Prime Factorization from Euclid to Noether

Keith Conrad
Number Theory Day

March 1, 2023

An unsuccessful attempt at Fermat's Last Theorem

On **March 1**, 1847, Lamé told the Paris Academy of Sciences that he had proved Fermat's Last Theorem: there is no solution in $\mathbf{Z}^+$ to $x^n + y^n = z^n$ when $n \geq 3$.

It suffices to treat $n = p$ an odd prime. Then $x^p + y^p$ factors:

$$z^p = x^p + y^p = (x+y)(x+\zeta y)\cdots(x+\zeta^{p-1}y),$$

for $\zeta \in \mathbf{C}$ where $\zeta^p = 1$ and $\zeta \neq 1$. For the numbers

$$\boxed{a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1}}$$

where $a_j \in \mathbf{Z}$, Lamé wanted to use an analogue of the "coprime power property" of $\mathbf{Z}^+$:

$$ab = c^n \text{ and } \gcd(a,b) = 1 \Longrightarrow a = x^n \text{ and } b = y^n.$$

The proof of that property in $\mathbf{Z}^+$ uses unique factorization, so Liouville asked Lamé why his setting has unique factorization.

In fact, there is *not* unique factorization there if $p = 23$.

Unique factorization in $\mathbf{Z}^+$

Theorem. *Integers have unique factorization*:

(*i*) *each* $n > 1$ *is a product of primes* $p_1 p_2 \cdots p_r$ (*repetitions ok*),

(*ii*) *if* $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ *for prime* p_j & q_k, *then* $r = s$ *and* $p_j = q_j$ *after relabeling*.

Usually we collect like primes together:

$$\boxed{n = p_1^{e_1} \cdots p_m^{e_m}} \ (p_j \text{ distinct primes}, e_j \geq 1).$$

1. Who first established this?
2. What good is it?
3. How broadly (beyond **Z**) have results like this been found?

Prime numbers in ancient Greece

Prime numbers appeared in Books VII and IX of Euclid's *Elements*, presented entirely geometrically.

Book VII.

Defn. A *prime* p is bigger than 1 and 1 is it only (proper) factor.

Prop. 30: $p \mid ab \Longrightarrow p \mid a$ *or* $p \mid b$.

Prop. 31, 32: *Every integer bigger than* 1 *has a prime factor*.

Book IX.

Prop. 12: $p \mid a^m \Longrightarrow p \mid a$.

Prop. 13: $d \mid p^m \Longrightarrow d = p^j$ *where* $j \leq m$.

Prop. 14: $p \mid \mathrm{lcm}(p_1, \ldots, p_r) \Longrightarrow p$ *is one of* $p_1, \ldots, p_r$.

Prop. 20: *There are infinitely many primes*.

Observations.

Prop. 31, 32 are the nearest to existence of prime factorization.

Prop. 13, 14 are the nearest to its uniqueness.

Unique factorization was *not* important for Euclid.

Prime factorization later

Existence of prime factorization was shown numerous times later:

1. al-Farisi's *Memorandum* [...] *on* [...] *amicability* (ca. 1300),
2. Prestet's *Nouveaux Elemens de Mathématiques* (1689),
3. Euler's *Elements of Algebra* (1770),
4. Legendre's *Théorie des Nombres* (1798)

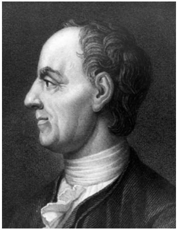
They all explicitly stated existence, while none proved uniqueness, but al-Farisi and Prestet came close.

A common reason they cared about prime factorization was to list, count, or sum all factors.

Example 1. Since $1881 = 3^2 \cdot 11 \cdot 19$, its factors are $3^a 11^b 19^c$ for $0 \leq a \leq 2$, $0 \leq b \leq 1$, and $0 \leq c \leq 1$: $3 \cdot 2 \cdot 2 = 12$ factors.

If $n = p_1^{e_1} \cdots p_m^{e_m}$ then n has $(e_1 + 1) \cdots (e_m + 1)$ factors. Without unique factorization, this count would be wrong.

