42553 is a congruent number

Susumu Komoto(Tohoku Bunka Gakuen University)
Toru Watanabe, Hideo Wada(Sophia University)

Abstruct

A congruent number is a positive, square-free integer if it is the area of a right triangle with rational number sides. Equivalently, n is a congruent number if the elliptic curve $y^2 = x^3 - n^2x$ has a point of infinite order, which is known to come from a non-trivial solution to one of a finite number of biquadratic Diophantine equations. All congruent number less than 71,473 are known. We also show how the Diophantine equation $877X^4 - 4Y^4 = Z^2$ can be solved without the use of Gaussian integers.

1 Introduction

At first we must tell what a congruent number is. A positive integer n is called a congruent number if it is the area of some right triangle with rational sides.

The congruent property depends only on its square-free factor. The triangle with the side lengths 6, 8, 10 is twice size triangle of the triangle with the side lengths 3, 4, 5. There exists a triangle with area 6, then there exists a triangle with area 24 as well. Then we shall always assume that the number is a square free positive integer.

Another property: n is congruent if and only if the elliptic curve $y^2 = x^3 - n^2x$ has non-trivial rational points. Where trivial points mean (0,0),($-n$,0) and (n,0). When n=6, point (25/4, 35/8) is lying on the curve.

History: In 1993 K. Noda and H. Wada determined all congruent numbers less than 10,000. In 1998 F. Nemenzo determined all congruent numbers less than 42,553. 42553 was the smallest number which had not been determined whether congruent or not.

In 1984 Bremner and Cassels found $y^2 = x^3 + 877x$ has a large generator point. (Congruent number case, the part 877 is minus and square.) And this was found using the arithmetic of $\mathbf{Z}[i]$.

Our results: We found a rational point on E: $y^2 = x^3 - 42,553^2x$. Therefore 42,553 is a congruent number! That point comes from a solution to the equation $7^2X^4 - Y^4 = 6079Z^2$.

We have determined all congruent numbers less than 71,473. 71,473 is the smallest number which has not been determined whether congruent or not. Except for 3 numbers(71473, 90697, 98242), numbers less than 100,000 have been determined whether congruent or not.

Furthermore, we found a point of elliptic curve $y^2 = x^3 + 877x$ without the use of Gaussian integers. The solution comes from the equation $877X^4 - 4Y^4 = Z^2$. For several times variable transformation, we found a solution.

We found the points of elliptic curves $y^2 = x^3 + px$ for all prime p less than 2000 with p is congruent to 5 modulo 8. Especially, 1877 was so hard that Bremner and Cassels seemed to not be able to found it.

Background: The rational points on the elliptic curve over $\mathbf{Q}$ form a finitely generated abelian group(Mordell-Weil Theorem). Namely, E($\mathbf{Q}$) is the group of rational points of E. E($\mathbf{Q}$) is isomorphic to torsion part and $\mathbf{Z}^r$. And torsion part corresponds to trivial points. r is called the rank of E. n is congruent if and only if r is positive.

2 The case $n = 42553$

We shall show that 42553 is a congruent number, namely how to solve the next diophantine equation:

$$7^2 \cdot X^4 - Y^4 = 6079 \cdot Z^2$$

such that $(X, 6079YZ) = 1$, $(Y, 6079 \cdot 7XZ) = 1$. We have

$$(7X^2 + Y^2)(7X^2 - Y^2) = 6079Z^2.$$

We assume X=odd, Y=odd. As $(X, Y) = 1$, we have $(7X^2+Y^2, 7X^2-Y^2) = 2$. Therefore we have

$$7X^2 + Y^2 = 8b^2,$$

$$7X^2 - Y^2 = 2 \cdot 6079a^2,$$

$$4ab = Z,\ (a, b) = 1,\ a = \text{odd}.$$

So we have

$$\begin{aligned} 7X^2 &= 4b^2 + 6079a^2, & (1) \\ Y^2 &= 4b^2 - 6079a^2. & (2) \end{aligned}$$

From (2), we have

$$6079a^2 = (2b + Y)(2b - Y).$$

We may assume $b > 0$. As a=odd, we have $(2b + Y,\ 2b - Y) = 1$. So we have

$$2b + Y = 6079c^2,$$

$$2b - Y = d^2,$$

$$(c, d) = 1,\ cd = a.$$

(If nesessary we change the sign of Y.) So we have

$$4b = 6079c^2 + d^2 \equiv 0 \pmod 8,$$

$$2Y = 6079c^2 - d^2.$$

We have b=even. From (1), we have

$$4 \cdot 7X^2 = 6079^2c^4 + 6 \cdot 6079c^2d^2 + d^4.$$

Put $e = c^2$, $f = d^2$. Then we have

$$4 \cdot 7X^2 = 6079^2e^2 + 6 \cdot 6079ef + f^2.$$

Using a computer we found a solution $e = 1$, $f = 1737$, $X = 1921$. Put

$$\begin{pmatrix} e \\ f \\ X \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1737 & 1 & 0 \\ 1921 & 0 & 1 \end{pmatrix} \begin{pmatrix} g \\ h \\ i \end{pmatrix}.$$

