Introduction to Algebraic Number Theory
Part II

A. S. Mosunov

University of Waterloo
Math Circles

November 14th, 2018

DETOUR

Detour: Mihăilescu's Theorem

- In 1844 it was conjectured by Catalan that the only perfect powers that differ by one are 8 and 9.
- Last time I mentioned Tijdeman's Theorem: there are only finitely many perfect powers that differ by one.
- I was unaware that the conjecture of Catalan **was solved** by the Romanian mathematician Preda Mihăilescu in 2002 in his article "Primary Cyclotomic Units and a Proof of Catalan's Conjecture".
- See a popular video about Catalan's Conjecture: `https://www.youtube.com/watch?v=Us-__MukH9I` (**subscribe to Numberphile!**)
- The question about prime powers that differ by 2 is still open!

Detour: Mihăilescu's Theorem

Figure: Eugéne Charles Catalan (left) and Preda Mihailescu (right)

RECALL

- We were learning about **algebraic number theory.**
- It studies properties of numbers that are roots of polynomial equations, like i, $\frac{-1+\sqrt{-3}}{2}$, $\sqrt[3]{2}$, and so on.
- We learned about Gaussian integers, i.e. numbers of the form $a+bi$, where a, b are integers and i satisfies $i^2+1=0$.
- The set of Gaussian integers is denoted by $\mathbb{Z}[i]$. You can add, subtract and multiply Gaussian integers, and the result will be a Gaussian integer. Therefore $\mathbb{Z}[i]$ is a **ring**.
- We saw that every Gaussian integer $a+bi$ has a **norm** $N(a+bi)=a^2+b^2$ and that the norm is multiplicative:

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

Generalizing Primes

- We generalized the notion of divisibility.
- We learned about **units**: elements of $\mathbb{Z}[i]$ that divide everything. There are four of them: $1, -1, i$ and $-i$. In comparison, the ring of integers $\mathbb{Z}$ has only two units.
- We generalized the notion of primes: a Gaussian integer α is called a **Gaussian prime** if it is not a unit and any factorization $\alpha = \beta\gamma$ in $\mathbb{Z}[i]$ forces β or γ to be a unit.
- We saw that some rational primes p can **split** in $\mathbb{Z}[i]$:

$$\begin{aligned} 2 &= i(1-i)^2 \\ 5 &= (2+i)(2-i) \\ 13 &= (2+3i)(2-3i). \end{aligned}$$

  We say that 2 **ramifies** in $\mathbb{Z}[i]$ because it is divisible by a square of a Gaussian prime. Other primes are **unramified**.
- Some primes, like $3, 7, 11, 19$, are both rational primes and Gaussian primes. Such primes are called **innert**.

Other Theorems in $\mathbb{Z}[i]$

- **The Remainder Theorem for Gaussian Integers.** Let a, b be Gaussian integers. Then there exist Gaussian integers q and r such that $b = aq + r$, where $N(r) < N(a)$.
- Let a and b be Gaussian integers. A Gaussian integer g such that $g \mid a$ and $g \mid b$, with $N(g)$ the largest, is called the **greatest common divisor of** a **and** b. It is denoted by $\gcd(a, b)$.
- **The Fundamental Theorem of Arithmetic.** Up to multiplication by a unit, any non-zero Gaussian integer can be written uniquely (up to reordering) as the product of Gaussian primes.
- **Fermat's Theorem on Sums of Two Squares.** every rational prime p of the form $4k + 1$ is a sum of two squares.

EXERCISE

The Ring of Eisenstein Integers

- **Exercise 1.** Let
$$\omega = \frac{-1+\sqrt{-3}}{2}.$$
Verify that $\omega^2+\omega+1=0$.
- **Exercise 2.** The set
$$\mathbb{Z}[\omega] = \{a+b\omega\colon\ a,b\in\mathbb{Z}\}$$
is called the **ring of Eisenstein integers**. Prove that it is a ring. That is, show that for any Eisenstein integers $a+b\omega$, $c+d\omega$ the numbers $(a+b\omega)+(c+d\omega)$, $(a+b\omega)-(c+d\omega)$, $(a+b\omega)(c+d\omega)$ are Eisenstein integers as well.
- **Exercise 3.** For any Eisenstein integer $a+b\omega$ define the **norm**
$$N(a+b\omega) = a^2-ab+b^2.$$
Prove that the norm is multiplicative: $N(\alpha\beta)=N(\alpha)N(\beta)$. Verify that it is non-negative; that is, $N(\alpha)\geq 0$ and $N(\alpha)=0$ if and only if $\alpha=0$.

The Ring of Eisenstein Integers

- **Exercise 4.** We say that γ is an **Eisenstein unit** if $\gamma \mid 1$. Prove that if γ is an Eisenstein unit then its norm is equal to one.
- **Exercise 5.** Find all Eisenstein integers of norm one (there are six of them) and show that all of them are Eisenstein units.
- **Exercise 6.** An Eisenstein integer γ is **prime** if it is not a unit and every factorization $\gamma = \alpha\beta$ with $\alpha, \beta \in \mathbb{Z}[\omega]$ forces one of α or β to be a unit. Find Eisenstein primes among rational primes
$$2, 3, 5, 7, 11, 13.$$
- **Homework.** Think for which positive integers n the Diophantine equation
$$n = x^2 - xy + y^2$$
has a solution (start by showing that if m and n are of the above form then so is mn).

