29. *On an Identity of Desboves*

By Jasbir Singh CHAHAL
Mathematical Department, Brigham Young University

(Communicated by Shokichi IYANAGA, M. J. A., March 12, 1984)

§1. **Introduction.** A. Desboves (cf. [2], see also [3], p. 631, line 2) employed the identity

$$(1)\qquad \begin{aligned}&(y^2+2xy-x^2)^4+(2x^3y+x^2y^2)(2x+2y)^4\\&=(x^4+y^4+10x^2y^2+4xy^3+12x^3y)^2\end{aligned}$$

to show, among others, that $x^4+ay^4=z^2$ is solvable in $\boldsymbol{Z}$ if a is of the form $(2x+y)x^2y$ or $2x^2+y^4$. The purpose of this note is to show that this identity can also be used to get a point of infinite order of $E(\boldsymbol{Q})$, the group of rational points on certain elliptic curves E of the form

$$(2)\qquad y^2=x^3+Ax, \qquad A\in\boldsymbol{Q}.$$

Here, without loss of generality, we can assume that A is a non-zero integer, free of fourth powers. In another context it has been widely conjectured (cf. [5] or the table on p. 147 of [4]) that if a positive integer $n\equiv 5, 6, 7$ (mod. 8) then n is a congruent number, i.e., it is the area of a right triangle of all sides rational. We shall rather show that any residue class modulo 8 contains infinitely many congruent numbers.

§2. **The main result.** First we state the following theorem which we shall need in the sequel and which was proved independently by E. Lutz and T. Nagell (cf. [1], p. 264, Theorem 22.1).

Theorem 1. *Suppose $P=(x,y)\in E(\boldsymbol{Q})$ is a point of finite order on the elliptic curve $y^2=x^3+Ax+B$ with $A, B\in\boldsymbol{Z}$. Then x and y are necessarily integers.*

Theorem 2. *For any integer $\lambda\neq 0$, let E_λ be the curve*

$$(3)\qquad y^2=x^3+A_\lambda x,$$

where $A_\lambda=8\lambda(2\lambda-1)^2$. Then $E_\lambda(\boldsymbol{Q})$ has a point of infinite order.

Proof. A solution (s,t,u) with $t\neq 0$ of $s^4+At^4=u^2$ leads to a solution $x=s^2/t^2$ and $y=su/t^3$ of (2). The following identity

$$\begin{aligned}&(1-12\lambda+4\lambda^2)^4+8\lambda(2\lambda-1)^2(2(1+2\lambda))^4\\&=(1+40\lambda-104\lambda^2+160\lambda^3+16\lambda^4)^2,\end{aligned}$$

which follows from (1) by putting $x=1-2\lambda$, $y=4\lambda$ gives a rational point $P=(x,y)$ on (3) with

$$x=x(\lambda)=\frac{(1-12\lambda+4\lambda^2)^2}{4(1+2\lambda)^2},$$

$$y=y(\lambda)=\frac{(1-12\lambda+4\lambda^2)(1+40\lambda-104\lambda^2+160\lambda^3+16\lambda^4)}{8(1+2\lambda)^3}$$

with neither x nor y being an integer. Thus P is a point of infinite order.

Remark. If an integer $A\neq 0$ is not of the form $8\lambda(2\lambda-1)^2$ with $\lambda\in \boldsymbol{Z}$ we may still be able to find a point of infinite order on (2) as follows:

For $A, B\in \boldsymbol{Q}^{\times}$, let us write $A\sim B$ if $A/B\in(\boldsymbol{Q}^{\times})^4$, the group the fourth powers of the elements of $\boldsymbol{Q}^{\times}$. For $A, B\in\boldsymbol{Q}^{\times}$, the curves $y^2=x^3+Ax$ and $y^2=x^3+Bx$ are birationally equivalent over $\boldsymbol{Q}$ if and only if $A\sim B$, say $A=c^4B$. Then (c^2x, c^3y) is a point on the first curve if and only if (x, y) lies on the second curve. For any rational $\lambda=a/b\neq 0$, $1/2$ with $(a, b)=1$, $(x(\lambda), y(\lambda))$ is still a rational point on (3), but it need not be of infinite order. Now $A_\lambda=8ab(2a-b)^2/b^4\sim 8ab(2a-b)^2$. Thus if b is odd, then $(b^2x(\lambda), b^3y(\lambda))$ is a point of infinite order of (2) with $A=8ab(2a-b)^2$. Furthermore, if $8ab(2a-b)^2$ has a factor d^4 with d integer, then $(b^2x(\lambda)/d^2, b^3y(\lambda)/d^3)$ is again a point of infinite order on (2) with $A=8ab(2a-b)^2/d^4$. In this way we get a point of infinite order on (2), for example, with $A=3, 14, 33, 60, 95$:

a	2	4	6	8	10
b	3	7	11	15	19
$A_\lambda\sim$	3	14	33	60	95

This leads to the following question: let Φ be the composite map

$$\boldsymbol{Q}^{\times}-\{1/2\}\xrightarrow{A_\lambda}\boldsymbol{Q}^{\times}\xrightarrow{\pi}\boldsymbol{Q}^{\times}/(\boldsymbol{Q}^{\times})^4.$$

Put

$$D=\{a/b\in\boldsymbol{Q}^{\times}\mid (a, b)=1,\ b \text{ odd}\}$$

$$D^*=\{m\in\boldsymbol{Z}\mid m\neq 0 \text{ and } m \text{ free of } 4^{th} \text{ powers}\}.$$

What numbers in D^* are represented by $\Phi_{|D}$? Apart from the fact that there are infinitely many numbers in D^* represented by $\Phi_{|D}$ (cf. Appendix), this seems to be an open question.

