Vietnam Journal of Mathematics **33:** *SI* (2005) 93–96

Vietnam Journal
of
MATHEMATICS

The Congruent Number Problem and Its Generalizations

V. Nguyen-Khac

Institute of Mathematics, 18 Hoang Quoc Viet Road, 10307 Hanoi, Vietnam

Abstract. We briefly review the classical congruent number problem and its variations by previous authors. The aim of the note is to propose our function field analogue of the problem which turned out to be closely related to the function field variant of the Birch-Swinnerton-Dyer conjecture a` la Tate.

1. A natural number n is called a *congruent* number, if it equals to the area of a right triangle with rational lengths of its sides. As an example we have $6 = S_{\triangle(3,4,5)}$ (*famous Pythagoras' triangle*), or a bit more complicated example $5 = S_{\triangle\left(20/3,3/2,41/6\right)}$. An old problem since the ancient Greek mathematics time, nowadays known as *the congruent number problem*, was to determine all the congruent numbers. In other words, how can we find an algorithm to decide whether a given natural number n is congruent. The problem turned out to be very delicated, because it has a deep connection with the so called *conjecture of Birch & Swinnerton-Dyer* (*abbr. BSD* conjecture) - one of the seven famous problems for XXI century recently announced by the Clay Mathematics Institute with 1 million *USD* prize for each (certainly with a correct solution). Presumably it was first proved by P. de Fermat (~ 1650) that if n is an exact square then there are no such right triangles, *i.e.* it is not a congruent number.

More precisely the stuff is going as follows. Assume $n = S_{\triangle(a,b,c)}$ with $a^2 + b^2 = c^2$. Then we have a natural parametrization:

$$a = \frac{1-t^2}{1+t^2}\ c,\ b = \frac{2t}{1+t^2}\ c.$$

So $n = \alpha^2\ t(1-t^2)$, where $\alpha = \dfrac{c}{1+t^2}$. Thus putting $x := -nt,\quad y := \dfrac{n^2}{\alpha}$ we come to the following elliptic curve (affine form)

$$E_n\colon\ \ y^2 = x^3 - n^2\ x.$$

Thus if n is a congruent number then E_n has a rational point (x, y) with $y \neq 0$. By a theorem of Nagell and Lutz (1937) one can see that the only torsion points of E_n are points (x, y) with $y = 0$, or n is a congruent number if and only if the elliptic curve E_n has a $\mathbb{Q}$-rational point of infinite order. It is equivalent to saying that the Mordell-Weil rank r of $E_n(\mathbb{Q})$ is greater than 0. As a corollary we deduce that if n is a congruent number then there are infinitely many rational right triangles with area $= n$.

2. For an elliptic curve E defined over $\mathbb{Q}$ one of the basic problems is to determine $E(\mathbb{Q})$. The known Fermat method-chord-tangent process gives us the addition law on $E(\mathbb{Q})$. Mordell's theorem (1922) says that $E(\mathbb{Q})$ is a finitely generated abelian group: $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}$. The torsion part was completely determined by Mazur (1977): $E(\mathbb{Q})_{tors}$ is one of the following 15 groups $-\mathbb{Z}/n\mathbb{Z}$: $n = 1 - 10$, or 12; $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$: $m = 1 - 4$.. The free part is quite mysterious in connection with the so-called BSD conjecture mentioned above. For testing how many points are in $E(\mathbb{Q})$ Birch & Swinnerton-Dyer computed the product $\prod\limits_{p<M} \dfrac{N_p}{p}$, where $N_p := {}^{\#}\{(x, y)\colon\ y^2 \equiv x^3 + ax + b \pmod{p}\}$ $+1$ (for the point "∞"). By the well-known Hasse-Weil bound: $|a_p| \leqslant 2\sqrt{p}$, where $a_p := p + 1 - N_p$. Intuitively if $E(\mathbb{Q}) = \infty$, then there must be "infinitely many" p such that N_p is "big", *i.e.* the ratio $\dfrac{p}{N_p}$ is "small". Hence the infinite product of $\dfrac{p}{N_p}$ is "very small". But that product for "good" primes p (*i.e.* such that the reduced curve $E/\mathcal{F}_p$ is not singular) is nothing but the formal value of Hasse's L-function $L(E, s)$ at $s = 1$. More precisely let

