^\times$.

Define the **class group**

$$\mathrm{Cl}(\mathcal{O}_D) = \mathrm{Id}(\mathcal{O}_D)/\sim,$$

and multiply classes by

$$[I][J] = [IJ].$$

For $\mathbb{Z}[\sqrt{-5}]$,

$$\mathrm{Cl}(\mathcal{O}_{-5}) = \{[(1)], [P_2]\}.$$

We assign well-definedness of the multiplication as homework.

The principal multiple lemma supplies inverses

Associativity and commutativity descend from ideal multiplication, and $[(1)]$ is the identity.

Given $[I]$, choose I' with

$$II' = (\alpha).$$

Then

$$[I][I'] = [II'] = [(\alpha)] = [(1)].$$

Thus every class has an inverse.

Conclusion

$\mathrm{Cl}(\mathcal{O}_D)$ is an abelian group.

A norm bound makes the class group finite

The geometry argument gives a constant C_D such that for every nonzero ideal I, some ideal J satisfies

$$(\alpha) = IJ, \qquad \|J\| \leq C_D.$$

Passing to classes,

$$[(1)] = [I][J],$$

so

$$[I] = [J]^{-1}.$$

Only finitely many ideals have norm at most C_D. Therefore only finitely many classes occur:

$$\boxed{\mathrm{Cl}(\mathcal{O}_D) \text{ is finite.}}$$

We assign the finiteness details as homework.

The identity class is exactly the principal ideals

If $I = (\alpha)$, then

$$I = \alpha(1),$$

so $[I] = [(1)]$.

Conversely, if $[I] = [(1)]$, then

$$I = \lambda(1)$$

for some $\lambda \in K^\times$. Since $I \subseteq \mathcal{O}_D$ and $\lambda \in I$, we have $\lambda \in \mathcal{O}_D$. Hence

$$I = (\lambda)$$

is principal.

Thus the class group measures exactly the obstruction to principality.

DAY 13

Rabinowitsch

Prime producing polynomials meet unique factorization. Worlds collide.

Trivial class group is equivalent to unique factorization

Because $[I] = [(1)]$ exactly when I is principal,

$$\mathrm{Cl}(\mathcal{O}_D) \text{ trivial} \iff \mathcal{O}_D \text{ is a PID} \iff \mathcal{O}_D \text{ is a UFD.}$$

But a nontrivial class group still contains useful information. The opening cube argument did not require every ideal class to vanish; it required only that no class have order 3.

The elementwise power-product principle can fail

In a UFD, if p is prime, ab is a p-th power, and a, b have no common nonunit divisor, then each factor is a p-th power up to a unit.

But in $\mathcal{O}_{-26} = \mathbb{Z}[\sqrt{-26}]$,

$$(1 + \sqrt{-26})(1 - \sqrt{-26}) = 3^3,$$

the two factors have no common nonunit divisor, yet both are irreducible.

The missing hypothesis involves ideals and their classes.

The proper pth power product principle uses the class group

Proper pth power product principle

Let p be prime and $\alpha, \beta \in \mathcal{O}_D \setminus \{0\}$. Suppose

$$\alpha\beta = \gamma^p,$$

the ideals $(\alpha), (\beta)$ have no common nonunit ideal factor, and $\mathrm{Cl}(\mathcal{O}_D)$ has no element of order p. Then

$$\alpha = (p\text{-th power})(\text{unit}),$$

and similarly for β.

Unique ideal factorization isolates a p-th power ideal

From

$$(\alpha)(\beta) = (\gamma)^p$$

and ideal coprimality, unique factorization of ideals gives

$$(\alpha) = I^p, \qquad (\beta) = J^p$$

for some ideals I, J.

In the class group,

$$[(1)] = [(\alpha)] = [I]^p.$$

Thus the order of $[I]$ divides p.

The class-group hypothesis returns us to elements

Since $\mathrm{Cl}(\mathcal{O}_D)$ has no element of order p,

$$[I] = [(1)].$$

Therefore I is principal, say $I = (\lambda)$. Then

$$(\alpha) = I^p = (\lambda^p).$$

Hence

$$\alpha = u\lambda^p$$

for some unit u. The same argument applies to β.