§3. Application. The following result on congruent numbers is a consequence of Theorem 2.

Theorem 3. *If $n=m(4m^2+1)$ for a positive integer m, then n is a congruent number.*

Proof. It is well-known (cf. [6]) that n is a congruent number if and only if

$$y^2=x^3-n^2x \tag{4}$$

has a point of infinite order. In Theorem 2, let $\lambda=-2m^2$. Then $(x(\lambda)/4, y(\lambda)/8)$ is a point of infinite order on (4) with $n=m(4m^2+1)$.

Corollary 4. *For any integer r $(0\leq r<8)$, there are infinitely many integers n, such that*

(i) $n \equiv r \pmod{8}$ *and*

(ii) n *is a congruent number.*

Proof. If $n=m(4m^2+1)$, then n is a congruent number. Write $m=2s+t$ with $t=0$ or 1, according as m is even or odd. Then

$$\begin{aligned} n &= (2s+t)(4(2s+t)^2+1) \\ &\equiv 4t^3+2s+t \pmod{8}. \end{aligned}$$

Now given r, one can choose $t=0$ or 1 and infinitely many s, such that

$$4t^3+2s+t \equiv r \pmod{8}.$$

Appendix

Theorem. *There are infinitely many integers* λ, *such that*

(i) λ *is free of fourth powers and*

(ii) $2\lambda-1$ *is square-free.*

Proof. Put $\lambda_1=2$. So $2\lambda_1-1=3$. Suppose λ_{i-1} has been chosen for $i \geq 2$. For positive integers i and n, let $N_m^i(n)$ denote the number of integer multiples of m^i which lie in the open interval $(n, 2n)$. Then

$$N_m^i(n) \leq \begin{cases} (n/m^i)+1, & \text{if } 2 \leq m^i < n \\ 1, & \text{if } n \leq m^i < 2n. \\ 0, & \text{if } 2n \leq m^i \end{cases}$$

The number of integers in the interval $(n, 2n)$ which are multiple of a fourth power is less than

$$\textstyle\sum_{m=2}^{n1/4} (n/m^4)+n^{1/4}+((2n)^{1/4}-n^{1/4}).$$

Using the fact that

$$\textstyle\sum_{m=2}^{\infty} (1/m^4)=(\pi^4/90)-1,$$

it follows that the number $f(n)$ of odd integers λ in the interval $(n, 2n)$ which are free of fourth power is larger than

$$\frac{n}{2}-\left(\left(\frac{\pi^4}{90}-1\right)n+(2n)^{1/4}\right)>\frac{40}{100}n-(2n)^{1/4}.$$

Similarly, the number $g(n)$ of odd integers in the interval $(2n, 4n)$ which contain a square is less than

$$\begin{aligned} &2n\left(\frac{1}{3^2}+\frac{1}{5^2}+\frac{1}{7^2}+\sum_{m=11}^{\infty}\frac{1}{m^2}+(2n)^{1/2}\right)+(2n^{1/2}-(2n)^{1/2}) \\ &<2n\left(\frac{1}{3^2}+\frac{1}{5^2}+\frac{1}{7^2}+\int_{10}^{\infty}\frac{1}{x^2}\,dx\right)+2n^{1/2} \\ &<\frac{35}{100}n+2n^{1/2}. \end{aligned}$$

Now for sufficiently large $n>\lambda_{i-1}$, we have $f(n)>g(n)$, because

$$\frac{40}{100}n-(2n)^{1/4}>\frac{35}{100}n+2n^{1/2}.$$

For the above mentioned $f(n)$ integers λ, the integers $2\lambda-1$ are all odd and among these integers $2\lambda-1$, at the most $g(n)$ can have a square factor. So there is at least one λ_i with the required properties.

Remark. In view of Theorem 2, the above theorem shows that there are infinitely many non-isomorphic elliptic curves over $\boldsymbol{Q}$ of positive rank.

References

[1] J. W. S. Cassels: Diophantine equations with special reference to elliptic curves. J. London Math. Soc., **41**, 193–291 (1966).

[2] A. Desboves: Sur l'emploi des identités algébriques dans la résolution, en nombres entiers, des équations d'un degré supérieur au second. Comptes Rendus, Paris, **87**, 159–161 (1878).

[3] L. E. Dickson: History of the Theory of Numbers. vol. II, Chelsea, New York (1971).

[4] T. Ono: Variations on a theme of Euler. Jikkyō, Tokyo (1980) (in Japanese).

[5] N. M. Stephens: Congruent properties of congruent numbers. Bull. London Math. Soc., **7**, 182–184 (1975).

[6] J. B. Tunnell: A classical diophantine problem and modular forms of weight 3/2. Invent. math., **72**, 323–334 (1983).