$$L(E, s) := \prod_p (1 - a_p\ p^{-s} + p^{1-2s})^{-1}.$$

$L(E, s)$ converges in the half-plane $\mathrm{Re}(s) > 3/2$, and heuristically

$$L(E, s)\ \text{“}=\text{”}\ \prod_p \left(\frac{N_p}{p}\right)^{-1}$$

A famous conjecture of Hasse asserts that $L(E, s)$ has an analytic continuation to the whole $\mathbb{C}$. Fortunately this is true for the congruent number curve E_n (Hecke-Deuring). It is known that the conjecture is a consequence of the so-called modularity conjecture (Shimura-Taniyama-Weil) which implies also Fermat's last theorem. The last conjecture was recently set up by Wiles-Taylor-Breuil-Conrad-Diamond (2000).

The BSD conjecture tells us that the Mordell-Weil rank r is equal to the order of $L(E, s)$ at $s = 1$. Besides it predicts a deep relation between the behaviour of $L(E, s)$ as $s \to 1$ and other invariants of E such as its torsion order, Tamagawa numbers measuring how dense are $\mathbb{Q}$-rational points on E, and especially

the order of the Shafarevich-Tate group Ш. Some particular cases are known: if $^{\#}E(\mathbb{Q}) = \infty$, then $L(E,1) = 0$ (Coates-Wiles, 1977); if $\mathrm{ord}_{s=1}\ L(E,s) = 1$, then $^{\#}E(\mathbb{Q}) = \infty$ (Gross-Zagier, 1984); if $L(E,1) \neq 0$, then $^{\#}E(\mathbb{Q}) < \infty$ (Kolyvagin, 1988). In general we are still far from a complete solution of a 1 million USD prize problem set by the Clay Mathematics Institute.

Concerning our congruent number curve E_n we have the following theorem.

Theorem. [6] $L(E_n,1) = 0$ *iff* $c(n) = 0$, *where* $c(n)$ *is the* n*-th coefficient of the modular form of weight* $3/2$ *for* $\Gamma_0(128)$:

$$\sum_{k=1}^{\infty} c(k)q^k = \{q\prod_{k=1}^{\infty}(1-q^{8k})(1-q^{16k})\}\sum_{k\in\mathbb{Z}} q^{2k^2}$$

Tunnell's criterion. *Assuming the validity of the BSD conjecture, for a square-free natural number* n *let* $d := 1$ *if* n *odd, and* $d := 2$ *if* n *even,* $N_1 := {}^{\#}\{(a,b,c) \in \mathbb{Z}^3\colon\ \dfrac{n}{d} = 2d\ a^2 + b^2 + 8c^2\}$, $N_2 := {}^{\#}\{(a,b,c) \in \mathbb{Z}^3\colon\ \dfrac{n}{d} = 2d\ a^2 + b^2 + 32c^2\}$. *Then* n *is congruent iff* $N_1 = 2\ N_2$.

The criterion can be deduced from the following formula for the formal value $L(E_n,s)_{|s=1}$

$$L(E_n,1) = \frac{d\ (N_1 - 2N_2)}{\sqrt{n}} \times 0.163878597\ldots$$

In particular, according to the results of Coates-Wiles and Gross-Zagier mentioned above, if $N_1 \neq 2\ N_2$ then one can say definitely that n is not a congruent number. The other implication is also true modulo the BSD conjecture as stated in the Tunnell criterion.

3. θ-**variant**: $\theta = 2\pi/3$, or $\pi/3$. A positive square-free n is called θ-congruent iff $n\sqrt{3}$ = the area of a rational triangle with an angle θ. The question leads to elliptic curves $y^2 = x(x+n)(x-3n)$ and $y^2 = x(x-n)(x+3n)$ (M. Yoshida - Chiba, Kaneko).