For $\mathcal{O}_{-5}$, whose class group has order 2, the principle applies with $p = 3$; this is the promised route to the statement that $y^2 = x^3 - 5$ has no integer solutions (HW!).

Euler's prime producing machine

Start at 41, then add $2, 4, 6, 8, \ldots$:

$$\begin{aligned} 41 &= 41, \\ 41 + 2 &= 43, \\ 41 + 2 + 4 &= 47, \\ 41 + 2 + 4 + 6 &= 53, \\ 41 + 2 + 4 + 6 + 8 &= 61, \\ 41 + 2 + 4 + 6 + 8 + 10 &= 71. \end{aligned}$$

Every displayed value is prime. After $n - 1$ additions, the running total is

$$41 + 2(1 + 2 + \cdots + (n-1)) = n^2 - n + 41.$$

How long does this prime-producing experiment continue?

Euler's polynomial is a defining polynomial

The values

$$n^2 - n + 41$$

are prime for every integer $0 < n < 41$, but the value at $n = 41$ is obviously composite.

Notice

$$x^2 - x + 41$$

is the minimal polynomial of

$$\tau = \frac{1 + \sqrt{-163}}{2},$$

so it defines $\mathcal{O}_{-163}$.

Prime-producing behavior is about to become a statement about unique factorization.

Rabinowitsch connects prime values and UFDs

Rabinowitsch's theorem

Let $A \geq 2$ and suppose $1 - 4A$ is squarefree. Then

$$n^2 - n + A \text{ is prime for every } 0 < n < A$$

if and only if

$$\mathcal{O}_{1-4A} = \mathbb{Z}\left[\frac{1+\sqrt{1-4A}}{2}\right]$$

is a UFD.

For $A = 41$, this says that Euler's prime run and unique factorization in $\mathcal{O}_{-163}$ are the same phenomenon.

UFD $\Rightarrow$ prime values: assume a composite value

Let

$$m(x) = x^2 - x + A$$

and suppose $\mathcal{O}_{1-4A}$ is a UFD. If $m(n)$ were composite for some $0 < n < A$, then

$$1 < m(n) < A^2.$$

So some prime $p < A$ divides $m(n)$.

Since $m(x)$ has the root n modulo p, the prime p splits or ramifies:

$$(p) = P_1 P_2, \qquad \|P_i\| = p.$$

A principal prime above p would have norm too small

Because the ring is a PID, write $P_1 = (\alpha)$, where

$$\alpha = \frac{a + b\sqrt{1 - 4A}}{2}, \qquad a \equiv b \pmod 2.$$

Then

$$\mathrm{N}(\alpha) = \|P_1\| = p < A.$$

But

$$\mathrm{N}(\alpha) = \frac{a^2 + (4A - 1)b^2}{4}.$$

If $b = 0$, this norm is a square, not the prime p. If $b \neq 0$, then

$$\mathrm{N}(\alpha) \geq A - \frac{1}{4},$$

and integrality forces $\mathrm{N}(\alpha) \geq A$, a contradiction.

The converse needs a small-prime principality criterion

Recall that a prime ideal P **lies above** p if $(p) \subseteq P$.

Small-prime criterion

Let $D < 0$ be squarefree with $D \equiv 1 \pmod 4$. If every rational prime

$$p \leq \sqrt{|D|/3}$$

lies below only principal prime ideals, then $\mathcal{O}_D$ is a PID.

For $D = -19$, only $p = 2$ must be checked, and (2) is inert and principal. This recovers the UFD result far more quickly.

Prime values force every relevant small prime to be inert

Assume $n^2 - n + A$ is prime for $0 < n < A$. To apply the criterion with $D = 1 - 4A$, it suffices to show every prime

$$p \leq \sqrt{(4A-1)/3}$$

is inert.

If not, $m(x) = x^2 - x + A$ has a root modulo p. Because roots pair as r and $1 - r$, choose

$$1 \leq r \leq \frac{p+1}{2} < A.$$

Then $m(r)$ is prime and divisible by p.

The size of the prime value gives the contradiction

Since $0 < r < A$, the hypothesis says $m(r)$ is prime. But

$$m(r) = r^2 - r + A \geq A$$

while

$$p \leq \sqrt{(4A-1)/3} < A.$$

Thus $m(r) > p$, contradicting that the prime number $m(r)$ is divisible by p.

