“Es steht schon bei Dedekind”[1]

Lecture at the DM/Algebra Seminar on 11/4/2005.

Felix Lazebnik.

The content of this lecture is influenced very much by writings and translations by **John Stillwell**, and several books at the end of these notes which I highly recommend.

The most important thing I wish to share is the realization of the similarity between several contributions by R. Dedekind to modern mathematics: residue classes, the theory of real numbers and the theory of ideals.

These notes are very rough and informal; I did not make any serious attempt to polish them. Some comments I made during the lecture may be missing: I forgot what exactly I said, and I do not believe that some of them were really important. On the other hand, several remarks that I planned to make at the lecture, and did not because of the shortage of time, are included in these notes.

I do assume that most listeners had at least one course of abstract algebra or number theory, but it will be easier for those who had two.

======================

1. When we think how we came to like mathematics, or how our tastes were formed, or which were the most memorable moments, we can make a relatively short list of these events. Thinking about this lecture I compounded about twenty five, with about five being major. To me, one of the most cherished events are those when mathematical facts which were disjoint in my mind, suddenly come together, and I thought that I could hear “the harmony of heavens.” One such moment happened last summer, and I wish to share it with you today.

2. This June I was working on a problem with Robert Coulter and Marie Henderson. I was looking through my books and library books trying to generalize something. Fortunately, or unfortunately, I have many books. Those of you who read something on algebraic number theory, may agree that many books talk about the same things in completely different ways; different terminology; opposite order; etc... Being lazy to think, I put a book away, and began reading “seemingly” the same in another book. Spending a week this way, I brought myself to the point, where I had everything mixed, and even things, which I thought I understood well before, began to make much less sense.

Until I opened the book by Dirichlet (1805 – 1859) ”Lectures on Number Theory”. It was like taking a swim in the calm warm ocean. The first hour I read stuff which is more elementary that what I teach in Math 210. Then I began to read Translator’s Introduction by John Stillwell. I found it to be excellent. I read his writings before, but this one made an unusual effect on me. Then I read nine Supplements at the end of this book written by Dedekind. The German edition to the book is often referred to as Dirichlet-Dedekind. 180 pages by Dirichlet follow by 150 pages by Dedekind. Stillwell mentions that there were two more supplements in German edition, but he did not include them because they were going to be published soon as a separate book which he was preparing. I decided to buy it, and in a few days (thanks to Amazon) the book arrived: “Theory of Algebraic Integers” by R. Dedekind. It had an Introduction by Stillwell, even better than the one for Dirichlet’s book, but then it had Dedekind’s Theory of Ideals. When I began reading, I understood that “one of those moments” was coming.

[1] This is a famous phrase by Emmy Noether, which can be translated as “It’s already in Dedekind.”

1 Some history of studies of non-uniqueness of prime factorization

1.1 Fermat (1601–1665).

He is credited with the rebirth of the interest to Number Theory, and with pushing it further. He tried to challenge his contemporaries with these problems, but many of them did not think that the problems are worth of their time. Huygens' comment: *"There is no lack of better things for us to do"*.

Fermat's many conjecture appeared from thinking about extending the ancient results of Pythagorians and Diophantus on $x^2 + y^2 = z^2$.

Which integers n can be written as $x^2 + y^2$?

The identity

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

was known even to Diophantus (150-350?). Hence it was sufficient to answer the question for $n = p$, p is prime. Actually Fermat knew about more general identities

$$(x^2 + Dy^2)(z^2 + Dt^2) = u^2 + Dv^2,$$

where $u = xz - Dyt$ and $v = xt + yz$. That is what Fermat got by using them.

$p = x^2 + y^2 \Leftrightarrow p \equiv 1 \mod 4$

$p = x^2 + 2y^2 \Leftrightarrow p \equiv 1, 3 \mod 8$

$p = x^2 + 3y^2 \Leftrightarrow p \equiv 1 \mod 3$

$p = x^2 + 4y^2 \Leftrightarrow p \equiv 1 \mod 4$

In all these cases the representation is essentially **unique**: up to the change of signs of x and y (and their order in the first one).

$p = x^2 + 5y^2 \Leftrightarrow$???

Something here was not clear. Both with describing of exactly those p's that work, and also the uniqueness of the factorization.

