Lecture 6 (04 June 2009)

Sums of Squares

The two squares. In our first lecture we have found the description of all Pythagorean triples, i.e. the solution of the diophantine equation $x^2 + y^2 = z^2$. A triple (x, y, z) of relatively prime positive integers with y being even, is Pythagorean, if there exists $m, n \in \mathbb{N}$, relatively prime of different parity, such that $x = m^2 - n^2, y = 2mn, z = m^2 + n^2$, and all such pairs (m, n) give rise to a primitive Pythagorean triple.
Looking at the equation from another perspective, we see that we have answered the question about which squares could be represented as sum of two squares: z^2 is sum of two relatively prime squares if and only if z is a sum of squares. It is natural to ask the questions: which natural numbers are sum of two squares? The goal of this section is to give a complete answer to this question. We will do so in five steps:

1. reduction to primes;
2. primes of the form $4k + 3$ are never sum of two squares;
3. primes congruent to 1 modulo 4 always divide an integer of the form u^2+1,
4. descent from $u^2 + 1 = np$ to $x^2 + y^2 = p$,
5. putting it all together.

Step 1. Consider the equality

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

It says that if two numbers are sum of two squares, so is their product.
For example $493 = 17 * 29$ and $17 = 1^2 + 4^2$, $29 = 2^2 + 5^2$
give $493 = (1 * 2 - 4 * 5)^2 + (1 * 5 + 4 * 2)^2 = 18^2 + 13^2$. Since every number is product of primes, we are well advised to find out which primes are sum of squares first, and gluing this together into an answer for the arbitrary integer.

Step 2. Let $p = 4k+3$ be a prime. Then p is not a sum of two squares. Indeed, sum of two squares of the same parity is an even number, and if x is odd and y even, then

$$x^2 + y^2 = (2x_1 + 1)^2 + (2y_1)^2 \equiv 4x_1^2 + 4x_1 + 1 + 4y_1^2 \equiv 1 \pmod 4$$

while $p \equiv 3 \pmod 4$. Note that we haven't used that p is prime to get the result, but only that p is congruent to 3 modulo 4.

Step 3. Let $p = 4k + 1$ be a prime. We give an explicit integer u such that $u^2 + 1 \equiv 0 \pmod{p}$. By Wilson's theorem, $(p-1)! + 1 \equiv 0 \pmod{p}$. So

$$\begin{aligned}(p-1)! + 1 &= 1 * 2 * \cdots (2k-1) * (2k) * (2k+1) * (2k+2) \cdots (4k-1) * (4k) + 1 = \\ &= 1 * 2 * \cdots (2k-1) * (2k) * (p-2k) * (p-(2k-1)) \cdots (p-2) * (p-1) + 1 \equiv \\ &\equiv 1 * 2 * \cdots (2k-1) * (2k) * (-2k) * (-(2k-1)) \cdots (-2) * (-1) + 1 \equiv \\ &\equiv (-1)^{2k}((2k)!)^2 + 1 \equiv ((2k)!)^2 + 1 \pmod{p}\end{aligned}$$

and we see that $u = (2k)!$ fits the bill.

Step 4. Here we show that if $p = 4k + 1$ is a prime, than $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$. By Step 3 there exist integers u, v and n such that $u^2 + v^2 = np$. If $n = 1$, we are all set. We show that if $n > 1$, we could produce an equation $u_1^2 + v_1^2 = n_1 p$, with $n_1 < n$. Using this *descent procedure* repeatedly, we will get the needed representation after finitely many steps.

If n is even, than u, v are of the same parity, and we take
$u_1 = (u - v)/2$, $v_1 = (u + v)/2$, $n_1 = n/2$, and then $u_1^2 + v_1^2 = n_1 p$ as one could easily check. If n is odd, then select $a, b \in \mathbb{Z}$ with
$a \equiv u \pmod{n}$ and $b \equiv v \pmod{n}$, $\quad |a| < n/2$ and $|b| < n/2$. and look at the identity

$$(a^2 + b^2)(u^2 + v^2) = (au + bv)^2 + (au - bv)^2.$$

By the choice of a and b both the multipliers on the left and the adders on the right are divisible by n, so setting
$u_1 = (au+bv)/n$, $v_1(au-bv)/n$, $n_1 = (a^2+b^2)/n$ works this time, with $n_1 < n/2$ following from the inequalities on a, b.

