Congruent Number Problem and Elliptic curves

December 12, 2010

Contents

Chapter 1

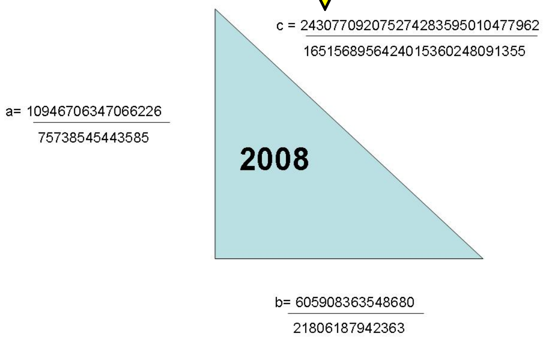
Congruent Number problem

Definition 1 ***Congruent Numbers:*** *A positive rational number $r \in \mathbb{Q}$ is called a "Congruent number" if it its the area of some right triangle with rational sides.*

Suppose $r \in \mathbb{Q}$ is a congruent number and X, Y, Z are the corresponding sides of the right triangle, then we can choose a $s \in \mathbb{Q}$ such that $s^2 r$ is a squaree free integer. And $s^2 r$ is a congruent number, corresponding to the right triangle with sides sX, sY and sZ. (If $r = \frac{p^2 u}{q^2 v}$ where u and v are square free and p, q, u and v are pairwise relatively prime, then choose $s = \frac{qv}{p}$.) Henceforth, we assume that n is squarefree.

The question of determining whether a given rational number is a congruent number is called **The Congruent number problem**.

If X, Y, Z are the sides of a right triangle and furthermore, if X, Y, Z are pairwise coprime, then the general solutions can be given as $X = m^2 - n^2$, $Y = 2mn$ and $Z = m^2 + n^2$ where m, n are integers that are relatively prime. So theoretically it is possible to list down all pythagoreann triples and consequently list all congruent numbers. Note however, that this does not give us an algorithm to determine whether a GIVEN number is congruent or not. The following figure shows that the naive apporach to list down all pythagorean triples is not a great algorithm.


c = 2430770920752742835950104779626 / 1651568956424015360248091355
a= 10946706347066226 / 75738545443585
2008
b= 605908363548680 / 21806187942363

1.1 1 is not a congruent number

Let us suppose that X, Y, Z correspond to rational sides of a right triangle such that $\frac{XY}{2} = 1$. Then by multiplying by a suitable rational number a, we get a triangle with sides x, y, z (and they are a primitive triple) such that $\frac{xy}{2} = a^2$. So there exists m, n integers that are relatively prime such that $x = m^2 - n^2$ and $y = 2mn$. so

$$xy = (m^2 - n^2)mn = a^2$$

. Since m and n are coprime and since the right hand side of the above equation is a square, it would imply that m,n and $m^2 - n^2$ are all squares i.e. $m = u^2$, $n = v^2$ and $m^2 - n^2 = d^2$ which means that

$u^4 - v^4 = d^2$

Lemma 2 ***Fermat's infinite descent*** *There are no solutions to the equation* $x^4 = y^4 + u^2$.

PROOF: Without loss of generality, assume that x, y and u have no common factor. Also we claim that we can assume u is odd. Suppose there exists such a solution, then we can form a pythagorean triple (u, y^2, x^2) because $(x^2)^2 = (y^2)^2 + u^2$. Since they form a primitive pythagorean triple, there exists integers m, n that are relatively prime such that $u = 2mn$ (we assume u is even), $y = m^2 - n^2$ and $x = m^2 + n^2$. Here x, y are both odd and hence $(xy)^2 = m^4 - n^4$ which is an equation of the form above and xy is odd.
Thus we assume that u is odd. Assume that among all solutions for the equation above, u is the smallest positive integer. Since $(x^2)^2 = (y^2)^2 + u^2$, we proceed similarly finding two relatively prime integers p, q such that $y^2 = 2pq$ and $u = p^2 - q^2$ and $x^2 = p^2 + q^2$. Since p, q are coprime, we can set $q = 2a^2$ and $p = b^2$. Also $x^2 = p^2 + q^2$ form a pythagorean triple. So we can write $p = r^2 - s^2, q = 2rs$ and $x = r^2 + s^2$.
Since $2a^2 = 2rs$ we have that $r = c^2$ and $s = d^2$. These along with $p = b^2$ imply that $b^2 = c^4 - d^4$. Here b is smaller than u contradicting the minimality of u. Thus we get the following result.