1.2 Euler (1707–1783).

$p = x^2 + 5y^2 \Leftrightarrow p \equiv 1, 9 \mod 20$; $2p = x^2 + 5y^2 \Leftrightarrow p \equiv 3, 7 \mod 20$ (Euler's conjectures, 1744)

Cooking his great theorems, Euler loved mixing different mathematics. Analysis, combinatorics, number theory, trigonometry,... . Complex numbers were one of his favorite ingredients.

That is how he approached the Pythagorean triples. Given $x^2+y^2 = z^2$, he rewrote it as $(x+iy)(x-iy) = z^2$. Assuming $\gcd(x + iy, x - iy) = 1$, by analogy with usual integers, $x + iy = (a + ib)^2$, which gives $x = a^2 - b^2$ and $y = 2ab$, so $z = a^2 + b^2$

Here is how he found all integer solutions of $y^3 = x^2 + 2$.

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

He could argue that $\gcd(x - \sqrt{-2}, x + \sqrt{-2}) = 1$. So they are cubes themselves. Set $x - \sqrt{-2} = (a + b\sqrt{-2})^3$, get $x = a^3 - 6ab^2$, $1 = 3a^2b - 2b^3$. So b divides —1. And he gets $x = \pm 5, y = 3$ as the only solutions.

And when Euler wanted to solve $x^3 + y^3 = z^3$, he wrote

$$x^3 + (\zeta y)^3 = (x + y)(x + \zeta y)(x + (\zeta^2 y) = z^3,$$

where $\zeta^3 = 1$, $\zeta \neq 1$. Again, he argues that the factors are relatively prime. So each is cube, ... , a contradiction!

Of course, when he claims that if a product of two relatively prime numbers is a cube, then each number is a cube, he uses the analogy with usual integers, namely the uniqueness of their prime factorization. In the second example, he mistakenly assumes that there exists unique prime factorization in $\mathbb{Z}[\sqrt{-3}]$ which is false: $4 = 2 \times 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$, but the argument can be saved. It is true in $\mathbb{Z}[\zeta]$. (Gauss did not like to think about ζ as an integer, but Eisenstein and Dedekind (his last student) thought otherwise.)

1.3 Lagrange (1736–1813).

In 1773 Lagrange considered a generalization of Fermat's question: which integers can be represented by quadratic forms? In other words, he considered the equation

$$n = ax^2 + 2bxy + cy^2,$$

with integers n, a, b, c given, and integers x, y unknown.

Equivalence of forms: $ax^2 + 2bxy + cy^2$ and $a'x'^2 + 2b'x'y' + c'y'^2$.

Unimodular transformations.

$D = b^2 - ac$ is preserved. Equivalence implies $D = D'$. Vice versa: not always.

$h(D)$ is the number of non-equivalent forms with given discriminant, or just the **number of classes**. With these notions, Fermat's results can be stated as:

$$\begin{array}{rcllll}
h(-1) & = & 1 & --- & x^2 + y^2 & \\
h(-2) & = & 1 & --- & x^2 + 2y^2 & \\
h(-3) & = & 1 & --- & x^2 + 3y^2 & \\
h(-4) = h(-1) & = & 1 & --- & x^2 + 4y^2 & \\
h(-5) & = & 2 & --- & x^2 + 5y^2 & \text{and} \quad 2x^2 + 2xy + 3y^2 \text{ !!!}
\end{array}$$

The form $2x^2 + 2xy + 3y^2$ did represent the classes of primes $p \equiv 3, 7 \mod 20$!!! But

$$(2x^2 + 2xy + 3y^2)(2x'^2 + 2x'y' + 3y'^2) = X^2 + 5Y^2,$$

where $X = 2xx' + yx' + yx' - 2yy'$, and $Y = xy' + yx' + yy'$.

And

$$(x^2 + 5y^2)(2x'^2 + 2x'y' + 3y'^2) = X^2 + 2XY + 3Y^2,$$

where $X = xx' - yx' - 3yy'$ and $Y = xy' + 2yx' + yy'$.

And

$$(x^2 + 5y^2)(x'^2 + 5y'^2) = X^2 + 5Y^2,$$

where $X = xx' - 5yy'$ and $Y = xy' + yx'$.