An analytic use of prime factorization



Example 2. Euler needed uniqueness of prime factorization in his work on the zeta-function: for $s > 1$,

$$\begin{aligned}
\sum_{n\geq 1} \frac{1}{n^s} &= \prod_p \frac{1}{1 - 1/p^s} \\
&= \frac{1}{1-1/2^s}\frac{1}{1-1/3^s}\frac{1}{1-1/5^s}\frac{1}{1-1/7^s}\cdots \\
&= \left(1 + \frac{1}{2^s} + \frac{1}{4^s} + \cdots\right)\left(1 + \frac{1}{3^s} + \frac{1}{9^s} + \cdots\right)\cdots \\
&= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots
\end{aligned}$$

Prime factorization by Gauss

Gauss (1801) was the first to prove uniqueness, stating it as

Numerus compositus quicunque unico tantum modo in factores primos resolvi potest.

Composite numbers are resolved into prime factors in only one way.

The proof uses $p \mid ab \Longrightarrow p \mid a$ or $p \mid b$, which goes back to Euclid. Gauss criticized other authors for ignoring this property as well as ignoring the need to prove uniqueness of prime factorization.

A new concept of integers

Gauss (1832) introduced "complex integers"

$$\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\},$$

and basic number theory with them: primes, modular arithmetic, Euclid's algorithm, *etc.* We'll focus on factoring in $\mathbf{Z}[i]$.

$$7 + 4i = (1 + 2i)(3 - 2i)$$

Here are two different factorizations of 10:

$$10 = 2 \cdot 5 = (3 + i)(3 - i).$$

That doesn't violate unique factorization since

$$2 = (1 + i)(1 - i), \;\; 5 = (2 + i)(2 - i),$$
$$3 + i = (1 + i)(2 - i), \;\; 3 - i = (1 - i)(2 + i),$$

so the factorizations of 10 did not use primes in $\mathbf{Z}[i]$. Compare:

$$210 = 6 \cdot 35 = 10 \cdot 21.$$

Primality depends on *context*: in $\mathbf{Z}[i]$, 2 and 5 **not** prime, 3 is, ...

In $\mathbf{Z}[i]$, ± 1 & $\pm i$ are universal factors: $\alpha = (\pm 1)(\pm\alpha) = (\pm i)(\mp i\alpha)$.

Definition. Call nonzero p in $\mathbf{Z}[i]$ prime if
(a) $p \neq \pm 1$ or $\pm i$,
(b) its only factors are $\pm 1, \pm i, \pm p, \pm ip$.

The primes in $\mathbf{Z}[i]$ are a mix of familiar and unfamiliar numbers:

$$\pm 3,\ \pm 3i,\ \pm 7,\ \pm 7i,\ \pm 11,\ \pm 11i,\ \pm 19,\ \pm 19i, \ldots,$$

$$\pm(1 \pm i),\ \pm(2 \pm i),\ \pm(1 \pm 2i),\ \pm(2 \pm 3i),\ \pm(3 \pm 2i), \ldots.$$

Theorem. (Gauss) *For each $\alpha \neq 0, \pm 1, \pm i$ in $\mathbf{Z}[i]$,*

(*i*) *α is a product of primes: $\alpha = p_1 p_2 \cdots p_r$ (repetitions ok),*

(*ii*) *if $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ for prime p_j & q_k, then $r = s$ and $\boxed{p_j = u_j q_j}$ after relabeling, where $u_j = \pm 1, \pm i$.*

Example. $7 + 4i = (1 + 2i)(3 - 2i) = (2 - i)(2 + 3i)$, where $2 - i = (-i)(1 + 2i)$ and $2 + 3i = (i)(3 - 2i)$.

The coprime power property

In $\mathbf{Z}$, $ab = c^n$ and $\gcd(a, b) = 1 \Longrightarrow a = \pm x^n$ and $b = \pm y^n$.
Its proof uses unique factorization in $\mathbf{Z}$, so carries over to $\mathbf{Z}[i]$:

$$\alpha\beta = \gamma^n \text{ and } \gcd(\alpha, \beta) = 1 \Longrightarrow \alpha = ux^n \text{ and } \beta = vy^n,$$

where $uv = 1$ (u, v are among $\pm 1, \pm i$).