Theorem 3 *1 is not a congruent number.*

$2, 3, 4$ have been proved not to be congruent numbers but $5, 6, 7$ are.

Chapter 2

Certain Elliptic Curves

Consider

$$y^2 = x^3 - n^2 x.$$

Call this curve E_n. Given a right triangle with rational sides X, Y, Z and area n, we obtain a point (x, y) in the xy-plane having rational coordinates and lying on this curve by setting

$$x = (Z/2)^2$$

$$y = (X^2 - Y^2)Z/8$$

But given a rational point lying on such a curve, does not necessarily come from a right triangle with area n and having rational sides.

Theorem 4 *Let (x, y) be a point with rational coordinates on the curve $y^2 = x^3 - n^2 x$. Suppose that x satisfies the three conditions*

1. *it is the square of a rational number*
2. *its denominator is even*
3. *its numerator has no common factor with n.*

Then there exists a right triangle with rational sides and area n, which correspondes to x

Proof: Let $u = \sqrt{x} \in \mathbb{Q}^+$. Set $v = \frac{y}{u}$, so that $v^2 = x^2 - n^2$. Let t be the denominator of u, i.e. the smallest positive integer such that $tu \in \mathbb{Z}$. By assumption t is even. Notice that the denominators of v^2 and x^2 are the same. This denominator is t^4. Thus, $t^2 v, t^2 n, t^2 x$ form a primitive pythagorean triple, with $t^2 n$ even. There exists integers a, b such that $t^2 n = 2ab, t^2 v = a^2 - b^2$ and $t^2 x = a^2 + b^2$. Then the right triangle with sides $\frac{2a}{t}, \frac{2b}{t}$ and $2u$ has the desired area n.

If $P = (x, y)$ is a point on the elliptic curve not of order 2, then with the additional law on the points on elliptic curves, we get that then the x-coordinate of $2P$ is

$$\frac{(x^2 + n^2)^2}{(2y)^2}$$

This point satisfies all the conditions of theorem 4

- It is clearly the square of a rational number.
- If the numerator had a common factor with n say d, then d divides x and consequently divides y^2 also. But n was assumed to be squarefree. So the numerator does not have a common factor with n.

- We write $x = \frac{x_1}{x_2}$ where x_1, x_2 are integers with no common factors. Thus the x-coordinate of $2P$ turns out to be
$$\frac{(x_1^2 + n^2 x_2^2)^2}{4(x_1)(x_2)(x_1 + nx_2)(x_1 - nx_2)}$$
. We divide it into three cases. Case i): If the numerator is odd, then we are done because the denominator is even because of the 4 present. Case ii: If the numerator is even, then x_1, x_2 and n, are odd, Consequently the numerator is a multiple of 4 and not 8. The denominator however is a multiple of atleast 16, and so the denominator is even.

Hence by theorem 4, it is sufficient to find a point not of order 2 to say that n is congruent.

Chapter 3

Using the Mordell Weil theorem

Theorem 5 *Let $q = p^f$ and $p \nmid 2n$. Suppose that $q \equiv 3(mod4)$. Then there are $q + 1$ $\mathbb{F}_q$-points on the elliptic curve $y^2 = x^3 - n^2x$*

Proof: There are 4 points of order 2 - $(0, 0), (n, 0), (-n, 0)$ and the point at infinity. Now we count all pairs (x, y) where $x \neq 0, n, -n$. Since $f(x) = x^3 - n^2x$ is an odd function of x, and since -1 is not a square in $\mathbb{F}_q$, it follows that only one of the two elements $f(x)$ and $f(-x)$ can be a square in $\mathbb{F}_q$. Also, exactly one of them will be a square in $\mathbb{F}_q$ because the group of squares in $\mathbb{F}_q^*$ form a subgroup of index 2. Therefore we only one from the pair $\{x, -x\}$ form a square. Whichover of them forms a square we obtain two points in the elliptic curve $(x, \pm\sqrt{f(x)})$ or else $(-x, \pm\sqrt{f(-x)})$. These give $q - 3$ points. We had 4 points of order 2. So we all in total $q + 1$ points in $\mathbb{F}_q$.

