ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 44, Number 4, 2014

INTEGER POINTS ON ELLIPTIC CURVES

R.C. VAUGHAN

ABSTRACT. We show that the number of integer points on an elliptic curve $y^2 = f(x)$ with $X_0 < x \le X_0 + X$ is $\ll X^{1/2}$ where the implicit constant depends at most on the degree of $f(x)$. This improves on various bounds of Cohen [**4**], Bombieri and Pila [**1**] and of Pila [**9**], and others. In particular it follows that the number of positive integral solutions to $x^3 + y^2 = n$ is $\ll n^{1/6}$.

1. Introduction and statement of results.

Theorem 1.1. *Suppose that $c \in \mathbf{Z}\backslash\{0\}$ and f is a polynomial of degree d with integer coefficients such that $cy^2 - f(x)$ is absolutely irreducible. Suppose further that X_0 and X are real numbers with $X \ge 1$, and let $N_f(X; X_0)$ be the number of integral points (x, y) with $X_0 < x \le X_0 + X$ and $cy^2 = f(x)$. Then*

$$N_f(X; X_0) \ll X^{1/2}$$

where the implicit constant depends at most on d.

Of course, we should not forget Siegel's theorem [**12**] which tells us that the total number of integral points on the curve is finite. However, Siegel's method gives no local bound. The version of Hilbert's irreducibility theorem given by Fried [**5**] gives a bound similar to the theorem above, but the arbitrary constants therein could depend on f, and in particular on the coefficients of f. The bound of Cohen [**4**] (see Serre [**11**]),

$$N_f(X; X_0) \ll X^{1/2}(\log X)^{\gamma},$$

Research supported by NSA grant number H98230-09-1-0015.

Received by the editors on December 12, 2011, and in revised form on December 18, 2011.

DOI:10.1216/RMJ-2014-44-4-1377

where $0 < \gamma < 1$, has an extraneous logarithmic factor and that of Bombieri and Pila [**1**], and Pila [**9**],

$$N_f(X;X_0) \ll X^{1/2}(\log X)^{2d+3}$$

would only be directly applicable when $\max_{[X_0,X_0+X]} |f(x)| \ll X^d$ with an implicit constant which is independent of f. The bounds of Bombieri and Pila [**1**], and Pila [**9**], are formulated slightly differently. They count the number of lattice points on the curve which also lie in a square of side length N. Thus, the relationship between x and N also depends on $f(x)$ and so can be affected by the intrusion of large coefficients of f. There has been some quite recent work by Helfgott and Venkatash [**7**] in which it is shown, for example, that the total number of integer solutions of the equation

$$y^2 = x^3 - 27\Delta$$

is

$$\ll |\Delta|^{\theta+\varepsilon}, \quad \text{where } \theta = 0.20070\ldots,$$

and, in the slightly more general case of

$$y^2 = x^3 + D,$$

they obtain the bound

$$\ll D^{0.22377\ldots}.$$

There are two further papers which give bounds which, whilst weaker than Theorem 1.1, are of a similar nature and are more general. Broberg [**2**] has shown that

$$N_f(X;X_0) \ll X^{1/2+\varepsilon}\|f\|(cX_0)^{\varepsilon}$$

where $\|f\|$ denotes the height of f, and the method also applies when f is a binary form, and Browning and Heath-Brown [**3**] have shown that

$$N_f(X;X_0) \ll X^{1/k+\varepsilon}$$

when the equation to be studied is replaced by

$$cy^k = f(x).$$

For this equation, the argument given here, under the assumption of absolute irreducibility, would only give

$$N_f(X;X_0) \ll X^{1/d(k)}$$

where $d(k)$ is the divisor function. We remark in passing that this curious exponent occurs because

$$\sum_{p\le x}(k,p-1)\frac{\log p}{p} \sim d(k)\log x.$$

However, when $3 \le k$, the bound of Pila [**9**], modulo the above remark concerning the coefficients of f, would give the stronger bound

$$N_f(X;X_0) \ll X^{1/k}(\log X)^{2d+3}.$$

Our initial interest in this subject was stimulated by the following special case, a segment of the Mordell equation.