2-Dimensional Variant [7] Find a cuboid K with sides $X, Y, Z \in \mathbb{Q}$ such that the face diagonals on the XY, YZ-planes $P, Q \in \mathbb{Q}$ and the body (internal) diagonal $W \in \mathbb{Q}$. It is equivalent to finding rational solutions $(X,Y,Z,P,Q,W) \in \mathbb{Q}^6$ to the system of equations $X^2+Y^2 = P^2$, $Y^2+Z^2 = Q^2$, $X^2+Y^2+Z^2 = W^2$.

Theorem. *Non-trivial solutions of the system above* $\overset{1-1}{\longleftrightarrow} S_1(\mathbb{Q})$, *where* S_1 *is a* $K3$*-surface defined by*

$$y^2 = z(z^2+4)x(x^2-1).$$

Now let $E_1\colon w_1 = x(x^2-1)$, $E_2\colon w_2 = z(z^2+4)$ which are isogenous; $\iota\colon \big((x,w_1),(z,w_2)\big) \mapsto \big((-x,w_1),(-z,w_2)\big)$ - involution on $E_1 \times E_2$; $S_2 := E_1 \times E_2/\iota$ - a Kummer surface defined by

$$w^2 = x(x^2-1)z(z^2-1).$$

Theorem. *Let n be a dimension 1 congruent number, $(A,B),(C,D)$ a pair of non-trivial solutions: $B^2 = A^3 - nA,\ D^2 = C^3 - nC$. Then*

$$(A/n, C/n, BD/n^3) \in S_2(\mathbb{Q}),$$

and conversly every non-trivial $\mathbb{Q}$-rational point of $S_2(\mathbb{Q})$ can be obtained in this way.

4. Function Field Variant

For simplicity let $k := \mathcal{F}_q$ be a finite field of characteristic ≥ 5. In the same manner one can define the congruent property for a unitary square-free polynomial $f \in k[t]$. It leads to the congruent elliptic curve $E_f\colon y^2 = x^3 - f^2x$ defined over the function field $K := k(t)$. Let C/k be the hypereeliptic curve with affine model: $u^2 = f(t)$. We remark that E_f is a potentially constant elliptic curve, namely it becomes isomorphic to the constant curve $E_1\colon y^2 = x^3 - x$ after the quadratic extension $K(u) = k(C)$, *i.e.* after the double covering base change $C \to \mathbb{P}^1$. Let P_∞ be a single k-rational point of C at infinity. One can embed C into the Jacobian variety $J(C)$ by taking any point $P \in C$ to the class of the divisor $P - P_\infty$. So the Mordell-Weil group $E_f(K)$ can be identified with $\mathrm{Hom}_k(J(C), E_1)$ via considering k-rational maps $C \to E_1$ sending P_∞ to the origin 0 of E_1. Since Tate's analogue of the BSD conjecture is true in our case [1–4], and in view of [5] we have proved

Theorem. *In the notation above polynomial f is congruent if and only if $J(C)$ contains E_1 among its k-isogenous factors.*

References

1. W. J. Gordon, Linking the conjectures of Artin-Tate and Birch-Swinnerton-Dyer, *Comp. Math.* **38** (1979) 99–163.
2. J. Milne, The Tate-Šafarevič group of a constant abelian variety, *Invent. Math.* **6** (1968) 91–105.
3. J. Milne, On a conjecture of Artin and Tate, *Ann. of Math.* **102** (1975) 517–533.
4. J. Tate, On the conjecture of Birch and Swinnerton-Dyer and a geometric analogue, *Séminaire Bourbaki 1966, exposé* **306** (reprinted in 1995) 415–440.
5. J. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. Math.* **2** (1966) 44–134.
6. J. B. Tunnell, A classical Diophantine problem and modular forms of weight 3/2, *Invent. Math.* **72** (1983) 34–323.
7. N. Yui, Congruent number problems in dimensions one and two, The Clay Mathematics Institute workshop "Algorithmic Number Theory" at MSRI, August 14-23, 2000.