We state the **Mordel Weil Theorem** and **Dirichlets theorem on primes in arithmetic progression.**

Theorem 6 ***(Mordell Weil Theorem)*** *The group $E(\mathbb{Q})$ of $\mathbb{Q}$-points of an elliptic curve defined over $\mathbb{Q}$ is finitely generated abelian group.*

Theorem 7 ***(Dirichlets theorem on primes in an arithmetic progression)*** *For any two positive coprime integers a and d, there are infinitely many primes of the form $a + nd$, where $n \in \mathbb{N}$. In other words, there are infinitely many primes which are congruent to a modulo d.*

Using the above two theorems we prove the following theorem.

Theorem 8

$$|E_n(\mathbb{Q})_{Tor}| = 4$$

Before proving this theorem, consider the elliptic curves modulo a prime. If E is an elliptic curve over $\mathbb{Q}$ and if p does not divide $2n$, we can view the same elliptic curve over $\mathbb{F}_p$. So given a point $P = (x, y, z)$ in $E(\mathbb{Q})$, we can reduce the point modulo $\overline{P} = (\overline{x}, \overline{y}, overlinez)$ to get a point $E(\mathbb{F}_p)$.

Lemma 9 *Given two points $P_1 = (x_1, y_1, z_1)$ and $P_2 = (x_2, y_2, z_2)$ on the elliptic curve $E_n(\mathbb{Q})$. $\overline{P_1} = \overline{P_2}$ if and only if p divides $y_1z_2 - y_2z_1$, $x_2z_1 - x_1z_2$ and $x_1y_2 - x_2y_1$.*

First assume p divides $y_1z_2 - y_2z_1$, $x_2z_1 - x_1z_2$ and $x_1y_2 - x_2y_1$. Consider the two cases

1. p divides x_1. Then p divides x_2z_1 and x_2y_1 and therefore divides x_2 because it cannot divide x_1, y_1 and z_1. Suppose that $p \nmid y_1$ (an analogous argument will apply if $p \nmid z_1$). Then $\overline{P_2} = (0, \overline{y_1y_2}, \overline{y_1z_2}) = (0, \overline{y_1y_2}, \overline{y_2z_1}) = \overline{P_1}$.

2. p does not divide x_1. Then $P_2 = (\overline{x_1x_2}, \overline{x_1y_2}, \overline{x_1z_2}) = (\overline{x_1x_2}, \overline{x_2y_1}, \overline{x_2z_1}) = \overline{P_1}$.

Conversely, suppose that $\overline{P_1} = \overline{P_2}$. Without loss of generality, suppose that $p \nmid x_1$. Then since $\overline{P_1} = \overline{P_2}$, we have that $p \nmid \overline{x_2}$. Hence $(\overline{x_1x_2}, \overline{x_1y_2}, \overline{x_1z_2}) = \overline{P_1} = \overline{P_2} = (\overline{x_2x_1}, \overline{x_2y_1}, \overline{x_2z_1})$. Since the two are the same, these two points are equal if and only if the two second and third coordinates are equal, i.e. if p divides $x_1y_2 - x_2y_1$ and $x_1z_2 - x_2z_1$. Finally we must show that p divides $y_1z_2 - y_2z_1$. If both y_1 and z_1 are divisible by p then this is trivial. Otherwise repeat the same argument replacing x_1.