If $g = 1$, $h = 0$, $i = 0$ then $e = 1$, $f = 1737$, $X = 1921$. So the coefficient of g^2 is 0. Indeed we have

$$0 = 4 \cdot 9987gh - 8 \cdot 7 \cdot 1921gi + h^2 - 28i^2.$$

h must be even. Put $h = 2j$ and divided by 4, we get

$$0 = 2g(9987j - 13447i) + j^2 - 7i^2.$$

Put

$$\begin{pmatrix} k \\ \ell \end{pmatrix} = \begin{pmatrix} 9987 & -13447 \\ -3761 & 5064 \end{pmatrix} \begin{pmatrix} j \\ i \end{pmatrix}.$$

From $9987 \cdot 5064 - 3761 \cdot 13447 = 1$, we have

$$\begin{pmatrix} j \\ i \end{pmatrix} = \begin{pmatrix} 5064 & 13447 \\ 3761 & 9987 \end{pmatrix} \begin{pmatrix} k \\ \ell \end{pmatrix},$$

$$k(2g - 73371751k - 389664282\ell) = 2 \cdot 7 \cdot 6079^2\ell^2.$$

k must be even. So ℓ must be even. Put $k = 2m$, $\ell = 2n$. Divided by 4 we have

$$m(g - 73371751m - 389664282n) = 2 \cdot 7 \cdot 6079^2n^2.$$

Put $r = g - 73371751m - 389664282n$. Then we have

$$\begin{pmatrix} g \\ j \\ i \end{pmatrix} = \begin{pmatrix} 1 & 73371751 & 389664282 \\ 0 & 5064 \cdot 2 & 13447 \cdot 2 \\ 0 & 3761 \cdot 2 & 9987 \cdot 2 \end{pmatrix} \begin{pmatrix} r \\ m \\ n \end{pmatrix},$$

$$mr = 2 \cdot 7 \cdot 6079^2n^2.$$

If a prime $p \neq 6079$ divides m, r, then

$$p|m, r \Rightarrow p|n \Rightarrow p|g, j, i \Rightarrow p|g, h, i \Rightarrow p|e, f \Rightarrow p|c, d.$$

So we have $(m, r) = 1$ or 6079. We assume that

$$m = 2 \cdot 7 \cdot 6079^2s^2, \quad r = t^2, \quad n = st.$$

Then we have

$$\begin{aligned} c^2 &= (t + 194832141s)^2 - 7s^2, && (3) \\ d^2 &= f = 1737g + 2j. && (4) \end{aligned}$$

Put $v = t + 194832141s$. Then from (3) we have

$$7s^2 = (v + c)(v - c).$$

We have $(v, c) = 1$, because

$$p|v, c \Rightarrow p|s, t \Rightarrow p|g, j, i.$$

We assume $v =$odd. Moreover we assume

$$v + c = 7 \cdot 8y^2, \quad v - c = 2x^2, \quad s = 4yx.$$

Then we have

$$v = 28y^2 + x^2,$$

$$c = 28y^2 - x^2,$$

$$d^2 = 1737v^2 + 267477s^2 + 4 \cdot 13447vs.$$

Using a computer we found a solution $x = 14609, \quad y = -4338$. From this we have

$$\begin{aligned} d &= 89697426147, \\ c &= 313487951, \\ X &= -1831552406584343522639, \\ Y &= -3724108191962548382965. \end{aligned}$$

Divided by $(X, Y) = 7^2 \cdot 6079^2$, we have a solition:

$$\begin{aligned} X &= 1011483919871, \\ Y &= 2056657258885, \\ Z &= 741219148677604544116 56. \end{aligned}$$

3 The case $p = 877$

Let p be a prime number with $p \equiv 5 \pmod 8$. In this section, we look for solutions of the diophantine equation

$$Z^2 = pX^4 - 4Y^4 \qquad (5)$$

such that $\gcd(X,\ 2YZ) = \gcd(Y,\ pXZ) = 1$. Since $\gcd(X,\ Y) = 1$, then we notice that $X \equiv Y \equiv 1 \pmod 2$.

First we put

$$e = \pm X^2,\ f = \pm Y^2, \qquad (6)$$

then we obtain the equation

$$Z^2 = pX^4 - 4Y^4 = p(\pm X^2)^2 - 4(\pm Y^2)^2 = pE^2 - 4F^2. \tag{7}$$

Since $p \equiv 5 \pmod 8$， there are integers a, b such that $p = 4a^2 + b^2$. Therefore we have a solution (7):$(E, F, Z) = (1, a, b)$. Next, we put

$$\begin{pmatrix} E \\ F \\ Z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & 0 & 1 \end{pmatrix} \begin{pmatrix} G \\ H \\ I \end{pmatrix}, \quad \begin{pmatrix} G \\ H \\ I \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -a & 1 & 0 \\ -b & 0 & 1 \end{pmatrix} \begin{pmatrix} E \\ F \\ Z \end{pmatrix}. \tag{8}$$

