

From Tue Dec 7 15:15:41 2004
Date: Tue, 7 Dec 2004 15:15:36 -0500 (EST)
From: Alya Asarina
To: Daniel Rogalski
Subject: Re: announcements (paper, etc.)

11/17 lecture notes.

Here are my lecture notes from the last lecture:

Last time:

Proposition: Let m in \mathbb{Z} , $m \geq 1$. Then every solution to the equation $x^3 + y^3 = m$ (x, y in \mathbb{Z}) satisfies $\max(|x|, |y|) \leq 2\sqrt[3]{m/3}$.

Consider the integer solutions of $x^3 + y^3 = m$, counting (x, y) and (y, x) as one solution (symmetry).

Question: How many solutions are there for each m ?

$1 \leq m \leq 1728$: 1 sol'n in positive integers
 $m = 1729$: 2 sol'ns in positive integers
3, 4, ... solutions?

Proposition: For every integer $N \geq 1$, there is a integer $m > 1$ s.t. the cubic curve $x^3 + y^3 = m$ has at least N points with integer coordinates.

Proof:

Claim: $x^3 + y^3 = 9$ has infinitely many rat'l solutions.

Proof:

Ch. 1, sect. 3: There is essentially a one-to-one correspondence between rational points on $x^3 + y^3 = 9$ and on $Y^2 = X^3 - 48$ given by

$$X = 12/(x+y), Y = 12(x-y)/(x+y)$$

(We're basically converting our eq'n to Weierstrass normal form.)

Consider $(2, 1)$ on $x^3 + y^3 = 9$.

$(x, y) = (2, 1)$ on $x^3 + y^3 = 9 \rightarrow Q = (12/3, 12 \cdot 1/3) = (4, 4)$ on $Y^2 = X^3 - 48$.

Compute: $2Q = (28, -148)$, $3Q = (73/9, 595/27)$, so by Nagell-Lutz Q has infinite order. nQ is rational, so $Y^2 = X^3 - 48$ and $x^3 + y^3 = 9$ have infinitely many rat'l pts.

Since there are infinitely many rat'l pts on $x^3 + y^3 = 9$, we can pick N of them: P_1, \dots, P_N .

Let $P = (a/b, c/d)$ be a P_i given in lowest terms.

Plug in: $a^3/b^3 + c^3/d^3 = 9$

$$a^3 \cdot d^3 + c^3 \cdot b^3 = 9b^3 \cdot d^3$$

So $b^3 | a^3 \cdot d^3$, $d^3 | c^3 \cdot b^3$. $\gcd(a, b) = \gcd(c, d) = 1$, so $b^3 | d^3$, $d^3 | b^3$, and $b^3 = \pm d^3$. Taking positive denominators, we have $b = d$, so we can write (from above) $P_i = (a_i/d_i, c_i/d_i)$.

Pick m to clear denominators of P_i 's.

Let $m = 9 (d_1 \cdot d_2 \cdot \dots \cdot d_N)^3$. Then multiplying the coordinates of any P_i by $d_1 \cdot d_2 \cdot \dots \cdot d_N$ gives an integer point on $x^3 + y^3 = m$. That is, let

$P_i' = (a_i \cdot d_1 \cdot \dots \cdot d_{i-1} \cdot d_{i+1} \cdot \dots \cdot d_N, c_i \cdot d_1 \cdot \dots \cdot d_{i-1} \cdot d_{i+1} \cdot \dots \cdot d_N)$.

Then P_1', \dots, P_N' are integer points on $x^3 + y^3 = 9$

$(d_1 \cdot d_2 \cdot \dots \cdot d_N)^3$. QED

The proposition is still true if we consider only $x, y > 0$.

Claim: If $x^3 + y^3 = m$ ($m > 0$) has infinitely many rational solutions, it has infinitely many rational solutions with $x, y > 0$.

Sketchy Proof:

The set of real points on this curve looks like the group of complex #'s on unit circle under multiplication (the circle group). Thus a subgroup generated by a point of infinite order is dense in the set of real points on the curve. Since there are real points with $x, y > 0$, an open set of such points will contain infinitely many rational points with $x, y > 0$.

Next question: Given an integer N , is it possible to find an integer $m \geq 1$ s.t. $x^3 + y^3 = m$ has at least N solutions with $\gcd(x, y) = 1$ and $x > y$?

Answer: unknown

For $N=3$, $m=3242197$ works, and there's an m for $x, y > 0$.

For $N=4$, we don't know.

Theorem (Silverman): Let $m \geq 1$ be an integer, and let C_m be the cubic curve $C_m: x^3 + y^3 = m$. Then there is a constant $k > 1$ independent of m s.t.

$$\#\{(x, y) \text{ in } C_m(\mathbb{Q}) \mid x, y \text{ in } \mathbb{Z}, \gcd(x, y) = 1\} \leq k^{(1 + \text{rank } C_m(\mathbb{Q}))}.$$

Interpretation: Integer pts w/ $\gcd(x, y) = 1$ "tend to be somewhat linearly independent." Find lots of these \implies rank is large. So if we find a sequence of m 's s.t. the number of int points in $C_m(\mathbb{Q})$ w/ $\gcd(x, y) = 1 \rightarrow$ infinity, we'll have shown that there are cubics of arbitrarily large rank (open question).

$x^3 + y^3 = (x+y)(x^2 - xy + y^2)$, so finding all integer sol'ns for $x^3 + y^3 = m$ is easy (consider factorizations). But hard to tell when eqn's that don't factor have infinitely many solutions. For example, $x^2 - 2y^2 = m$ often does.

Theorem (Thue): Let a, b, c , be non-zero integers. Then the equation $ax^3 + bx^3 = c$ has only finitely many solutions in integers x, y . [Proof to be finished next time.]

(x, y) solves $ax^3 + bx^3 = c \implies (ax, y)$ solves $X^3 + a^2 * b * Y^3 = a^2 * c$, so it is enough to prove Thue's theorem for $a=1$.

By replacing y by $-y$ and/or b by $-b$ if necessary, it is enough to look at the equation $x^3 - b * y^3 = c$ with b, c positive integers.

Let $\beta = \text{cube root}(b)$.

$$x^3 - by^3 = (x - \beta y)(x^2 + \beta xy + \beta^2 y^2)$$

β an integer \implies done, so take β not an integer.

x, y large $\implies |x/y - \beta|$ small:

$$x^2 + \beta xy + \beta^2 y^2 = (x + (1/2)\beta y)^2 + (3/4)\beta^2 y^2 >= (3/4)\beta^2 y^2, \text{ so}$$

$$|c| >= |x - \beta y| * (3/4)\beta^2 y^2.$$

Dividing by $(3/4)\beta^2 y^3$, we get $|x/y - \beta| \leq$

$$(4|c|/3\beta^2) * (1/|y|^3).$$

(x, y) sol'n w/ $|y|$ large $\implies |x/y - \beta|$ small, so x/y is close to β .

To prove that finitely many integer sol'ns, prove that finitely many rat'ls w/ this approximation property.

Next time:

Diophantine Approximation Theorem: Let $b > 0$ be an integer which is not a perfect cube, and let $\beta = \text{cube root}(b)$. Let C be a fixed positive constant. Then there are only finitely many pairs of integers (p, q) w/ $q > 0$ which satisfy $|p/q - \beta| \leq C/q^3$.