So all relevant small primes are inert. The small-prime criterion then makes $\mathcal{O}_{1-4A}$ a PID, completing Rabinowitsch's theorem once that criterion is proved.

DAY 14

Rabinowitsch, continued

A few primes tell the whole story.

Choose the smallest bad rational prime

Assume the small-prime criterion is false. By well-ordering, let p be the least rational prime lying below a nonprincipal prime ideal.

By hypothesis,

$$p > \sqrt{|D|/3}.$$

The prime p is not inert. Hence

$$m(x) = x^2 - x + \frac{1-D}{4}$$

has a root modulo p. Choose a representative

$$1 \leq r \leq \frac{p+1}{2}.$$

The root produces a smaller integer factor

The chosen bound on r gives

$$\begin{aligned} r^2 - r + \frac{1-D}{4} &\leq \left(\frac{p+1}{2}\right)^2 - \frac{p+1}{2} + \frac{1-D}{4} \\ &= \frac{p^2 - D}{4} \\ &< p^2, \end{aligned}$$

where the last inequality is equivalent to $p^2 > |D|/3$.

Since p divides this positive integer, write

$$r^2 - r + \frac{1-D}{4} = ps$$

with $s < p$.

Minimality makes every prime factor of s principal

Every rational prime dividing s is smaller than p. By minimality of p, all prime ideals above those primes are principal. Therefore

$$(s) = (\pi_1) \cdots (\pi_k)$$

as a product of principal prime ideals.

With $\tau = (1 + \sqrt{D})/2$,

$$(r - \tau)(r - \tilde{\tau}) = \left(r^2 - r + \frac{1 - D}{4} \right) = (p)(\pi_1) \cdots (\pi_k).$$

Unique ideal factorization lets us divide the (π_i) between the two conjugate factors.

After division, (p) splits into principal factors

Successively cancelling the principal prime ideals gives

$$(\pi)(\rho) = (p),$$

where

$$\pi = \frac{r - \tau}{\text{a product of the } \pi_i}, \qquad \rho = \frac{r - \tilde{\tau}}{\text{the complementary product}}.$$

Neither π nor ρ is a unit. For instance, if π were a unit, then $(\rho) = (p)$, so

$$p \mid r - \tilde{\tau} = r - 1 + \tau.$$

That would put $(r-1)/p + (1/p)\tau$ in $\mathcal{O}_D = \mathbb{Z}[\tau]$, impossible.

Norms contradict the choice of p

Taking norms in

$$(\pi)(\rho) = (p)$$

gives

$$|\,\mathrm{N}(\pi)|\,|\,\mathrm{N}(\rho)| = p^2.$$

Both factors exceed 1, so each equals p. Hence (π) and (ρ) are prime ideals above p, and both are principal.

This contradicts the choice of p as lying below a nonprincipal prime ideal. Therefore every prime ideal is principal, and $\mathcal{O}_D$ is a PID.

Four implies forty

The stronger form of the argument says it is enough that

$$n^2 - n + A$$

be prime for

$$0 < n \leq \frac{1}{2}\sqrt{\frac{4A-1}{3}} + \frac{1}{2}.$$

For $A = 41$, the right side is less than 5. Thus checking $n = 1, 2, 3, 4$ proves $\mathcal{O}_{-163}$ is a UFD.

Rabinowitsch's theorem then sends the conclusion back: $n^2 - n + 41$ is prime for every $1 \leq n \leq 40$. So checking $n = 1, 2, 3, 4$ is enough to guarantee the checks will pass for $n = 1, 2, \ldots, 40$. Weird, but that's mathematics, a bottomless well of surprises.

Two classification questions, morally one

Rabinowitsch's theorem raises a natural question:

$$\text{For which } A \geq 2 \text{ is } \mathcal{O}_{1-4A} \text{ a UFD?}$$

More generally, we could ask:

$$\text{For which squarefree } D < 0 \text{ is } \mathcal{O}_D \text{ a UFD?}$$

These questions are morally the same. In HW, you are asked to show that

$$D < -2 \text{ and } \mathcal{O}_D \text{ a UFD} \quad \Longrightarrow \quad D \equiv 1 \pmod 4.$$

Thus, for $D < -3$, every imaginary quadratic UFD must have $D = 1 - 4A$ with $A \geq 2$.