Substituting in (7), we get

$$0 = 4F^2 + Z^2 - pE^2 = 4(aG + H)^2 + (bG + I)^2 - pG^2 = 8aGH + 2bGI + 4H^2 + I^2. \tag{9}$$

Moreover we put $I = 2J$, we obtain

$$0 = 8aGH + 2bGI + 4H^2 + I^2 = 4\{G(2aH + bJ) + H^2 + J^2\}. \tag{10}$$

Since $\gcd(2a, b) = 1$， there are integers c, d such that $2ad - bc = 1$. we put

$$\begin{pmatrix} K \\ L \end{pmatrix} = \begin{pmatrix} 2a & b \\ c & d \end{pmatrix} \begin{pmatrix} H \\ J \end{pmatrix}, \quad \begin{pmatrix} H \\ J \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & 2a \end{pmatrix} \begin{pmatrix} K \\ L \end{pmatrix}. \tag{11}$$

Substituting in (10), we get

$$k\{G + (c^2 + d^2)K - 2(2ac + bd)l\} = -pL^2. \tag{12}$$

Moreover we put $R = G + (c^2 + d^2)K - 2(2ac + bd)L$, we obtain

$$KR = -pL^2. \tag{13}$$

Since $KR = -pL^2$, if $q \mid K, R$ for prime number $q \neq p$ then

$$q \mid L \ \Rightarrow q \mid G,\ H,\ J \ \Rightarrow q \mid G,\ H,\ I \ \Rightarrow q \mid E,\ F.$$

Therefore $\gcd(K,\ R) = 1$. Hence we have a parametrization of $(K,\ R,\ L)$:

$$\left\{ \begin{array}{lcl} K & = & \alpha S^2, \\ R & = & \beta T^2, \\ L & = & ST, \end{array} \right. \tag{14}$$

where $\alpha\beta = -p$ and $\gcd(S,\ T) = 1$. Then we have a parametrization of $(G,\ H,\ J)$:

$$\left\{ \begin{array}{lccccr} G = & \beta T^2 & - & (c^2 + d^2)\alpha S^2 & + & 2(2ac + bd)ST, \\ H = & & & d\alpha S^2 & - & bST, \\ J = & & & -c\alpha S^2 & + & 2aST. \end{array} \right. \tag{15}$$

From $\pm X^2 = G$, then we obtain

$$\begin{aligned}
\pm X^2 &= \frac{1}{\beta}\{\beta^2T^2 + 2(2ac+bd)ST - (c^2+d^2)\alpha\beta S^2\} \\
&= \frac{1}{\beta}\{(\beta T + (2ac+bd)S)^2 + (p(c^2+d^2) - (2ac+bd)^2)S^2\} \\
&= \frac{1}{\beta}\{(\beta T + (2ac+bd)S)^2 + S^2\}.
\end{aligned}$$

Moreover we put $U = \beta T + (2ac+bd)S$. From $\pm Y^2 = aG + H$ and $Z = bG + 2J$, we have a parametrization of $(X^2,\ Y^2,\ Z)$:

$$\left\{\begin{array}{rcrcrcr}
\beta X^2 &=& U^2 & & &+& S^2, \\
\pm\beta Y^2 &=& aU^2 &-& bSU &-& aS^2, \\
\beta Z &=& bU^2 &+& 4aSU &-& bS^2,
\end{array}\right. \tag{16}$$

where $\beta = 1$ or p.

Case 1 : We have a parametrization of $(X^2,\ Y^2)$:

$$\left\{\begin{array}{rcrcrcr}
X^2 &=& U^2 & & &+& S^2, \\
Y^2 &=& aU^2 &-& bSU &-& aS^2.
\end{array}\right.$$

From $X^2 = U^2 + S^2$, We have a parametrization of $(X,\ U,\ S)$:

$$X = (V^2+W^2), \quad (\pm U,\ \pm S) = (V^2-W^2,\ 2VW) \text{ or } (2VW,\ V^2-W^2), \tag{17}$$

where V is even number and W is odd number. Finally, we look for integers V and W such that

$$aU^2 - bSU - aS^2 = \text{square}. \tag{18}$$

If found the integers V and W, we get a solution of the diophantine equation $Z^2 = pX^4 - 4Y^4$.

Example

Let $p = 877$. We look for integers V and W such that the condition (18). The search shows that $V = 67506, W = 7423$ satisfy this condition. Hence we have obtained the solution,

$$X = 4612160965, Y = 8547136197, Z = 612776083187947368101.$$

Let $p = 1877$. The search shows that $V = 1210136, W = 676253$ satisfy this condition. Hence we have obtained the solution,

$$X = 1921747258505, Y = 8901377587109, Z = 2209332229729787426157319 1.$$

4 New result

Kazuo Matsuno tought us that 71,473 is a congruent number. He used Symbolic Algebra "MAGMA" which includes a program based on "4-descent method". He used a computer about one month and he found all congruent numbers less than 300,000.