How Things Fail

- Remember Euler's "almost" correct idea to solve the Diophantine equation $y^2 = x^3 - 2$: factor

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

  and show that $y + \sqrt{-2}$ and $y + \sqrt{-2}$ are coprime in $\mathbb{Z}[\sqrt{-2}]$ for $y \neq 0$. Then

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3 \text{ and } y - \sqrt{-2} = (c + d\sqrt{-2})^3$$

  for some $a, b, c, d \in \mathbb{Z}$.
- His idea would not work for the equation $y^2 = x^3 - 5$, because the Fundamental Theorem of Arithmetic **does not** hold in $\mathbb{Z}[\sqrt{-5}]$.

Failure of Unique Factorization

- **Exercise 1.** Consider the ring

$$\mathbb{Z}[\sqrt{-5}] = \left\{ a + b\sqrt{-5} \colon a, b \in \mathbb{Z} \right\}$$

  along with the norm map $N(a + b\sqrt{-5}) = a^2 + 5b^2$, which is known to be multiplicative. Prove that ± 1 are the only units in $\mathbb{Z}[\sqrt{-5}]$.
- **Exercise 2.** Prove that the numbers $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are prime in $\mathbb{Z}[\sqrt{-5}]$.
- **Exercise 3.** Using Exercise 2 prove that the unique factorization fails in $\mathbb{Z}[\sqrt{-5}]$.
- The rings where unique factorization holds are called **Unique Factorization Domains** (UFD's).
- In 1966, Alan Baker classified all rings of the form $\mathbb{Z}[\sqrt{-d}]$ and $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ that are UFD's. There are only 13 of them, for example $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right]$.

Euclidean Domains

- The rings which possess some procedure resembling the Euclidean algorithm for finding the greatest common divisors are called **Euclidean domains**.
- We saw that both $\mathbb{Z}$ and $\mathbb{Z}[i]$ are Euclidean domains. So is $\mathbb{Z}[\omega]$.
- Every Euclidean domain is a UFD, but the converse is not true. An example of a UFD that is not a Euclidean domain is

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right].$$

Rings With Infinitely Many Units

- As it turns out, the rings of the form $\mathbb{Z}[\sqrt{d}], \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ behave very differently when d is positive or negative.
- For example, the rings

$$\mathbb{Z}\left[\sqrt{d}\right] = \{a + b\sqrt{d} \colon a, b \in \mathbb{Z}\}$$

  contain infinitely many units.
- **Exercise 1.** Find at least one unit different from ± 1 in the rings $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{5}]$. **Hint:** the norm map is $N(a + b\sqrt{d}) = a^2 - db^2$ and it is multiplicative. Convince yourself that $N(a + b\sqrt{d}) = \pm 1$ and then find one solution to the Diophantine equation you obtained.
- **Exercise 2.** Suppose that you have found a unit $a + b\sqrt{d}$ for $d = 2$ or 5. Prove that for any positive integer n the number $(a + b\sqrt{d})^n$ is also a unit. Prove that there are infinitely many units.

Rings With Infinitely Many Units

- (Special case of) **Dirichlet's Unit Theorem.** As it turns out, in $\mathbb{Z}[\sqrt{d}]$ and $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ there always exists **exactly one** unit $x_0 + y_0\sqrt{d} > 1$ such that any other unit has the form $(x_0 + y_0\sqrt{d})^n$, where n is a (possibly negative) integer. It is called the **fundamental unit**.
- Here are some examples of fundamental units:

$\mathbb{Z}[\sqrt{2}]$	$1+\sqrt{2}$
$\mathbb{Z}[\sqrt{3}]$	$2+\sqrt{3}$
$\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$	$\frac{1+\sqrt{5}}{2}$
$\mathbb{Z}[\sqrt{31}]$	$1520+273\sqrt{31}$
$\mathbb{Z}[\sqrt{94}]$	$2143295+221064\sqrt{94}$

- The fundamental unit $x_0 + y_0\sqrt{1621}$ of $\mathbb{Z}[\sqrt{1621}]$ is ridiculously big (x_0 has 76 decimal digits).

Pell's Equation

- An equation of the form $x^2 - dy^2 = \pm 1$ where $d > 0$ is not a perfect square is called a **Pell's equation**.
- Around 1766 – 1769 Joseph-Louis Lagrange proved that this equation always has a solution $(x, y) \neq (\pm 1, 0)$ for any integer d that is not a perfect square.
- **Archimedes' cattle problem.** In 1773, a German philosopher Gotthold Lessing discovered a Greek manuscript containing a poem with the mathematical problem, that gets reduced to the Pell's equation

$$x^2 - 609 \cdot 7766 \cdot v^2 = 1.$$

- This problem is attributed to Archimedes and it asks to compute the number of cattle in a herd of the sun given relations between different kinds of bulls and cows in a herd.
- The exact solution was first computed in 1965 at the University of Waterloo by Hugh Williams, Gus German and Robert Zarnke.

Pell's Equation

Figure: Hugh Williams, Gus German and Robert Zarnke

Next Time

- We will see that it is possible to fix the failure of Unique Factorization.
- We will learn how algebraic number theory allowed Ernst Kummer to make a big breakthrough towards the resolution of Fermat's Last Theorem.
- We will learn about algebraic numbers and see that not all numbers can be written in such nice forms as $\sqrt{2}$ or $\frac{1+\sqrt{-3}}{2}$.

THANK YOU FOR COMING!