And, by completing the square, we get

$$2x^2 + 2xy + 3y^2 = 2[(x + y/2)^2 + 5(y/2)^2],$$

a result known to Brahmagupta in 600 AD... Here $y/2$ is integer as y is even if the form $2x^2 + 2xy + 3y^2$ represents an odd prime p.

Lagrange proved Euler's Conjecture.

Forms are closed under the multiplication !!! (or **composition**, as they liked to say in those times). With this operation, the classes form a group of two elements (in modern language).

1.4 Legendre (1752–1833).

Showed in 1798 that this phenomena was not an accident: always the case for any nonequivalent quadratic forms forms with the same negative discriminant.

1.5 Gauss (1777–1855).

He was 21 at the time, and busy with similar problems. In 3 years he will publish his *Disquisitiones Arithmeticae*, which will change number theory forever.

Studied the group of non-equivalent classes of forms. Abelian finite groups. Came close to representing them as a direct product of cyclic groups. Very hard analysis. The proof is monstrous. Especially associativity: 37 statements, most of which Gauss leaves to the reader. It was 70 years before he was really understood.

Dirichlet, Dedekind and Hilbert simplified his presenattion.

Gauss later admitted that he ignored 'imaginaries' while doing that. In particular, Gauss proves that the ring of algebraic integers in $\mathbb{Q}(\sqrt{p})$ has $h = 1$ for

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

and conjectured that these are all. Proved by Baker (1966) and Stark (1967) independently. An equivalent statement is that the rings of quadratic algebraic integers of $\mathbb{Q}(\sqrt{p})$ with p from the list are the only ones with prime factorization. As far as I know, there is no similar complete description for positive p.

1.6 Kummer (1810–1893).

And Kummer was the next player. Primes and irreducibles. At that time people knew that numbers $a + b\sqrt{-5}$, a, b integers, have no unique factorization into primes:

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

Before we proceed, I wish to present one of my favorite example by Hilbert (1862-1943).

Hilbert's Example. Consider $S = \{1, 5, 9, 13, 17, 21, 25, 29, \ldots, 441, \ldots\}$. Closed under multiplication. Forget about addition. Primes in S are $\{5, 9, 13, 17, 21, 29, \ldots, 49, \ldots, \}$. No unique factorization into primes in S:

$$441 = 21 \times 21 = 9 \times 49. \quad !!!$$

Numbers $3, 7, 11$ are extraterrestrials for S. In $\mathbb{Z}$, $3 = \gcd(9, 21)$, $7 = \gcd(21, 49)$. If we add these "*idealic*" factors, the uniqueness of prime factorization will be saved:

$$441 = 3^2 7^2 \quad !!!$$

This example not only shows the problem with prime factorization and a hint how to fix it, it also shows (= proves) that it is impossible to prove The Prime Factorization Theorem in $\mathbb{Z}$ if we forget that the numbers in $\mathbb{Z}$ can be added!

Like Euler factored in $x^3 + y^3 = z^3$, Kummer, considering $x^p + y^p = z^p$, writes

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

where $\zeta^p = 1$. He gets uniqueness of prime factorization for 'integers' in $\mathbb{Q}(\zeta)$ for $p = 5, 7, 11, 13, 17, 19$, but not 23, for which he shows that the (analogous) class number $h = 3$. Fermat theorem was not his goal – reciprocity laws were. He, following similar results by Jacobi, and Dirichlet, trying to use analysis for computations of class numbers, gets *analytic* formuli. It is complicated to write details and explain. In the simplest case, $\mathbb{Z}[i]$, such a formula gives:

$$h(-1) \cdot \frac{\pi}{4} = \sum_{n \geq 1} (-1)^{n-1} \frac{1}{2n - 1}.$$

But it was known to the fathers of Calculus (Gregory (1671)) that the right hand side is $\frac{\pi}{4}$. So $h(-1) = 1$.

Kummer knew that the uniqueness of prime factorization was lost among the integers of $\mathbb{Q}(\zeta)$, $\zeta^p = 1$, but he kept pushing. Kummer work was very hard to penetrate, and his *ideal numbers* were never defined... But what he did define was the notion of divisibility of "them" (!), showed (or not, I did not understand) that they restore the uniqueness of prime factorization, and used it in a very powerful way for his reciprocity laws. Kummer referred to his numbers as 'ideal imaginary numbers'. Not many mathematicians were in piece with just imaginary numbers at that time... Very few people could read him and, actually, read him. Richard Dedekind was one of them.

