SOME CLASSICAL PROBLEMS LEADING TO MODERN NUMBER THEORY

Mladen Dimitrov

July 28th 2000

1 Introduction

People from the Antiquity were interested in studying relations between geometry and natural numbers. One of the most classical problems is that of finding all Pythagorean triangles, in other words triples (a, b, c) of positive integers with $a^2 + b^2 = c^2$. The primitive triples (i.e. these with no common factor) are parametrized by the pairs of positive integers (m, n), with $g.c.d.(m, n) = 1$ and $m - n$ odd positive, in the following way : $a = 2mn$, $b = m^2 - n^2$ and $c = m^2 + n^2$. Pythagoras lived around 500 BC and was the first to formalize the notion of "proof". He said that "Everything is a number", but he didn't accept irrationals. Later around 300 BC Euclid wrote "The Elements", where he compiled in several books the greek knowledge of mathematics. At last Diophantus came around 300 AD and studied rational solutions of algebraic equations. His famous book "Arithmeticae" was republished in the Renaissance and gave the taste for number theory to the french mathematician Fermat.

2 Fermat's Notes

Fermat wasn't a professional mathematician, but he studied the book of Diophantus and left many statements and remarks in the margins of "Arithmeticae". Here are some of them :

Let p be an odd prime number.

Statement 2.1 *There exist integers x and y such that $p = x^2 + y^2$ if and only if $p \equiv 1 (mod\ 4)$.*

Statement 2.2 *There exist integers x and y such that $p = x^2 + 2y^2$ if and only if $p \equiv 1$ or $3 (mod\ 8)$.*

Statement 2.3 *There exist integers x and y such that $p = x^2 + 3y^2$ if and only if $p \equiv 1 (mod\ 3)$.*

Statement 2.4 *There exist integers x and y such that $p = x^2 - 2y^2$ if and only if $p \equiv 1$ or $7 (mod\ 8)$.*

Statement 2.5 *If d is a squarefree positive integer, then the equation $x^2 - dy^2 = 1$ has infinitely many integer solutions.*

Statement 2.6 *The only integer solution of the equation $x^3 = \frac{y(y+1)}{2}$ is $x = y = 1$.*

Statement 2.7 *The only integer solution of the equation $x^3 = y^2 + 2$ is $(x, y) = (3, 5)$.*

Statement 2.8 *Each number is both the sum of at most three triangular numbers, and the sum of at most four square numbers.*

Statement 2.9 *There doesn't exist a right triangle with rational sides and area 1 or 2.*

Statement 2.10 *The equation $x^n + y^n = z^n$ has no nontrivial rational solutions, if the integer n is at least 3.*

All these problems have led to beautiful mathematics. The first half of them are related to quadratic number fields, which are discused in the next section.

The other problems (except the eighth) are very closely related to the study of rational points on elliptic curves. For exemple one can prove that there exists a right triangle with rational sides and integer area d if and only if the elliptic curve $y^2 = x^3 - d^2x$ has rational points of infinite order. Similary, for the last problem (the famous Fermat's last theorem), if n is a prime larger than 5, then a non trivial solution $a^n + b^n = c^n$ would give birth to an elliptic curve $y^2 = x(x - a^n)(x + b^n)$ that would be so peculiar that it would contradict the Modularity Conjecture. This is the way *Wiles* proved this theorem in 1994.

3 Quadratic Number Fields

In the study of the statements 1 to 5, we see that the difficulty is that $x^2 - dy^2$ doesn't factor over $\mathbb{Q}$. Meanwhile it does factor over $\mathbb{C}$: $x^2 - dy^2 = (x + \sqrt{d}y)(x - \sqrt{d}y)$. So we are naturally led to make the following definition:

If d is a squarefree integer different from 0 and 1, define $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} | a, b \in \mathbb{Q}\}$, which is a field extension of $\mathbb{Q}$ of degree 2.

It's natural to ask if we have some kind of theorem about existence and uniqueness of factorization in these fields. But before we have to answer some questions :

Question 1 What's the counterpart of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$?