Example. (Pythagorean triples) In $\mathbf{Z}^+$, suppose $a^2 + b^2 = c^2$ with $\gcd(a, b) = 1$. Factor the left side in $\mathbf{Z}[i]$:

$$(a + bi)(a - bi) = c^2.$$

Can show $\gcd(a + bi, a - bi) = 1$, so coprime power property with $n = 2$ says $a + bi = \pm(k + \ell i)^2$ or $\pm i(k + \ell i)^2$. Focus on 1st:

$$(k + \ell i)^2 = k^2 - \ell^2 + (2k\ell)i \Longrightarrow a = k^2 - \ell^2, b = 2k\ell$$

and $c^2 = a^2 + b^2 = (k^2 + \ell^2)^2$, so $c = k^2 + \ell^2$. A parametric formula for all triples: $\boxed{(a, b, c) = (k^2 - \ell^2, 2k\ell, k^2 + \ell^2)}$

The coprime power property

$$\alpha\beta = \gamma^n \text{ and } \gcd(\alpha,\beta) = 1 \Longrightarrow \alpha = ux^n \text{ and } \beta = vy^n,$$

where $uv = 1$ (u, v are among $\pm 1, \pm i$).

Example. Show the only **Z**-solutions to $y^2 = x^3 - 4$ are $(2, \pm 2)$ and $(5, \pm 11)$. Rewrite the equation in $\mathbf{Z}[i]$ as

$$x^3 = y^2 + 4 = (y + 2i)(y - 2i).$$

If y odd, then $\gcd(y+2i, y-2i) = 1$, so coprime power property says $\boxed{y + 2i = (k + \ell i)^3}$. Can show same result if y even too.

$$\begin{aligned} y + 2i &= (k + \ell i)^3 \\ &= (k^3 - 3k\ell^2) + (3k^2\ell - \ell^3)i \\ &= k(k^2 - 3\ell^2) + \ell(3k^2 - \ell^2)i. \end{aligned}$$

Thus $y = k(k^2 - 3\ell^2)$ and $2 = \ell(3k^2 - \ell^2)$, forcing $\ell = \pm 1$ or ± 2. This leads to $y = \pm 11, x = 5$ and $y = \pm 2, x = 2$.

Failure of the coprime power property

Example. In $\mathbf{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbf{Z}\}$,

$$(1 + \sqrt{-3})(1 - \sqrt{-3}) = 4 = 2^2.$$

The only common factors of $1 \pm \sqrt{-3}$ are ± 1, but $1 \pm \sqrt{-3} \neq \pm\Box$ since coefficient of $\sqrt{-3}$ isn't even:

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

Since unique factorization implies the coprime power property, if coprime power property breaks in $\mathbf{Z}[\sqrt{-3}]$ then so must unique factorization, and in fact

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

gives us two *unrelated* prime factorizations of 4 in $\mathbf{Z}[\sqrt{-3}]$.

Remark. For primes in $\mathbf{Z}$ or $\mathbf{Z}[i]$, $p \mid ab \Longrightarrow p \mid a$ or $p \mid b$. But in $\mathbf{Z}[\sqrt{-3}]$, 2 is prime, $2 \mid (1 + \sqrt{-3})(1 - \sqrt{-3})$, and $2 \nmid (1 \pm \sqrt{-3})$.

Another failure of the coprime power property

Polynomials in x have unique factorization up to order and scaling by nonzero constants:

$$1-x^2 = (1-x)(1+x) = (2-2x)\frac{1+x}{2} = \left(\frac{2}{3}-\frac{2}{3}x\right)\left(\frac{3}{2}+\frac{3}{2}x\right).$$

But now consider the set **T** of all (trigonometric) polynomials in $\sin\theta$ and $\cos\theta$. These are the finite Fourier series:

$$\sin^3\theta + \cos^3\theta = \frac{3}{4}\cos\theta + \frac{1}{2}\sin\theta - \frac{1}{2}\sin\theta\cos(2\theta) + \frac{1}{4}\cos(3\theta).$$

Example. In **T**, rewrite $\sin^2\theta + \cos^2\theta = 1$ as

$$(1+\sin\theta)(1-\sin\theta) = (\cos\theta)^2,$$

where the only common factors of $1 \pm \sin\theta$ are nonzero constants, but $1 \pm \sin\theta \neq \pm\square$ in **T**. So **T** does not have unique factorization!