2 Dedekind and Ideals

"My first demand is that arithmetics remains free from intermixture with extraneous elements,..."

Dedekind (1831–1916). The last student of Gauss he was a quite man who lived a quite life. In 1852 he completed his Ph.D. under Gauss (in 4 semesters) studying Eulerian integrals. Gauss testified that he *"knew a great deal"*, and *"was independent"*. In addition Gauss wrote that he had *"favourable expectations of his future career"*. (What a style!)

Being a good mathematician in conventional ways, Dedekind differed from many in believing that it was *"beneficial to meditate on issues"*, and he did that.

Objects in mathematics, which are hard to define, are not rare, and they existed forever. Just a few examples are:

- the notion of irrational in Greek mathematics
- complex ("imaginary") numbers discovered by Italians in the 16th century, where they suggested formuli for solving cubic and quartic equations. Complex numbers continued to be a mystery to many mathematicians even after Argand and Gauss suggested their geometric interpretation.
- The notion of a function or of a limit;
- The notion of a number (what is a number?);
- The notion of a geometry (what is Geometry?).

How important are the above questions anyway? Does one gain much by answering them? My answer is: "Sometimes certainly Yes". And one of the best examples is Dedekind's attempt to understand what Kummer's 'ideal numbers' were.

• What is a residue modulo n? Maybe a set (yes an infinite set, so what? – 1858, again in 1872)? " *"Horor of infinity" haunted math since Zeno and could not be dispelled overnight,"* especially with Kronecker present.

• What is a real number? Or maybe just an irrational number?

Dedekind cuts (1972). A real number is an ordered partition of $\mathbb{Q}$! For example, $\sqrt{2}$ can be thought the pair (A, B), where

$$A = \{r \in \mathbb{Q} : \; r^2 \le 2 \;\text{ or }\; r < 0\} \quad \text{and} \quad B = \mathbb{Q} \setminus A.$$

The rationals themselves can be thought in exactly this way, with a number belonging to any class. For example, a positive rational number m/n can be thought the pair (A, B), where

$$A = \{r \in \mathbb{Q} : \; r^2 \le m^2/n^2 \;\text{ or }\; r < 0\} \quad \text{and} \quad B = \mathbb{Q} \setminus A.$$

And the properties they posses remain the same if we think about them this way. One can easily introduce the order and operations on these partitions, and then prove (patiently!) that they satisfy all axioms of $\mathbb{R}$.

• By the way, some irrationals have something to do with the uniqueness of prime factorization: $(m/n)^2 = 2$ is equivalent to

$$m^2 = 2n^2.$$

Look at the exponent of 2 in both sides of this equality. It is even on the left, and odd on the right. Uniqueness of prime factorization gives a contradiction...

• What is the ideal number? Dedekind understood that the ideal number of Kummer was characterized by those numbers which it divided. Maybe the set of those numbers should be identified with the ideal numbers? If we take $\mathbb{Z}$ and consider number 5, is not it the same as to consider $\{0, \pm 5, \pm 10, \pm 15, \ldots\}$, or just $5\mathbb{Z}$? And, in general, to match n with $n\mathbb{Z}$?

Can we count with them as with usual integers? Yes, we may try

$$(a + b)\mathbb{Z} := a\mathbb{Z} + b\mathbb{Z}, \quad \text{and} \quad ab\mathbb{Z} := a\mathbb{Z} \cdot b\mathbb{Z}.$$

Seems fine, but nothing new about integers is gained this way.

Can one deal with ideal numbers the same way?

(a) Since an ideal number α of Kummer was associated with the set of all numbers it divided, then the set had the property of being closed under addition and multiplication: $\alpha a \pm \alpha b = \alpha(a \pm b)$.

(b) if the ideal number divided a number, it divided all its multiples: if $b = \alpha a$, then $bc = \alpha(ac)$

Maybe, this what, should be a guiding principle: If a set I is associated with an ideal number α in some strange domain $\mathcal{O}$ of "integers", then

(I) The sum and differences of the numbers in I is a number in I

(II) Any product of a number of I with a number of $\mathcal{O}$ is a number in I.

Obvious candidates for ideals are $r\mathcal{O}$, i.e., the principal ideals. What is next? To make his ideal numbers useful, Kummer multiplied and (sometimes) divided them. But it was hard to generalize what he did.

