INTEGER POINTS ON ELLIPTIC CURVES-II

R.C. VAUGHAN*

Abstract. The object of this paper is to eliminate the main constraint in the hypothesis of Theorem 1.1 of Vaughan [2014] in the cubic case. We are able to treat the number of integer points on a curve $y^2 = f(x)$ where f is a cubic polynomial with integer coefficients even when the curve is not an elliptic curve.

1. Introduction and Statement of Results

The object of this paper is to eliminate the main constraint in the hypothesis of Theorem 1.1 of Vaughan [2014] in the cubic case. We are able to treat the number of integer points on a curve $y^2 = f(x)$ where f is a cubic polynomial with integer coefficients even when the curve is not an elliptic curve.

Theorem 1.1. *Suppose that $f(x) = Ax^3 + Bx^2 + Cx + D$ is a cubic polynomial with integer coefficients and $A \neq 0$. Suppose further that X_0 and X are real numbers with $X \geq 1$, let $\Delta = (A, 4BD - C^2)$, and let $N_f(X; X_0)$ be the number of integral points (x, y) with $X_0 < x \leq X_0 + X$ and $y^2 = f(x)$. Then*

$$N_f(X, X_0) \ll X^{\frac{1}{2}} \big(\log\log(30\Delta) \big)^{1/2}$$

where the implicit constant is absolute.

For history and background we refer the interested reader to our earlier paper Vaughan [2014].

It is useful to repeat here Theorem 1.2 of Vaughan [2014].

Date: 10th June 2020.

1991 *Mathematics Subject Classification.* 11G05, 11N36.

Key words and phrases. elliptic curve,larger sieve.

*Research supported in part by Simons Foundation Grant OSP1857531.

Corollary 1.2. *Let $n \in \mathbb{N}$. Then the number $R(n)$ of solutions of the Mordell equation*

$$x^3 + y^2 = n$$

in positive integers x, y satisfies

$$R(n) \ll n^{\frac{1}{6}}.$$

In connection with Corollary 1.2 it is perhaps worth observing that if

$$u^3 + v^3 = 2n \tag{1.1}$$

has many solutions is positive integers u and v, so does

$$x^3 + y^2 = n^2 \tag{1.2}$$

in x and y given by assuming $u < v$ and taking

$$x = uv, \quad y = \frac{v^3 - u^3}{2}.$$

What is curious here is it is possible that (1.2) has other solutions, i.e it could have more solutions than (1.1). One such example is $n = 2052$. Then

$$2n = 2^3 + 16^3 = 9^3 + 15^3$$

are the only solutions to this, but

$$n^2 = 32^3 + 2044^2 = 135^3 + 1323^2 = 152^3 + 836^2$$

For an elliptic curve it is expected that stronger bounds are possible, and Siegel'e theorem gives a bound which is independent of X, but depends substantially on the coefficients of f.

The following theorem shows that Theorem 1.1 is best possible and explains why the methods used are unlikely to do substantially better for elliptic curves without a fundamental new idea.

Theorem 1.3. *Let k and l be fixed integers and write the positive integer $A = A_1A_2^2$ where A_2^2 is the largest square dividing A. In the notation of Theorem 1.1 with $f(x) = A(x-k)^2(x-l)$ we have*

$$N_f(X,0) = 2(X/A_1)^{1/2} + O(1).$$

The theorem follows from the observation that $A_1A_2(x-k)|y$ and so, when $y \neq 0$ we have some positive integer t such that $x = A_1t^2 + l$ and $y = \pm A_1A_2t(A_1t^2 + l - k)$.

2. The proof of Theorem 1.1

We begin by following the proof of Theorem 1.1 of Vaughan [2014]. To that end we begin by quoting the version of Gallagher's larger sieve given there.

Lemma 2.1 (Gallagher)**.** *Suppose that $Q \geq 1$ and $X \geq 1$, Q, X and X_0 are real numbers, and $\{c_n\}$ is a sequence of non–negative real numbers with the property that $c_n = 0$ unless $X_0 < n \leq X_0 + X$. Define*

$$Z(q,a) = \sum_{n \equiv a \pmod q} c_n,$$

$Z = Z(1,0)$ and let $\mathcal{A}_q$ be a set of residue classes a such that $Z(q,a) = 0$ when $a \notin \mathcal{A}_q$. Finally let $g(q)$ denote the cardinality of A_q and let $\mathcal{Q} \subset [1,Q] \cap \mathbb{N}$ be such that $g(q) \neq 0$ whenever $q \in \mathcal{Q}$. Then, whenever the denominator on the right is positive, we have

$$Z^2 \leq \frac{\sum_{q\in\mathcal{Q}} \Lambda(q) - \log X}{\sum_{q\in\mathcal{Q}} \frac{\Lambda(q)}{g(q)} - \log X} \sum_n c_n^2.$$

We apply the lemma with $c_m = 0$ unless $X_0 < n \leq X_0 + X$ and $f(n)$ is a perfect square in which case we take $c_n = 1$. We suppose that $p > 6$ and $p \nmid \Delta$. The function $g(p)$ can be taken to be the number of x modulo p such that $f(x)$

is a quadratic residue modulo p or in the 0 residue class. Thus

$$g(p) = \frac{1}{2}g_0(p) + \frac{1}{2}\sum_{x=1}^{p}\left(1 + \left(\frac{f(x)}{p}\right)_L\right)$$

where we now reinterpret the sum as being over the elements of $\mathbb{F}_p$, $g_0(p)$ is the number of elements x with $f(x) = 0$ and we have used

$$\left(\frac{*}{p}\right)_L$$

to denote the multiplicative character of $\mathbb{F}_p$ corresponding to the Legendre symbol.