Step 5. Here we put the arguments from the previous steps together, and prove:

Theorem. A natural number n could be written as a sum of the squares of two integers if and only if every prime factor p of n which is of the form $4k+3$ enters the canonical decomposition of n to an even degree.

Examples: $306 = 2 * 3^2 * 17$ is sum of two squares, while $102 = 2 * 3 * 17$ is not.

Proof. Let n be a number with factorization of the kind described in the theorem. By repeatedly applying Step 4 and the formula (*) from Step 1, we represent the factor of n comprising of all the powers of 2 and primes $\equiv 1 \pmod{4}$ as a sum of two squares. The remaining factor is then a perfect square, so we distribute it and get the desired representation.

In the other direction, we have to show that if a number could be written as a sum of two squares, than all primes of the type $4k + 3$ divide it to an even power.

Let $x, y \in \mathbb{Z}$ and $p = 4k + 3$ are such that $p | x^2 + y^2$.

Assume that $(y, p) = 1$. Then there is a z such that $yz \equiv 1 \pmod{p}$ and the so $x^2 + y^2 \equiv 0 \pmod{p}$ gives $(xz)^2 \equiv -1 \pmod{p}$, or $(xz)^{p-1} \equiv (-1)^{2k+1} \equiv -1 \pmod{p}$ in contradiction with Fermat's little theorem. So the assumption $(y, p) = 1$ is false. Hence $p | y$ and then $p | x$, and consequently p enters n to an even degree. $\square$

The four squares theorem. This is the name of the following statement:

Theorem. Every natural number could be written as the sum of four integers.

It is contained Diophantus *Arithmetica* and was proved in 1770 by the French mathematician Joseph Louis Lagrange. His proof used the identity

$$(a^2+b^2+c^2+d^2)(t^2+u^2+v^2+w^2) = (at-bu-cv-dw)^2+(au+bt+cw-dv)^2+ \\ +(av-bw+ct+du)^2+(aw+bv-cu+dt)^2$$

together with descent techniques to give a proof similar in spirit to the one we exhibited for the two squares case.
Later the German mathematician Carl Gustav Jacobi used *theta functions* which are a type of analytic objects possessing a lot of symmetry, and power series expansions like

$$\vartheta(x) = \sum_{n=-\infty}^{\infty} e^{-n^2\pi x}$$

to give a very different proof which also provided a formula for the number of different ways a number could be represented as a sum of four squares.
A third important approach for proving this theorem was found by Herman Minkowski, who used his convex body theorem, which in its simplest case says that any convex and centrally symmetric shape in the coordinate plane with area bigger than 4 contains a point with integral coordinates different than the origin. Minkowski's theorem could be used for a short and aesthetically pleasing proof of the two squares theorem as well.

Beyond squares. Lagrange's four squares theorem could be generalized in at least two ways. One is the statement that every positive integer is sum of k-figural numbers, in particular a sum of 3 triangular numbers, or 4 square numbers, or 5 pentagonal numbers, etc. This was conjectured by Fermat and proved by Louis Auguste Cauchy.
A second is the so called Waring problem. Waring conjectured, that given $k \in \mathbb{N}$, there exists a constant $g(k)$, depending only on k, such that every $n > 1$ is sum of at most $g(k)$ $k-th$ powers. For example, Lagrange's theorem implies that $g(2) \leq 4$, and since 7 cannot be represented as a sum of 3 squares, $g(2) = 4$. The Waring conjecture has been proved, using methods from analytical number theory, which are very different that any part of the approach we used in the prove in the two squares theorem. However, the exact value of $g(k)$ is still conjectural, and his been established only for $k \leq 6$, in particular we know that $g(3) = 9, g(4) = 19$.

Combinations of squares. Which numbers are sums of the form x^2+2y^2? What about x^2+3y^2, or more general x^2+ny^2? We will say a few words on this question, which is partially answered by Gauss Reciprocity Law, and has ultimately lead to a whole new mathematical discipline, namely the Class Field Theory.