

NUMBER THEORY: MY DEVELOPMENT IN THE SUBJECT

VIPUL NAIK

ABSTRACT. My tryst with number theory has been long: I started on it with hobby math books.

1. BEGINNINGS IN SCHOOL

1.1. An encounter with primes and factoring. *Time period: 1997 - 2002*

When I was around eleven, I started reading a book by Keith Devlin titled *Mathematics: The New Golden Age*(book name). The first chapter discussed primality testing. It began with the Fermat test, which it claimed arose through some simple, but extremely clever, algebra. I tried for a long time to prove the theorem using the algebraic identities I had studied in school, but I could not succeed.

I learnt about Mersenne primes, Fermat primes, and other interesting numbers. I also read a book *The Man Who Loved Only Numbers*(book name) about Paul Erdos and his many exploits with primes. The fact that Fermat's conjecture, made 350 years ago, had been proved by Wiles only recently using advanced techniques, made me keen to know more of number theory.

I also came to know of appealing and simple unsolved problems in number theory, such as the Goldbach conjecture and the twin primes conjecture.

1.2. Olympiad preparation. *Time period: 2002-04*

On entering eleventh standard, I decided to study number theory seriously in order to do well on the Olympiads, and also to satisfy my natural curiosity in the subject.

I began by reading *Elementary Number Theory*(book name) by David Burton. I was taken in with the elegance of the proofs of Fermat's Little Theorem, as well as the statement and proof of Euler's theorem on the totient function. The most exciting part was the proof of the "quadratic reciprocity" result.

Alongside Burton, I also started reading *The Theory of Numbers*(book name) by Niven, Zuckermann and Montgomery. This book introduced me to a little linear algebra, the theory of quadratic forms, and the surprising group structure on elliptic curves. I also became familiar with the theory of algebraic integers and algebraic numbers, which was used to prove some harder results.

1.3. The Olympiad camps and the Olympiad. *Time period: May - July 2003, May - July 2004*

In the **International Mathematical Olympiad Training Camp**(camp name)¹, I came across many beautiful problems in number theory. While most of the number theory problems involved manipulations of congruences and inequalities, there were a few that used complicated versions of Fermat's little theorem and Euler's theorem in unexpected ways. The sixth problem of IMO 2003 was one of those gems:

Let p be a prime. Prove that there exists a prime q such that q does not divide $n^p - p$ for any integer n .

The proof uses a little bit of cyclotomic polynomials, and intersperses it with knowledge of the multiplicative group structure over p .

Later, while studying from *Abstract Algebra*(book name) by Dummit and Foote, I discovered the relation between this and a special case of Dirichlet's theorem on arithmetic progressions.

In the Training Camp for the 2004 Olympiad, I came across a question from the previous year's shortlist, whose solution required knowledge of an analogue of Fermat's little theorem for quadratic extensions. At the time, I had just started learning algebraic number theory, and this concrete application strengthened my appreciation for it.

©Vipul Naik, B.Sc. (Hons) Math, 3rd Year, Chennai Mathematical Institute.

¹For more details, see <http://en.wikipedia.org/wiki/IMOTC>

2. UNDERGRADUATE LIFE

2.1. Informal lectures. *Time period: October - November 2005*

Both my Olympiad background, and whatever I had read of algebraic number theory in commutative algebra texts, had made me very interested in number theory. Professor Balasubramanian, the director of **Institute of Mathematical Sciences**(place name), offered to conduct an informal lecture series for interested students. These lecture series went on for two months, and Professor Balasubramanian set up the language of algebraic number theory.

2.2. Elliptic curves and modular forms. *Time period: January - April 2006*

Professor Balasubramanian offered a course in **Elliptic Curves and Modular Forms**(course name) during my fourth semester. I had enjoyed reading about elliptic curves during my Olympiad days. Eager to learn more about them, I audited the course. In the course, I learnt a lot about the group structure of elliptic curves. Big results like the Mordell-Weil theorem and the Lutz-Nagell theorem were proved.

The second half of the course dealt with the vector spaces of modular forms, and also introduced concepts of $\Gamma(N)$. Some of the material was hard to grasp in the beginning, but gradual exposure to it made it seem more and more natural.

Towards the end of Professor Balasubramanian's course, I had learnt about Dirichlet L -functions. I talked to an M.Sc. student from CMI (Jagmohan Tanti) who told me about ongoing work on the "Selberg class" and the use of complex analysis in this work.

2.3. Microsoft Research Summer School. *Time period: May - June 2006*

The **Microsoft Research Summer School in Algorithms, Complexity and Cryptography**(camp name) focussed on important cryptographical problems and their implications both in complexity theoretic and in number theoretic terms. During the summer school, some concepts covered in the elliptic curves course were revisited in an unexpected way. I learnt interesting algorithms for factoring, in particular, Dixon's random squares algorithm.