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

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

in positive integers x, y satisfies

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

In general one would conjecture that if k and l are integers with

$$\min\{k,l\} \ge 2,$$

then the number $N(n)$ of solutions of $x^k + y^l = n$ in positive integers is $\ll n^\varepsilon$. Whilst this is easily established when $(k,l) > 1$, it is otherwise open. Yet in the case $(k,l) = 1$ one might even ponder the stronger statements

$$N(n) \ll \log n \quad \text{or} \quad N(n) \ll \log\log n.$$

2. The proof. We use the larger sieve of Gallagher [**6**], which we state in the following very slightly unusual form. For completeness, we include the short proof.

Lemma 2.1. [**6**]. *Suppose that $Q \ge 1$ and $X \ge 1$, 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 $X_0 < n \le X_0 + X$. 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 $\mathcal{A}_q$, and let $\mathcal{Q} \subset [1,Q] \cap \mathbf{N}$ be such that $g(q) \ne 0$ whenever $q \in \mathcal{Q}$. Then, whenever the denominator on the right is positive, we have*

$$Z^2 \le \frac{\sum_{q \in \mathcal{Q}} \Lambda(q) - \log X}{\sum_{q \in \mathcal{Q}} (\Lambda(q)/g(q)) - \log X} \sum_m c_m^2.$$

Proof. By squaring out it is easily seen that

$$\sum_{a \in \mathcal{A}_q} \left| Z(q,a) - \frac{Z}{g(q)} \right|^2 = \sum_{\substack{m,n \\ m \equiv n \pmod{q}}} c_m c_n - \frac{Z^2}{g(q)}$$
$$= \sum_m c_m^2 + \sum_{\substack{m \ne n \\ m \equiv n \pmod{q}}} c_m c_n - \frac{Z^2}{g(q)}.$$

Let

$$\lambda = \sum_{q \in \mathcal{Q}} \Lambda(q) \sum_{a \in \mathcal{A}_q} \left| Z(q,a) - \frac{Z}{g(q)} \right|^2.$$

Then

$$\lambda = \sum_{q \in \mathcal{Q}} \Lambda(q) \sum_m c_m^2 + \sum_{m \ne n} c_m c_n \sum_{\substack{q \mid m-n \\ q \in \mathcal{Q}}} \Lambda(q) - Z^2 \sum_{q \in \mathcal{Q}} \frac{\Lambda(q)}{g(q)}.$$

The sum $\sum_{\substack{q \mid m-n \\ q \in \mathcal{Q}}} \Lambda(q)$ is at most $\sum_{q \mid m-n} \Lambda(q) = \log |m-n| \le \log X$. Hence,

$$\lambda \le \Big(\sum_{q \in \mathcal{Q}} \Lambda(q) - \log X \Big) \sum_m c_m^2 - \Big(\sum_{q \in \mathcal{Q}} \frac{\Lambda(q)}{g(q)} - \log X \Big) Z^2,$$

and the lemma follows on noticing that $\lambda \ge 0$. □

We suppose first of all that the coefficients of f have greatest common divisor 1. We apply the lemma with $c_n = 0$ unless $X_0 <$

$n \le X_0 + X$ and $f(n)/c$ is a perfect square in which case we take $c_n = 1$. Let p be an odd prime. If $p \nmid c$ and a is such that $f(a)c^{-1}$ is a quadratic non-residue modulo p, and $x \equiv a \pmod{p}$, then $f(x)/c$ cannot be a perfect square. Hence, $Z(p,a) = 0$. Thus,

$$g(p) = \frac{1}{2}g_0(p) + \frac{1}{2}\sum_{a=1}^{p}\left(1 + \left(\frac{cf(a)}{p}\right)_L\right),$$