The rational roots property

Unique factorization in $\mathbf{Z}$ implies the rational roots theorem: if $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ with $c_j \in \mathbf{Z}$, then

$$f(r) = 0 \text{ for } r \in \mathbf{Q} \Longrightarrow r \in \mathbf{Z}.$$

This holds in $\mathbf{Z}[i]$ too: if $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ with $c_j \in \mathbf{Z}[i]$, then $f(r) = 0$ for $r \in \mathbf{Q}[i] \Longrightarrow r \in \mathbf{Z}[i]$.

Nonexample. A root of $x^2 - x + 1$ is $\frac{1}{2} + \frac{1}{2}\sqrt{-3}$: it is in $\mathbf{Q}[\sqrt{-3}]$ and not in $\mathbf{Z}[\sqrt{-3}]$. This is a second reason $\mathbf{Z}[\sqrt{-3}]$ doesn't have unique factorization besides failure of the coprime power property.

Enlarge $\mathbf{Z}[\sqrt{-3}]$ to include the number $\omega = \frac{1}{2} + \frac{1}{2}\sqrt{-3}$:

$$\mathbf{Z}[\omega] = \{a + b\omega : a, b \in \mathbf{Z}\}$$

contains $\mathbf{Z}[\sqrt{-3}]$ and *does* have the "rational roots property": for $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ with $c_j \in \mathbf{Z}[\omega]$,

$$f(r) = 0 \text{ for } r \in \mathbf{Q}[\omega] \Longrightarrow r \in \mathbf{Z}[\omega].$$

In $\mathbf{Z}[\omega]$, unlike $\mathbf{Z}[\sqrt{-3}]$, there is unique factorization.

Rational root property without unique factorization

In $\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbf{Z}\}$, the rational roots property holds: if $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ with $c_j \in \mathbf{Z}[\sqrt{-5}]$,

$$f(r) = 0 \text{ for } r \in \mathbf{Q}[\sqrt{-5}] \Longrightarrow r \in \mathbf{Z}[\sqrt{-5}].$$

But $\mathbf{Z}[\sqrt{-5}]$ does *not* have unique factorization:

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

and

$$\boxed{9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})}.$$

For nonsquare d in $\mathbf{Z}$, set

$$\mathbf{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbf{Z}\}.$$

In $\mathbf{Z}[\sqrt{d}]$ prime factorization exists, but often it is not unique, even when the rational roots property holds in $\mathbf{Z}[\sqrt{d}]$:

$$\mathbf{Z}[\sqrt{-5}],\ \mathbf{Z}[\sqrt{-6}],\ \mathbf{Z}[\sqrt{10}],\ \mathbf{Z}[\sqrt{26}],\ \mathbf{Z}[\sqrt{79}],\ \ldots.$$

Rescue unique factorization by changing what is factored

Dedekind, building on work of Kummer, replaced the factorization of elements with factorization of certain *sets* of elements.

Two properties of the multiples of a number γ in $\mathbf{Z}[\sqrt{d}]$:

- closed under addition/subtraction: $\alpha\gamma \pm \beta\gamma = (\alpha \pm \beta)\gamma$
- absorb multiplication by everything: $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.

Definition. A subset I of $\mathbf{Z}[\sqrt{d}]$ with those properties is an *ideal*:

$$x, y \in I \Longrightarrow x \pm y \in I, \quad x \in I \Longrightarrow \alpha x \in I.$$

Example. For each $\gamma \in \mathbf{Z}[\sqrt{d}]$, its multiples $\mathbf{Z}[\sqrt{d}]\gamma$ are an ideal: principal ideals.