Let us suppose that there are more than 4 torsion points. Then torsion subgroup contains either an element of odd order or 8 or 16 elements. In either case, there exists a subgroup $S = \{P_1, P_2, \ldots, P_m\} \subset E_n(\mathbb{Q})_{tors}$, where $m = \#S$ is either 8 or else an odd number.
Let us write each point in S as $P_i = (x_i, y_i, z_i)$. For each pair of points P_i, P_j, consider the "cross-product" vector $(y_iz_j - y_jz_i, x_jz_i - x_iz_j, x_iy_j - x_jy_i)$. Let n_{ij} be the greatest common divisor of the coordinates of this cross product. According to the lemma, the points P_i and P_j have the same image in $E_n(\mathbb{F}_p)$ if and only if p divides n_{ij}. Thus if p is a prime of good reduction and greater than all of the n_{ij}, then it follows that all images are distinct and that the map from $E_n(\mathbb{Q})$ to $E_n(\mathbb{F}_p)$ gives an injection of S into $E_n(\mathbb{F}_p)$.

But now for all but finitely many p (which are less than the maximum of the n_{ij}'s) the number m must divide $\#E_n(\mathbb{F}_p)$. Then for all but finitely many primes congruent to 3 modulo 4,we have $p \equiv -1$ modulo m. This contradicts Dirichlet's theorem on primes in an arithmetic progression. If $m = 8$, this means thata there are only finitely many primes of the form $8k + 3$. If $3 \nmid m$, then there are only finitely many primes of the form $4mk + 3$ and if 3 divides m, there are only finitely many primes of the form $12k + 7$. This concludes the proof of theorem 8.

This proves the following.

Theorem 10 *n is a congruent number if and only if $E_n(\mathbb{Q})$ is an elliptic curve of non-zero rank r.*

Now we state the Tunnell's theorem that assumes a weak form of BSD. Making this assumption, Tunnell's theorem provides us an algorithm to determine whether a given number is congruent or not.

Theorem 11 ***Weak form of BSD***
$L(E, 1) \neq 0$ if and only if the Mordel-Weil group $E(\mathbb{Q})$ is finite.

Theorem 12 ***Tunnell's theorem*** *Let n be an odd squarefree natural number. Consider the conditions*

- *n is congruent.*
- *the number of triples of integers (x, y, z) satisfying $2x^2 + y^2 + 8z^2 = n$ is equal to twice the number of triples satisfying $2x^2 + y^2 + 32z^2 = n$.*

If we assume "A Weak form of Birch-Swinnerton-Dyer" conjecture, then the two statements are equivalent.

Chapter 4

Elliptic Curves using Weistrass Functions

We define the Weistrass function $\wp(z)$ for a lattice L as follows:

$$\wp(z; L) = \frac{1}{z^2} + \sum_{l \in L, l \neq 0} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right)$$

The Weistrass function is a meromorphic function on the complex plane. It is doubly periodic and hence can be considered as a meromorphic function on $\mathbb{C}/L$. Also $\wp(z)$ is an even function and has a pole of order 2 at the lattice points. Since $\wp(z)$ is even, its derivative $\wp'(z)$ is an odd function. Here are some basic results (stated without proof, which can be proved using complex analysis) about lattice functions and in general $\wp(z)$.

- Lattice functions have to be meromorphic (if they are not constant). Let f be a lattice function. It turns out that if $\{m_i\}$ denotes the order of various zeroes of f and if $\{n_j\}$ denotes the order of various poles of f, then $\sum m_i = \sum n_j$.
- By considering the function $\wp(z) - u$ where $u \in \mathbb{C}$ we deduce that $\wp(z)$ takes on every possible value.
- $\wp(z)$ generates all the even functions on the lattice. Hence there is a polynomial equation in $\wp(z)$ that equals $\wp^{'}(z)^2$.
- If $f(z)$ is an elliptic function for a lattice L, then so are the two even functions $\frac{f(z)+f(-z)}{2}$ and $\frac{f(z)-f(-z)}{2\wp'(z)}$. This means that there exists rational functions $g(X)$ and $h(X)$ such that $f(z) = g(\wp(z)) + \wp'(z)h(\wp(z))$.
- Make the following definition for constants G_k. $G_k(L) =: \sum_{l \in L, l \neq 0} l^{-k}$
- Then $(\wp(z), \wp'(z))$ satisfy the following equation $y^2 = 4x^3 - 60G_4x - 140G_6$, where $y = \wp^{'}(z)$ and $x = \wp(z)$.
- There is a complex analytic map from $\mathbb{C}/L$ to the "projectization" of the elliptic curve $y^2 = 4x^3 - 60G_4x - 140G_6$ as follows.