Dickson checks Gauss's list to 1.5 million

Gauss's result and conjecture

Gauss shows that $\mathcal{O}_D$ is a UFD for

$$D = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

He conjectures that there are no others.

Dickson's bound (1911)

Dickson finds no further imaginary quadratic UFDs with

$$|D| \leq 1.5 \cdot 10^6.$$

This is striking numerical evidence, but it doesn't prove anything.

Gronwall–Hecke handle the Riemann-Hypothesis case

The **class number** is

$$h_D = \#\,\mathrm{Cl}(\mathcal{O}_D).$$

Gronwall–Hecke (1913)

If a certain specific variant of the Riemann Hypothesis is true, then

$$h_D \longrightarrow \infty \qquad (D \longrightarrow -\infty).$$

Thus, under this hypothesis, only finitely many imaginary quadratic rings are UFDs.

Heilbronn handles the opposite case

Heilbronn (1934)

If that same variant of the Riemann Hypothesis is false, then

$$h_D \longrightarrow \infty \qquad (D \longrightarrow -\infty).$$

Gronwall–Hecke cover one possibility; Heilbronn covers the other. Hence, unconditionally,

$$\boxed{h_D \longrightarrow \infty!}$$

In particular, only finitely many imaginary quadratic rings are UFDs.

Siegel gives a powerful but ineffective lower bound

Siegel's theorem (1935)

For every $\epsilon > 0$, there is a number $D_0(\epsilon) > 0$ such that, whenever $D < 0$ and $|D| \geq D_0(\epsilon)$,

$$h_D > |D|^{1/2-\epsilon}.$$

The theorem is **ineffective**: it gives no way to compute $D_0(\epsilon)$ from ϵ.

So it proves enormous growth without telling us where that growth must begin.

One disputed proof stands between a list and a theorem

Heilbronn–Linfoot (1934)

There is at most one $D < -163$ for which $\mathcal{O}_D$ is a UFD.

In 1952, Heegner proves that no such exceptional D exists, but his proof is not accepted at the time.

Baker and Stark later give accepted proofs. In 1969, Stark also shows that the gaps in Heegner's argument can be filled.

Thus Gauss's nine examples are the complete list.

The winner is still $n^2 - n + 41$

The classification yields:

$$\mathcal{O}_D \text{ is a UFD for } D < 0$$

exactly for

$$D = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Consequently Euler's polynomial

$$n^2 - n + 41$$

is the undisputed champion of the Rabinowitsch family, not only undefeated but undefeat*able*. No larger A produces primes throughout $0 < n < A$.

Getting real: the landscape changes for $D > 0$

For real quadratic fields, Gauss conjectured that $\mathcal{O}_D$ is a UFD infinitely often.

The Cohen–Lenstra heuristics predict, more precisely, that among the rings $\mathcal{O}_p$, with p prime, a positive proportion have class number 1:

$$\lim_{x\to\infty} \frac{\#\{p \le x : \mathcal{O}_p \text{ is a UFD}\}}{\#\{p \le x\}} = \prod_{\substack{\ell \text{ prime} \\ \ell > 2}} \prod_{j=2}^{\infty} \left(1 - \frac{1}{\ell^j}\right) \approx 0.7544.$$

This is **arithmetic statistics**: a structural question becomes a distribution question.

DAY 15

Stretching

the truth about nonunique factorization

Two failures of uniqueness are not equally bad

Compare

$$\mathbb{Z}[\sqrt{-5}]: \qquad 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

with

$$\mathbb{Z}[\sqrt{-26}]: \qquad 3 \cdot 3 \cdot 3 = (1+\sqrt{-26})(1-\sqrt{-26}).$$

All displayed factors are irreducible. The first identity has equal lengths; the second has lengths 3 and 2.

The Day 2 challenge asks for unequal lengths in $\mathbb{Z}[\sqrt{-5}]$. This was a trick question: no such example exists.

