A Birch-Goldbach theorem

J. Brüdern, R. Dietmann, J. Y. Liu and T. D. Wooley

Abstract. We prove an analogue of a theorem of Birch with prime variables.

Mathematics Subject Classification (2000). Primary 11D72, 11P32; Secondary 11E76.

Keywords. Diophantine equations, prime numbers.

1. Introduction

The problem of establishing the solubility of homogeneous diophantine equations in many variables is, with the exception of diagonal forms and their close kin, one of considerable complexity. Methods based on that due to Hardy and Littlewood (the *circle method*; see in particular [2] and [9]) are in general delicate, and do not lend themselves to the investigation of problems in which the variables are restricted to special sequences. The elementary method of Birch [1], meanwhile, in which one first seeks to diagonalise the equation, and then apply the circle method to the latter, replaces the original variables with linear forms in a new, much smaller set of variables. Thus, any restriction of the variables in the original problem to a special sequence demands that the resulting diagonal equation be solved in conjunction with a very large number of additional linear equations in variables from the restricted sequence. At present both approaches seem infeasible so far as solving general homogeneous equations in prime numbers is concerned. Our goal in this note is to show that homogeneous equations of odd degree in sufficiently many variables may, nonetheless, be solved with the variables constrained essentially to be prime numbers.

Theorem 1. *Given odd natural numbers $d_1, \dots, d_r$, there exists a positive number $s_0 = s_0(\mathbf{d})$, depending at most on $\mathbf{d}$, with the following property. Whenever $s >$*

*JL is supported in part by NSFC 10531060, and TW by a Royal Society Wolfson Research Merit Award. JB and TW thank the Hausdorff Institute for its hospitality during the completion of this work, and together with JL they are grateful to L. Coffee in Weihai for useful contributions to this project.

$s_0(\mathbf{d})$, and $f_i \in \mathbb{Q}[x_1, \dots, x_s]$ is a form of degree d_i for $1 \le i \le r$, there exist fixed integers $c_1, \dots, c_s$, with $(c_1, \dots, c_s) = 1$, satisfying the property that the system of equations $f_i(c_1 p_1, \dots, c_s p_s) = 0 \quad (1 \le i \le r)$ possesses infinitely many solutions in prime numbers $p_1, \dots, p_s$, not all equal.

The presence in the theorem of the auxiliary integers c_i obstructs a clean Goldbach analogue of Birch's theorem [1], but the conclusion would be invalid in their absence. Consider, for example, distinct prime numbers $\pi_1, \dots, \pi_s$, write $P = \pi_1 \dots \pi_s$, and define $P_i = (P/\pi_i)^{d+1}$. The diagonal equation $P_1 x_1^d + \cdots + P_{s-1} x_{s-1}^d = P_s x_s^d$ has the property that any integral solution $\mathbf{x}$ satisfies the condition that π_i^2 divides x_i for $1 \le i \le s$, whence a solution in prime numbers is impossible without some modification of the kind employed in the statement of Theorem 1.

Hitherto, the only available conclusions of this type have been restricted almost exclusively to the diagonal case. Thus, conclusions for diagonal equations are clearly within the compass of the methods of Hua [7] (see [4] and [13], for example). There is also forthcoming work of Marasingha concerning solutions of ternary quadratic equations in almost-primes. For general conjectures in this direction, meanwhile, we refer the reader to the recent paper of Bourgain, Gamburd and Sarnak [3]. The inquisitive reader will find some discussion concerning permissible choices for $s_0(\mathbf{d})$ in section 2 below. In particular, one may take $s_0(3) = 36$, so that homogeneous rational cubic equations are essentially soluble in prime numbers whenever they have 37 or more variables.

Results on quadratic forms must necessarily take account of local solubility issues.

Theorem 2. *Suppose that $Q \in \mathbb{Q}[x_1, \dots, x_s]$ is a quadratic form having signature $(r, s-r)$, with $\min\{r, s-r\} \ge 2$. Suppose that either:*

(i) one has $s \ge 7$, or

(ii) the solution set of the quadratic equation $Q(\mathbf{x}) = 0$ contains a projective line over $\mathbb{Q}_p$ for every prime number p, and also contains a projective line over $\mathbb{R}$.

Then there exist fixed integers $c_1, \dots, c_s$, with $(c_1, \dots, c_s) = 1$, satisfying the property that the equation $Q(c_1 p_1, \dots, c_s p_s) = 0$ possesses infinitely many solutions in prime numbers $p_1, \dots, p_s$, not all equal.