For the time being suppose that $p \nmid A$. If f is non-singular over the algebraic closure of $\mathbb{F}_p$, then the curve $y^2 = f(x)$ defines an elliptic curve $E_f(p)$ over $\mathbb{F}_p$ and Hasse's theorem [1936] gives

$$\left|\sum_{x=1}^{p}\left(\frac{f(x)}{p}\right)_L\right| = |N_f(p) - p - 1| \le 2\sqrt{p}$$

where $N_f(p)$ is the number of points on $E_f(p)$. Thus

$$\left|g(p) - \frac{p}{2}\right| \le \frac{3}{2} + \sqrt{p} \tag{2.3}$$

and this can be applied as in [2014].

Thus it remains to deal with the situation when f is singular over the algebraic closure $\mathbb{K}$ of $\mathbb{F}_p$. Then there are x_0 and x_1 on $\mathbb{K}$ such that $f(x) = A(x-x_0)^2(x-x_1)$. Moreover

$$9Af(x) - (3Ax + B)f'(x) = (6AC - 2B^2)x + 9AD - BC$$

where we have defined

$$f'(x) = 3Ax^2 + 2Bx + C = 2A(x-x_0)(x-x_1) + A(x-x_0)^2.$$

Thus

$$(6AC - 2B^2)x_0 + 9AD - BC = 0.$$

If $6AC - 2B^2 = 0$ in $\mathbb{F}_p$, then so is $9AD - BC = 0$ and $f(x) = (27A^2)^{-1}(3Ax + B)^3$. Hence

$$\sum_{x=1}^{p} \left(\frac{f(x)}{p}\right)_L = \left(\frac{27A^2}{p}\right)_L \sum_{x=1}^{p} \left(\frac{3Ax+B}{p}\right)_L = 0$$

and (2.3) holds.

Now suppose that $6AC - 2B^2 \neq 0$ in $\mathbb{F}_p$. Thus $x_0 \in \mathbb{F}_p$ and $x_1 = -BA^{-1} - 2x_0$ is also in $\mathbb{F}_p$. Thus

$$\begin{aligned}\sum_{x=1}^{p} \left(\frac{f(x)}{p}\right)_L &= \left(\frac{A}{p}\right)_L \sum_{x=1}^{p} \left(\frac{x-x_0}{p}\right)_L^2 \left(\frac{x-x_1}{p}\right)_L \\ &= -\left(\frac{A}{p}\right)_L \left(\frac{x_0-x_1}{p}\right)_L\end{aligned}$$

and (2.3) holds here also.

Now suppose that $p|A$. Then in $\mathbb{F}_p$, $f(x) = Bx^2+Cx+D$. If $p \nmid B$, then this is $(4B)^{-1}\big((2Bx+C)^2+4BD-C^2\big)$. Since $p|A$ and $p \nmid \Delta$ we have $p \nmid 4BD - C^2$ and thus (2.4) holds once more. If $p|B$, then again since $p \nmid \Delta$ we have $p \nmid C$ and so $f(x) = Cx + D$ and (2.3) follows yet again.

In the notation of Lemma 2.1 we can certainly choose $\mathcal{A}_p$ so that $g(p) = \frac{p}{2} + O(\sqrt{p})$ and $g(p) > 0$ when $p > 7$ and $p \nmid \Delta$ and then

$$\frac{1}{g(p)} = \frac{2}{p} + O(p^{-3/2}). \tag{2.4}$$

We also have $g(p) \leq p$ always, so we can choose $\mathcal{A}_p$ so that $g(p) = p$ when $p \leq 7$ or $p|\Delta$. We now take $\mathcal{Q}$ to be the set of primes p with $p \leq Q$ where Q is a parameter at our disposal. By Theorem 6.9 of Montgomery and Vaughan [2006],

$$\sum_{q\in\mathcal{Q}} \Lambda(q) \leq Q + O\left(\log(3\Delta) + \frac{Q}{\log Q}\right)$$

and by Theorem 2.7 *ibidem*,

$$\sum_{q\in\mathcal{Q}}\frac{\Lambda(q)}{g(q)}\ge\sum_{p\le Q}\frac{2}{p}-\sum_{p|210\Delta}\frac{1}{p}+O(1)$$
$$\ge 2\log Q-\log\log(30\Delta)+O(1).$$

We now choose $Q=CX^{1/2}\big(\log\log(30|A|)\big)^{1/2}$ for a suitable constant C. Then

$$\sum_{q\in\mathcal{Q}}\frac{\Lambda(q)}{g(q)}-\log X\gg 1.$$

With c_n defined as above it follows that

$$N_f(X,X_0)\ll X^{\frac12}\big(\log\log(30\Delta)\big)^{1/2}$$

as required.

References

[1936] Helmut Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper. I, II & III*, J für Reine und Angewandte Mathematik, 1936 (175), 55-62, 69-88, 193-208.

[2014] R. C. Vaughan, *Integer points on elliptic curves*, Rocky Mountain Journal of Mathematics 44(2014), 1–6.

RCV: Department of Mathematics, McAllister Building, Pennsylvania State University, University Park, PA 16802-6401, U.S.A.

Email address: rcv4@psu.edu