where $g_0(p)$ is the number of solutions of $f(x) \equiv 0 \pmod{p}$. Since f is non-trivial modulo p, we have $g_0(p) \le d$, and since $cy^2 - f(x)$ is absolutely irreducible, then by [**10,** Theorem 2B or 2C] of Schmidt we have

$$\sum_{a=1}^{p}\left(\frac{f(a)}{p}\right)_L \ll \sqrt{p}.$$

Thus, we can certainly choose $\mathcal{A}_p$ so that $g(p) = p/2 + O(\sqrt{p})$ and $g(p) > 0$ when $p > p_0(d)$, and then

$$\frac{1}{g(p)} = \frac{2}{p} + O(p^{-3/2}). \tag{2.1}$$

If $p \mid c$, then there are at most d values of a so that $f(a) \equiv cy^2 \pmod{p}$ for some y, and hence for $p > p_0(d)$ we can choose $\mathcal{A}_p$ so that $g(p) = p/2 + O(1)$, whence (2.1) holds once more. We now take $\mathcal{Q}$ to be the set of primes p with $p_0 < p \le Q$, where Q is a parameter at our disposal. Then by [**8,** Theorem 6.9] of Montgomery and Vaughan,

$$\sum_{q\in\mathcal{Q}} \Lambda(q) = Q + O(Q/\log Q)$$

and by Theorem 2.7 *ibidem*,

$$\sum_{q\in\mathcal{Q}} \frac{\Lambda(q)}{g(q)} = 2\log Q + O(1).$$

We now choose $Q = CX^{1/2}$ for a suitable constant C. Then

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

and since $c_m = 1$ or 0, it follows from the lemma that

$$\sum_m c_m \ll X^{1/2},$$

as required.

Now suppose that the coefficients of f have a greatest common divisor $d > 1$. We may certainly suppose that $(c, d) = 1$. Put $d = d_1 d_2^2$ where d_1 is square free. Thus, for a solution $d_1 d_2 \mid y$. Hence, we can replace f by $f_1 = f/d$ and y by $y d_1 d_2$ to obtain the equation $c d_1 y^2 = f_1(x)$, and appeal to the previous case.

REFERENCES

1. E. Bombieri and J.S. Pila, *The number of integral points on arcs and ovals*, Duke Math. J. **59** (1989), 337–357.

2. N. Broberg, *Rational points on finite covers of* $\mathbb{P}^1$ *and* $\mathbb{P}^2$, J. Number Theor. **101** (2003), 195–207.

3. T.D. Browning and D.R. Heath-Brown, *Plane curves in boxes and equal sums of two powers*, Math. Z. **251** (2005), 233–247.

4. S.D. Cohen, *The distribution of Galois groups and Hilbert's irreducibility theorem*, Proc. Lond. Math. Soc. **43** (1981), 227–250.

5. M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theor. **6** (1974), 211–231.

6. P.X. Gallagher, *The large sieve*, Mathematika **14** (1967), 14–20.

7. H.A. Helfgott and A. Venkatesh, *Integral points on elliptic curves and* 3*-torsion in class groups*, Amer. J. Math. **19** (2006), 527–550.

8. H.L. Montgomery and R.C. Vaughan, *Multiplicative number theory* I, *Classical theory*, Cambridge University Press, Cambridge, 2006.

9. J. Pila, *Density of integer points on plane algebraic curves*, Int. Math. Res. Notes **18** (1996), 903–912.

10. W.M. Schmidt, *Equations over finite fields, an elementary approach*, Lect. Notes Math. **536** (1976), Springer-Verlag, New York.

11. J.-P. Serre, *Lectures on the Mordell-Weil theorem*, second edition, Friedr. Viewag & Sohn Verlaug, Braunschweig, 1990.

12. C.L. Siegel, *Uber einige Anwendungen Diophantischer Approximationen*, Abh. Preuss. Akad. Wissen., 1929.

Department of Mathematics, McAllister Building, Pennsylvania State University, University Park, PA 16802
Email address: **rvaughan@math.psu.edu**