Our strategy for constructing prime solutions to equations is simple to describe. First we seek a rational line embedded in the solution set of the system of diophantine equations under consideration, and then we employ the recent work of Green and Tao [6] concerning long arithmetic progressions in the primes in order to identify a point on this line which possesses, essentially, prime coordinates only. The astute reader will recognise that the principal conclusions therefore also hold when the primes are restricted to lie in a set of positive relative density.

2. Marshalling lines of primes

Our key lemma provides the means of transforming rational lines on complete intersections into points having essentially prime coordinates.

Lemma 3. *Let $r \in \mathbb{N}$, and suppose that $f_i \in \mathbb{Q}[x_1, \dots, x_s]$ is homogeneous for $1 \le i \le r$. If the solution set of the system of equations $f_i(\mathbf{x}) = 0$ $(1 \le i \le r)$ contains a rational projective line, then there exist integers $c_1, \dots, c_s$, with $(c_1, \dots, c_s) = 1$, satisfying the property that the system of equations $f_i(c_1p_1, \dots, c_sp_s) = 0$ $(1 \le i \le r)$ possesses infinitely many solutions in prime numbers $p_1, \dots, p_s$, not all equal.*

Proof. If the solution set of the system $\mathbf{f} = \mathbf{0}$ contains a rational projective line, then by homogeneity, we may suppose that there exist linearly independent integral s-tuples $\mathbf{a}$ and $\mathbf{b}$ with the property that

$$f_i(\mathbf{a}t + \mathbf{b}u) = 0 \quad (1 \le i \le r) \tag{1}$$

for every pair of integers t and u. If for some index i one has $a_i = b_i = 0$, then we take $c_i = 1$. It is apparent that such coordinates make no contribution in the system of equations $\mathbf{f}(\mathbf{x}) = \mathbf{0}$. We may consequently suppose without loss that one at least of a_i and b_i is non-zero for each index i with $1 \le i \le s$. Further, since $\mathbf{a}$ and $\mathbf{b}$ are linearly independent, by replacing $\mathbf{a}$ and $\mathbf{b}$ by suitable linearly independent linear combinations of $\mathbf{a}$ and $\mathbf{b}$, there is no loss even in supposing that a_i and b_i are both non-zero for $1 \le i \le s$.

Now let $\tilde{a} = a_1a_2 \dots a_s$, and put $\tilde{a}_i = \tilde{a}/a_i$ $(1 \le i \le s)$. In addition, put $M = \max_{1 \le i \le s} |b_i\tilde{a}_i|$. By Theorem 1.1 of [6], there exist infinitely many non-trivial arithmetic progressions of length $2M + 1$ consisting of prime numbers. Let $\varpi_1, \dots, \varpi_{2M+1}$ denote any one such progression. For some integer l and natural number q, one may write $\varpi_j = l + qj$ $(-M \le j \le M)$. Put $k_i = b_i\tilde{a}_i$ and then $p_i = \varpi_{k_i}$ for each index i. Then for $1 \le i \le s$, one has $a_ip_i = a_i(l + qb_i\tilde{a}_i) = a_il + b_i(q\tilde{a})$, and an inspection of equation (1) shows that with $t = l$, $u = q\tilde{a}$ and $c_i = a_i$ $(1 \le i \le s)$, the system $\mathbf{f}(\mathbf{x}) = \mathbf{0}$ is satisfied with $\mathbf{x} = \mathbf{a}t + \mathbf{b}u = (c_1p_1, \dots, c_sp_s)$. Thus the proof of the lemma is complete. □

We remark that developments in the Green-Tao theory offer the prospect of finding primes by working directly with the linear space rather than embedding into an arithmetic progression. Such would more efficiently handle the auxiliary coefficients $\mathbf{c}$.

The proof of Theorem 1 is now easily accomplished through the implications of Birch's theorem (see [1]). Given odd natural numbers $d_1, \dots, d_r$, let d be the larger of 7 and $\max_{1 \le i \le r} d_i$. Then it follows from Theorem 5.1 of [12] that whenever $s > \psi^{((d-5)/2)}(2dr)$, and $f_i \in \mathbb{Q}[x_1, \dots, x_s]$ satisfy the hypotheses of the statement of Theorem 1 above, then the solution set of the system $\mathbf{f}(\mathbf{x}) = \mathbf{0}$ contains a non-trivial rational projective line. An application of Lemma 3 therefore delivers the conclusion of Theorem 1 with $s_0(\mathbf{d}) = \psi^{((d-5)/2)}(2dr)$.