  If $z \neq 0$

  $$z \longrightarrow (\wp(z), \wp^{'}(z), 1)$$

  $$0 \longrightarrow (0, 1, 0)$$

Chapter 5

Zeta-function on E_n

Determing the rank of an elliptic curve can be quite difficult. We look for progress by studying the zeta functions on the Elliptic curves.
Given a sequence N_r ,$r = 1, 2, 3, \ldots$, we define the corresponding “Zeta-function by ”

$$Z(T) =: exp\left(\sum_{r=1}^{\infty} N_r \frac{T^r}{r}\right)$$

For an elliptic curve E over $\mathbb{F}_q$, we can define $N_r =$ no. of points on E in $\mathbb{F}_{q^r}$
It turns out that the congruence-zeta function of any elliptic curve E defined over $\mathbb{F}_q$ has the form

$$Z(E/\mathbb{F}_q; T) = \frac{1 - 2a_E + qT^2}{(1-T)(1-qT)}$$

Now taking the logarithmic derivative on both sides, and comparing coefficients, we get

$$N_r = q^r + 1 - \alpha^r - (\frac{q}{\alpha}^r)$$

here α and $\frac{q}{\alpha}$ are roots of $1 - 2a_E + qT^2$.

α turns out to be an algebraic integer and can be given in terms of Gauss and Jacobi sums (which are defined later).

5.0.1 Gauss and Jacobi sums

Here, we simply state the definition of Gauss and Jacobi sums and some basic relations between them.
Let $\psi : \mathbb{F}_q \to \mathbb{C}^*$ be a nontrivial additive character (a nontrivial homomorphism from the additive group of finite field to the multiplicative group of complex numbers) defined by $\psi(x) = \zeta^{Tr(x)}$ where $\zeta = e^{\frac{2\pi i}{p}}$ and Tr is the trace from $\mathbb{F}_q$ to $\mathbb{F}_p$. Since the trace is a nontrivial additive map and its image is in $\mathbb{Z}/p\mathbb{Z}$, we get a proper non trivial additive character.
Now let $\chi : \mathbb{F}_q \to \mathbb{C}^*$ be any multiplicative character (a group homomorphism from the multiplicative group of the finite field to the multiplicative group of complex numbers). The trivial character is defined to be that character that sends every element to 1. We define $\chi(0) = 0$ for every character on the multiplicative group of the finite field. We define the Gauss sum (depending on the variable χ) as follows

$$g(\chi) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(x).$$

We define the Jacobi sum (depending on two variable multiplicative characters) by the formula

$$J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_q} \chi_1(x)\chi_2(1-x).$$

We denote the trivial character as χ_{triv}. χ_2 denotes the character that sends generator of the multiplicative group of finite field to -1. If $q \equiv 1$ modulo 4, then we call χ_4 the character defined on $\mathbb{F}_q^*$ that sends the generator of this multiplicative group to i. Here are some basic relations (χ, χ_1, χ_2 denote non trivial characters and $\overline{\chi}$ denotes the complex conjugate or the inverse character of χ.)

1. $g(\chi_{triv}) = 1$; $J(\chi_{triv}, \chi_{triv}) = q - 2$; $J(\chi_{triv}, \chi) = -1$;
   $J(\chi_1, \chi_2) = J(\chi_2, \chi_1)$; $J(\chi, \overline{\chi}) = -\chi(-1)$;
2. $g(\chi).g(\overline{\chi}) = \chi(-1)q$; $|g(\chi)| = \sqrt{q}$
3. $J(\chi_1, \chi_2) = g(\chi_1)g(\chi_2)/g(\chi_1\chi_2)$ if $\chi_2 \neq \overline{\chi_1}$.

Chapter 6

Bibliography

1. Introduction to Elliptic Curves and Modular forms by Neal Koblitz - I largely read chapter 1 of this book and I have written up stuff almost entirely from this book.

2. http://www.mathpages.com/home/kmath288.htm - This is where I got the proof of Fermat's Infinite descent.