A very important definition: I **divides** J if $J \subset I$. In this sense $2\mathbb{Z}$ divides $6\mathbb{Z}$. A prime ideal is an ideal different from R whose only divisors are P and R.

Another very important definition: the **product** IJ of ideals I and J defined as all possible (finite) sums of xy, where $x \in I$ and $y \in J$. One sees that according to this definition, I and J divide IJ, but, for the purpose of arithmetics, we wish to have I divides J if $J = IH$ for some ideal H. And we wish H to be unique! This, e.g., is true for principal ideals in $\mathbb{Z}$.

It took Dedekind about four years to come up with these definitions, and to prove that in any ring of algebraic integers (i.e., in $\mathcal{O}$), I divides J if and only if there exists a unique H such that $J = IH$. He also showed that properties (I) and (II) capture the idea of Kummer's 'ideal numbers' precisely. Instead of having unique factorization in $\mathcal{O}$, which we often do not have, Dedekind restores it in the set of ideals of $\mathcal{O}$. Elements of the ring $\mathcal{O}$ itself corresponds only to *some* ideals in $\mathcal{O}$, namely the principal ideals, similarly to rational numbers corresponding to *some* Dedekind cuts. They form a subset of ideals closed under multiplication, but, often, there are very few of them in order to have the uniqueness of prime factorization. Note that we have not been adding the ideals so far. This makes a great analogy with Hilbert's example. But there can be many other, non-principal ideals in the ring $\mathcal{O}$.

In order to 'measure' how far one is from the uniqueness of prime factorization, two ideals are compared on their relative deviation from being principal. Classes of ideals in $\mathcal{O}$. $I \sim J$ if there exists an ideal M such that both IM and JM are principal ideals (maybe different). With this definition, the system of principal ideals forms a class by itself. If it is the only one equivalence class, then we have the uniqueness of factorization. (Remember that PID implies UFD?) The greater number of classes, the greater the deviation from prime factorization in $\mathcal{O}$.

===================================

But what Dedekind did was much more than making Kummer's arguments more precise. His theory covered all related previous studies as well. Just as a genius sculptor shapes the subject in few decisive blows of his hummer, he shaped the algebraic number theory, and a large part of modern algebra. By a simple arguments he realized that one must restrict to the "integers" in **only** *finite* extensions of $\mathbb{Q}$. Inside these fields, he defines an integer as an element which is a root of *monic* polynomial over $\mathbb{Q}$. It is not very hard to argue that all integers defined this way form a ring. So his approach covered **all** such rings, when approaches of his predecessors covered only a few examples, and their methods could not be generalized. And he did much more.

To me, Dedekind's approach to defining new objects reminds of an introvert philosophy or searching and finding (or building?) the answers within oneself, or within a system.

I will stop here, since there is no way that whatever I say can substitute the sources that I used. These are great books and I highly recommend them. Especially the Dedekind's.

==================================

To prepare this talk I used the following sources.

References

[1] Z. I Borevich and I.R. Shafarevich, Number Theory, Academic Press, New York, 1966.

[2] D. M. Burton, The History of Mathematics, An Introduction, Fifth Edition, McGraw-Hill, 2003.

[3] H. Cohn, Advanced Number Theory, Dover Publ. Inc., New York, 1962.

[4] R. Dedekind, Theory of Algebraic Numbers, Cambridge University Press, 1996.

[5] P. G. L. Dirichlet, Lectures on Number Theory, Supplements by R. Dedekind, AMS-LMS, 1999.

[6] H. M. Edwards, Fermat's Last Theorem; Genetic introduction to algebraic number theory, Springer-Verlag, 1977.

[7] I. James, Remarkable Mathematicians, From Euler to von Neumann, AMS-Cambridge University Press, 2002.

[8] I. N. Stewart and D. O. Tall, Algebraic Number Theory, Second edition, Chapman and Hall, 1987.

[9] A. Weil, Number Theory; An Approach through History. From Hammurapi to Legendre, Birkhäuser, 1984.

[10] http://www-history.mcs.st-andrews.ac.uk/Mathematicians/Dedekind.html

[11] http://www-history.mcs.st-andrews.ac.uk/Mathematicians/Dirichlet.html

[12] http://www-history.mcs.st-andrews.ac.uk/Mathematicians/Kummer.html