Example. In $\mathbf{Z}[\sqrt{-5}]$, there are ideals *not* of the form $\mathbf{Z}[\sqrt{-5}]\gamma$ (nonprincipal ideals) using all linear combinations of two elements:

$$I = \mathbf{Z}[\sqrt{-5}]2 + \mathbf{Z}[\sqrt{-5}](1 + \sqrt{-5}),$$
$$J = \mathbf{Z}[\sqrt{-5}]3 + \mathbf{Z}[\sqrt{-5}](1 + \sqrt{-5}),$$
$$J' = \mathbf{Z}[\sqrt{-5}]3 + \mathbf{Z}[\sqrt{-5}](1 - \sqrt{-5}).$$

Multiplying ideals

Multiplication. For ideals I_1 and I_2, their product is the ideal

$$I_1 I_2 = \{x_1 y_1 + \cdots + x_m y_m : x_k \in I_1, y_k \in I_2\}.$$

Example. $\mathbf{Z}[\sqrt{d}]\gamma \mathbf{Z}[\sqrt{d}]\gamma' = \mathbf{Z}[\sqrt{d}]\gamma\gamma'$.

Example. In $\mathbf{Z}[\sqrt{-5}]$ with

$$\begin{aligned} I &= \mathbf{Z}[\sqrt{-5}]2 + \mathbf{Z}[\sqrt{-5}](1+\sqrt{-5}), \\ J &= \mathbf{Z}[\sqrt{-5}]3 + \mathbf{Z}[\sqrt{-5}](1+\sqrt{-5}), \\ J' &= \mathbf{Z}[\sqrt{-5}]3 + \mathbf{Z}[\sqrt{-5}](1-\sqrt{-5}), \end{aligned}$$

we have

$$I^2 = \mathbf{Z}[\sqrt{-5}]2, \quad JJ' = \mathbf{Z}[\sqrt{-5}]3,$$

$$IJ = \mathbf{Z}[\sqrt{-5}](1+\sqrt{-5}), \quad IJ' = \mathbf{Z}[\sqrt{-5}](1-\sqrt{-5}).$$

The unique factorization *failure* $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ in $\mathbf{Z}[\sqrt{-5}]$ can be viewed as rearrangements of ideals: $I^2JJ' = IJIJ'$. It's like $6 \cdot 35 = 10 \cdot 21$ in $\mathbf{Z}$ being rearrangements of $2 \cdot 3 \cdot 5 \cdot 7$.

Factoring ideals

In $\mathbf{Z}$, $a \mid b \iff a\mathbf{Z} \supset b\mathbf{Z}$, *e.g.*, $2\mathbf{Z} \supset 6\mathbf{Z}$.

Dedekind called an ideal P in $\mathbf{Z}[\sqrt{d}]$ *prime* if
(i) $P \neq \{0\}$ or $\mathbf{Z}[\sqrt{d}]$,
(ii) $P \supset I_1 I_2 \Longrightarrow P \supset I_1$ or $P \supset I_2$.

Ideals I, J, and J' in $\mathbf{Z}[\sqrt{-5}]$ on previous slide are all prime and

$$\mathbf{Z}[\sqrt{-5}]2 = I^2, \quad \mathbf{Z}[\sqrt{-5}]3 = JJ', \quad \mathbf{Z}[\sqrt{-5}](1+\sqrt{-5}) = IJ$$

are prime ideal factorizations.

Theorem. (Dedekind) *Assume $\mathbf{Z}[\sqrt{d}]$ has rational roots property.*

- *The ideals in $\mathbf{Z}[\sqrt{d}]$ have unique factorization into products of prime ideals.*
- *There is unique factorization of elements in $\mathbf{Z}[\sqrt{d}]$ if and only if there are no unexpected ideals: each ideal I is the multiples of something: $I = \mathbf{Z}[\sqrt{d}]\gamma$.*

What Dedekind proved is applicable beyond $\mathbf{Z}[\sqrt{d}]$.

Extending what is possible

Ideals are yet another case where mathematics lets us do what at first seems impossible.

- Solve equations without classical solutions: complex numbers.
- Intersect lines with no classical intersection: projective plane.
- Uniquely factor what doesn't have unique factorization: ideals.
- Differentiate what has no classical derivative: distributions.

Dedekind's ideals were one of three ways that the failure of unique factorization for elements was fixed in the late 19th century: also Kronecker's divisors and Zolotarev's semi-local rings.