Answer : The natural definition of an integer in $\mathbb{Q}(\sqrt{d})$ is a number which is root of a monic polynomial with coefficients in $\mathbb{Z}$. So the ring $\mathcal{O}$ of integers in $\mathbb{Q}(\sqrt{d})$ is formed by numbers of the form $a + b\sqrt{d}$, where a and b are both integers, or both half integers (the second case being allowed only if $d \equiv 1(\mod 4)$).

Question 2 What are units in $\mathcal{O}$?

Answer : The units are numbers of the form $a + b\sqrt{d}$, such that $a^2 - db^2 = \pm 1$.

Question 2 What are irreducible elements in $\mathcal{O}$?

Answer : An element $\pi \in \mathcal{O}$ is irreducible if it is not a unit and cannot be written as a product of two other non unit elements of $\mathcal{O}$. Such an element is either an ordinary prime, or a number of the form $a + b\sqrt{d}$, such that $a^2 - db^2$ is an ordinary prime.

We have the following theorem:

Theorem 3.1 *Let d be one of $-1, -2, -3$ or 2. Then $\mathcal{O}$ is a unique factorization domain, in the sense that every element of $\mathcal{O}$ decomposes into a product of irreducible elements in a unique way, up to a permutation of the factors and multiplication by unit elements.*

Proof of Statements 1,2,3 and 4 :

The equation $p = x^2 + dy^2$ has integer solutions

$\iff$ $p = (x + y\sqrt{d})(x - y\sqrt{d})$

$\iff$ p is not irreducible in $\mathcal{O}$

$\iff$ there exists an integer z such that $z^2 - d \equiv 0 (\mod p)$

$\iff$ $\left(\frac{d}{p}\right) = 1$, which gives the desired list of primes using Gauss' quadratic reciprocity law.

The important step in this proof is the following : If we have an integer z such that p divides $z^2 - d$, then the unique factorization tells us that p is not irreducible, because p doesn't divide $z - \sqrt{d}$, nor $z + \sqrt{d}$. This is no more true if we don't have the unique factorization : consider for exemple the identity $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3$.

Theorem 3.2 *(Baker, Stark 1966) Let d be negative. Then $\mathcal{O}$ is an unique factorization domain if and only if d is one of -1, -2, -3, -7, -11, -19, -43, -67 and -163.*

And the end of this section I would like to mention that the statement 5 says that there are infinitely many units in a real quadratic number field, which is a particular case of the Dirichlet's theorem about units in number fields.

4 Elliptic Curves

An elliptic curve E over $\mathbb{Q}$ is given by the equation $E : y^2 = x^3 + ax + b$, where $a, b \in \mathbb{Q}$ and $\Delta = 27b^2 - 4a^3 \neq 0$.

For a field F we denote by $E(F)$ the points of E whose coordinates are in F.

We define an addition law on the set $E(\mathbb{C}) \cup \{\infty\}$ as follows :

- ∞ is a zero element.
- The opposite of a point (x, y) is the point $(x, -y)$.
- The sum of two different, non opposite points is the opposite of the third point of intersection of the line passing through these two points and $E(\mathbb{C})$.

Remark 1 : When the two points are the same we take the tangent line, instead of the line passing through the two points.

Remark 2 : The sum of one point and its opposite is the zero element.

Proposition 4.1 *$(E(\mathbb{C}) \cup \{\infty\}), +)$ is an abelian group.*

Fermat's problems lead to the study of the set of rational points on an elliptic curve.

Theorem 4.2 *(Mordell 1922) $E(\mathbb{Q})$ is an abelian group of finite rank, i.e. the direct sum of a finite abelian group T and finite number r of copies of $\mathbb{Z}$.*

There are many methods to find T. The same is not true for the integer r, which is called the rank of the elliptic curve. So the problem of finding rational points on elliptic curves is ultimately related to the problem of finding the rank. The Birch-Swinnerton-Dyer conjecture would give an analytic method for finding the rank.

5 Acknowledgements

I would like to thank the Department of Mathematics of Pondicherry, and especially Prof. Indumathi, Prof. Ramaswamy and Prof. Jothilingam for their invitation and warm welcome.

Mladen Dimitrov
Département de Mathématiques et Applications
École Normale Supérieure
45, rue d'Ulm
75230 Paris Cedex 05, France
dimitrov@clipper.ens.fr