$\mathbb{Z}[\sqrt{-5}]$ has unique factorization length

Theorem

If

$$\pi_1 \cdots \pi_k = \rho_1 \cdots \rho_\ell$$

in $\mathbb{Z}[\sqrt{-5}]$, with all factors irreducible, then

$$k = \ell.$$

The key input is

$$\mathrm{Cl}(\mathcal{O}_{-5}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

Cancel associate factors first. We may then assume no π_i is associate to a ρ_j, and consequently none of these irreducibles is prime.

A nonprime irreducible contributes exactly two prime ideals

Let λ be one of the irreducible factors and write

$$(\lambda) = P_1 \cdots P_g$$

as a product of prime ideals. Since λ is not prime, $g \geq 2$.

No proper subproduct can be principal: otherwise

$$P_{i_1} \cdots P_{i_r} = (\alpha)$$

would split λ into nonunit factors, contradicting irreducibility. In particular, none of the P_i is principal.

Class number 2 rules out three prime-ideal factors

If $g \geq 3$, then $[P_1], [P_2], [P_3]$ are all the unique nontrivial class in $\mathrm{Cl}(\mathcal{O}_{-5})$. Hence

$$[P_1 P_2] = [(1)],$$

so $P_1 P_2 = (\alpha)$ is principal.

The complementary product is also principal, say

$$P_3 \cdots P_g = (\beta).$$

Both α and β are nonunits, while

$$(\lambda) = (\alpha\beta).$$

Thus λ is reducible, a contradiction. Therefore $g = 2$.

Counting prime ideals counts irreducible factors

Each irreducible π_i contributes exactly two prime ideals to the factorization of (π_i). Therefore

$$(\pi_1 \cdots \pi_k)$$

has $2k$ prime-ideal factors.

Likewise,

$$(\rho_1 \cdots \rho_\ell)$$

has 2ℓ prime-ideal factors. The two principal ideals are equal, and ideal factorization is unique, so

$$2k = 2\ell,$$

hence $k = \ell$.

Half-factorial domains remember length but forget factors

Half-factorial domain

An atomic domain R is half-factorial if every equality

$$\pi_1 \cdots \pi_k = \rho_1 \cdots \rho_\ell$$

between products of irreducibles satisfies $k = \ell$.

Thus $\mathbb{Z}[\sqrt{-5}]$ is half-factorial but not a UFD.

More generally, if

$$h_D = \# \operatorname{Cl}(\mathcal{O}_D) = 2,$$

then $\mathcal{O}_D$ is half-factorial.

Minimal principal products encode irreducibles

Anatomy of an irreducible

Suppose prime ideals $P_1, \ldots, P_r$ satisfy

$$P_1 \cdots P_r = (\pi),$$

and no proper nonempty subproduct is principal. Then π is irreducible.

If $\pi = \alpha\beta$ with both factors nonunits, the prime factorization of (α) would be a proper nonempty subproduct of the P_i and would be principal. Contradiction.

Every ideal class contains a prime ideal

Analytic lemma of Landau

Every element of $\mathrm{Cl}(\mathcal{O}_D)$ has the form $[P]$ for some nonzero prime ideal $P \subseteq \mathcal{O}_D$ — indeed, for infinitely many such P.

This is an analogue of Dirichlet's theorem on primes in arithmetic progressions. Both results can be viewed as special cases of the celebrated **Chebotarev density theorem**.

Landau's lemma lets us turn a combinatorial pattern in the class group into actual prime ideals, then into irreducible elements through the anatomy lemma.

A group with at least three elements has a minimal triple

If G is a finite abelian group with $|G| \geq 3$, there exist

$$g_1, g_2, g_3 \in G$$

such that

$$g_1 g_2 g_3 = e,$$

but no proper nonempty subsequence has product e.

We assign the proof as homework. The same property holds for the inverse triple

$$g_1^{-1}, g_2^{-1}, g_3^{-1}.$$

Class number greater than 2 creates an irreducible triple

Assume $h_D > 2$. Choose a minimal triple g_1, g_2, g_3 in $\mathrm{Cl}(\mathcal{O}_D)$, and use Landau's lemma to choose prime ideals P_i with

$$[P_i] = g_i.$$

Then $P_1P_2P_3$ is principal, say

$$P_1P_2P_3 = (\pi),$$

and no proper subproduct is principal. By the anatomy lemma, π is irreducible.