I also started getting a better feel for the known results on the structure of the multiplicative group modulo p .

2.4. A more algebraic-geometry flavour of number theory. *Time period: August - December 2006*

This semester, I credited the **Abelian varieties**(course name) course offered by Professor Ramanan. This course ostensibly had little to do with number theory the way I knew it at high school. Professor Ramanan's course aimed at discussing how the "complex torus" could be embedded as a complex-analytic manifold (and hence, as a complex projective variety).

However, the first part of the course covered a lot of ground similar to what Professor Balasubramanian had covered in his **Elliptic Curves and Modular Forms**(course name) course. Professor Ramanan also discussed the use of congruence subgroups and their significance from the viewpoint of algebraic geometry.

I later learnt that the theory of automorphic forms is considered a sibling of number theory. I am keen to learn both of these and also about why they are considered so close.

2.5. The congruence subgroup problem. *Time period: October - November 2006*

Professor Balasubramanian had mentioned the congruence subgroup problem during the **Elliptic Curves and Modular Forms**(course name) course. This semester, I began a detailed study of the problem from the book *The Congruence Subgroup Problem*(book name) by B Sury. It helped me understand generalizations of the ζ functions in algebraic number theory. I plan to continue the study next semester.

2.6. Transcendental number theory: Waalschmitz's talk. *Time period: November 2006*

Mikhael Waalschmitz gave a talk series on Transcendental Number Theory at the **Institute of Mathematical Sciences**(place name) a few weeks ago. He discussed generalizations of the usual results on Diophantine approximation to simultaneous Diophantine approximations. He considered numbers which are defined by means of infinite series, their algebraic approximability, and the four kinds of real numbers. He also discussed the slippery concept of "almost all numbers".

3. MY OWN INITIATIVES

3.1. Problems I formulated. During Olympiad preparation, I had come across the result: the ring of polynomials with rational coefficients that sends integers to integers, is additively a free module generated by polynomials of the form $\binom{x}{k}$.

This led me to consider the corresponding question over a ring of integers:

Let K be a number field. Let R be the ring of integers in K . Can we describe explicitly the ring of polynomials with coefficients in K , that map R to within R ?

I found the question somewhat hard, and I tried obtaining results for a few quadratic extensions. Later, I asked Professor Waalschmidt about the problem. He informed me that Ably has very recently settled the problem for the Gaussian integers. I plan to study more on this front.

3.2. Multiplicative number theory. I had enjoyed studying arithmetic functions, multiplicativity and the Dirichlet convolution during high school days. Improved understanding of group theory helped me get a better grasp of multiplicative number theory. I read Tom Apostol's *Introduction to Analytic Number Theory*(book name). In my fifth semester, I also gave a talk on multiplicative number theory as part of a Student Talks initiative.

4. FURTHER PLANS

4.1. Algorithmic/cryptographical questions in number theory. The Microsoft Research Summer School has whetted my appetite for number theory. I plan to study more about the cryptographical aspects of number theory and the upper and lower bounds for algorithmic problems, particularly in elliptic curves. I also want to learn more about pairing over elliptic curves on finite fields and about supersingular curves.

4.2. Multiplicative number theory. Professor Balasubramanian might take a course in multiplicative number theory next semester. I plan to attend the course if it happens.

4.3. Estimation techniques. I want to learn more about L -functions, and the use of complex analytical estimation techniques in number theory.

4.4. Congruence subgroup problem. I will resume my study of the congruence subgroup problem next semester.

APPENDIX A. BOOKS

A.1. Introductory books on number theory.

- (1) *Elementary Number Theory*(book name) by David M. Burton

How I used the book: This book introduced me formally to the notions of congruence, the proof of Fermat's little theorem, the proof of Euler's theorem, and the beautiful proofs of quadratic reciprocity. I found it an excellent introductory book with good exercises.

- (2) *An Introduction to Number Theory*(book name) by Niven, Zuckermann, and Montgomery.

How I used the book: Although this book is meant as a college-level book, many parts of it are accessible even to high school students. I liked the chapters on density theorems, as well as the introduction to notions of algebraic integers. The book gave me my first glimpse into the exciting world of elliptic curves.

A.2. Books on subtopics in number theory.

- (1) *An Introduction to Analytic Number Theory*(book name) by Tom Apostol.

How I used the book: After completing my first semester at CMI, I studied the techniques used in this book to estimate sums for common arithmetic functions such as σ . This knowledge built on earlier knowledge that I had acquired during Olympiad preparation.