Noether's paper on abstract structure of ideal theory

Noether worked on ideals in the 1920s. Always looked for algebraic concepts behind pages of computations and formulas.

- 1921: Primary ideal decomposition (Lasker–Noether theorem)
- 1927: Says when unique factorization of ideals occurs.

Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern.

Von

Emmy Noether in Göttingen.

Im folgenden wird eine abstrakte Charakterisierung all derjenigen Ringe gegeben, deren Idealtheorie übereinstimmt mit der Idealtheorie aller ganzen Größen des algebraischen Zahlkörpers — deren Ideale sich

Here is a version of Noether's result.

Theorem. *An integral domain has unique factorization of ideals if and only if*
(1) *it has an analogue of the rational roots property*,
(2) *every increasing sequence of ideals in it stabilizes*,
(3) *its prime ideals have no containment relations*.

Example. The set $\mathbf{T}$ of trigonometric polynomials fits all of these conditions, so $\mathbf{T}$ has unique factorization of ideals.

How does $(1+\sin\theta)(1-\sin\theta) = (\cos\theta)^2$, as a counterexample to unique factorization of *elements* in $\mathbf{T}$, get saved using *ideals* in $\mathbf{T}$?

The ideals $P = \mathbf{T}(1+\sin\theta) + \mathbf{T}\cos\theta$ and $Q = \mathbf{T}(1-\sin\theta) + \mathbf{T}\cos\theta$ turn out to be prime ideals and

$$P^2 = \mathbf{T}(1+\sin\theta), \quad Q^2 = \mathbf{T}(1-\sin\theta), \quad PQ = \mathbf{T}\cos\theta,$$

so $(1+\sin\theta)(1-\sin\theta) = (\cos\theta)^2$ turns into $P^2Q^2 = (PQ)^2$.

Using ideals

1. When $\mathbf{Z}[\sqrt{d}]$ has unique factorization of ideals, its elements have a coprime power property for *restricted* exponents.

Example. For nonzero α and β in $\mathbf{Z}[\sqrt{-5}]$ such that $\mathbf{Z}[\sqrt{-5}]\alpha$ and $\mathbf{Z}[\sqrt{-5}]\beta$ are relatively prime ideals,

$$\alpha\beta = \gamma^n \Longrightarrow \alpha = \pm x^n \text{ and } \beta = \pm y^n$$

when n is *odd*. (It fails for $(2+\sqrt{-5})(2-\sqrt{-5}) = 3^2$.)

2. For each A in $\mathrm{M}_n(\mathbf{Q})$, A and $A^\top$ are conjugate: $A^\top = UAU^{-1}$ for an invertible U in $\mathrm{M}_n(\mathbf{Q})$. This *need not* be true in $\mathrm{M}_n(\mathbf{Z})$!

Example. The matrix

$$A = \begin{pmatrix} 1 & -5 \\ 3 & -1 \end{pmatrix}$$

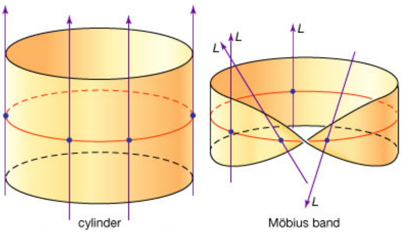
is conjugate to $A^\top$ in $\mathrm{M}_2(\mathbf{Q})$ but not in $\mathrm{M}_2(\mathbf{Z})$. Its characteristic polynomial is $x^2 + 14$ and A is found using ideals in $\mathbf{Z}[\sqrt{-14}]$.

3. For prime p and pth root of unity $\zeta \neq 1$ in $\mathbf{C}$, the numbers

$$a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1}$$

where $a_j \in \mathbf{Z}$ have unique factorization of ideals for all p but not unique factorization of elements for $p \geq 23$ (Uchida, Montgomery).

4. In geometric settings, ideals are related to line bundles. The elements of $\mathbf{T}$ are polynomial functions on the unit circle, and $\mathbf{T}$ having ideals that are not just multiples of something is related to the circle having a nontrivial line bundle: the Möbius strip.



Questions?