The inverse triple creates a second irreducible

Choose prime ideals Q_i with

$$[Q_i] = g_i^{-1}.$$

Then

$$Q_1 Q_2 Q_3 = (\rho)$$

for an irreducible ρ.

For each i, the product $P_i Q_i$ is principal:

$$P_i Q_i = (\lambda_i).$$

Because neither one-term subproduct is principal, the anatomy lemma makes each λ_i irreducible.

Two irreducibles equal a product of three

Now

$$\begin{aligned}(\pi)(\rho) &= P_1P_2P_3Q_1Q_2Q_3 \\ &= (P_1Q_1)(P_2Q_2)(P_3Q_3) \\ &= (\lambda_1)(\lambda_2)(\lambda_3).\end{aligned}$$

After adjusting by a unit,

$$\boxed{\pi\rho = \lambda_1\lambda_2\lambda_3.}$$

Thus $\mathcal{O}_D$ is not half-factorial whenever $h_D > 2$.

Combined with the class-number 1 and 2 cases, half-factoriality occurs exactly when $h_D \leq 2$.

Elasticity measures how far lengths can stretch

For $0 \neq \alpha \in \mathcal{O}_D$, define the **elasticity of** α:

$$\rho(\alpha) = \frac{\text{maximum length of a factorization of } \alpha \text{ into irreducibles}}{\text{minimum length of a factorization of } \alpha \text{ into irreducibles}}.$$

The **elasticity of the ring** is

$$\rho_D = \sup_{0 \neq \alpha \in \mathcal{O}_D} \rho(\alpha).$$

Then

$$\rho_D = 1 \iff \mathcal{O}_D \text{ is half-factorial} \iff h_D = 1 \text{ or } 2.$$

The identity $\pi\rho = \lambda_1\lambda_2\lambda_3$ already shows $\rho_D \geq 3/2$ when $h_D > 2$.

Robert Valenza's two most-cited papers

The definition of elasticity is due to **Robert J. Valenza**.

Number theory: 108 citations

R. J. Valenza, "Elasticity of Factorization in Number Fields," *Journal of Number Theory* **36**, 212–218 (1990).

According to Google Scholar in July 2026, this is his most-cited paper. Compare with his second most-cited paper.

Shakespeare attribution: 106 citations

W. E. Y. Elliott and R. J. Valenza, "And Then There Were None: Winnowing the Shakespeare Claimants," *Computers and the Humanities* **30**(3), 191–245 (1996).

The Davenport constant gives the exact elasticity

For a finite abelian group G, let its **Davenport constant** $\mathsf{Dav}(G)$ be the least integer d such that every sequence of d elements of G has a nonempty subsequence with product the identity.

Valenza–Narkiewicz–Steffan theorem

If $h_D = 1$, then $\rho_D = 1$. If $h_D > 1$, then

$$\boxed{\rho_D = \frac{1}{2}\,\mathsf{Dav}(\mathsf{Cl}(\mathcal{O}_D)).}$$

Large class number forces large stretchiness

The homework asks us to show:

$$\mathrm{Dav}(G) \leq 2 \quad \iff \quad |G| \leq 2,$$

and

$$\mathrm{Dav}(G) \to \infty \quad \text{whenever} \quad |G| \to \infty.$$

Consequently,

$$h_D \to \infty \quad \implies \quad \rho_D \to \infty.$$

Large class number forces irreducible factorization lengths to become increasingly elastic.

Warning: The situation can change drastically if we pass to a subring of $\mathcal{O}_D$ rather than work with all of $\mathcal{O}_D$: the elasticity of $\mathbb{Z}[5i]$ is infinite! See the final problem on the final HW.

The disease now has a precise diagnosis

Day 1

$$(1+\sqrt{-26})(1-\sqrt{-26}) = 3^3$$

showed that element factorization can fail.

Day 15 The class group predicts whether powers separate, whether lengths agree, and how far those lengths can stretch.

Arithmetic beyond $\mathbb{Z}$

We enlarged numbers to ideals, recovered unique factorization there, and then used ideal classes to understand exactly what remains nonunique among elements.