The definition of the function $\psi^{(n)}(x)$, unfortunately still not even astronomical, requires some explanation. Suppose that A is a subset of $\mathbb{R}$ and Ψ is a function

mapping A into A. When α is a real number, write $[\alpha]$ for the largest integer not exceeding α. Then we adopt the notation that whenever x and y are real numbers with $x \geq 1$, then $\Psi_x(y)$ denotes the real number $a_{[x]}$, where $(a_n)_{n=1}^{\infty}$ is the sequence defined by taking $a_1 = \Psi(y)$, and $a_{i+1} = \Psi(a_i)$ $(i \geq 1)$. Finally, when n is a non-negative integer we define the functions $\psi^{(n)}(x)$ by taking $\psi^{(0)}(x) = \exp(x)$, and when $n > 0$ by putting $\psi^{(n)}(x) = \psi_{42\log x}^{(n-1)}(x)$. Thus the above bound on $s_0(\mathbf{d})$ is of iterated exponential type. We note, however, that for cubics and quintics one can extract sharper bounds from [5], [10] and [11]. Thus, for example, it follows from Theorem 2(b) of [11] that the solution set of any homogeneous cubic equation in 37 or more variables contains a rational projective line, whence $s_0(3) \leq 36$.

Finally, we describe the proof of Theorem 2. We refer the reader to [8] for the necessary background material on the theory of quadratic forms. Let Q be a quadratic form satisfying the hypotheses of the statement of Theorem 2. If $s \geq 7$, then since the signature of Q is $(r, s-r)$ with $\min\{r, s-r\} \geq 2$, one finds that Q is indefinite. On recalling that quadratic forms in 5 or more variables possess non-trivial p-adic zeros for every prime p, it follows from the Hasse-Minkowski theorem that Q has a non-trivial rational zero. By a change of variables, therefore, we may suppose that Q takes the form

$$Q(\mathbf{x}) = x_1x_2 + Q_1(x_3, \dots, x_s). \tag{2}$$

But again, in view of the signature hypothesis on Q, we find that Q_1 is an indefinite quadratic form in at least 5 variables, and hence the Hasse-Minkowski theorem again shows that Q_1 has a non-trivial rational zero. Thus we may change variables again, and there is no loss in supposing that Q now takes the form

$$Q(\mathbf{x}) = x_1x_2 + x_3x_4 + Q_2(x_5, \dots, x_s). \tag{3}$$

But now the rational line $(t, 0, u, 0, \dots, 0)$ lies in the solution set of the equation $Q(\mathbf{x}) = 0$. Thus, prior to the various changes of variables encountered in this argument, the solution set of the quadratic equation $Q(\mathbf{x}) = 0$ does indeed contain a rational projective line. The conclusion of Theorem 2 consequently follows from Lemma 3 in case (i).

For case (ii) we must work a little harder. Observe first that under the hypotheses of case (ii), the quadratic form Q has zeros everywhere locally, and hence the Hasse-Minkowski theorem implies that Q has a rational zero. There is consequently again no loss in supposing that Q takes the form (2). Observe next that since the solution set of the equation $Q(\mathbf{x}) = 0$ contains a rational projective line over $\mathbb{R}$, then by a change of variables one may rewrite Q in the form (3) over $\mathbb{R}$. But the expression (2), which in the present setting is defined over $\mathbb{Q}$, also holds over $\mathbb{R}$. From Witt's theorem we know that every maximal nullspace of Q has the same dimension (see page 99 of [8]), and thus the rational quadratic form Q_1 must be isotropic over $\mathbb{R}$. The same argument applies when $\mathbb{R}$ is replaced by $\mathbb{Q}_p$, for each prime p, and thus we find that the equation $Q_1(\mathbf{x}) = 0$ is soluble everywhere locally. The Hasse-Minkowski theorem again shows that the quadratic form Q_1 has

a rational zero, and thus we may again change variables to show that Q takes the form (3), but now over the rational numbers. We therefore deduce, just as in the proof of case (i), that the solution set of the original quadratic equation $Q(\mathbf{x}) = 0$ contains a rational projective line, and the conclusion of Theorem 2 follows from Lemma 3 in case (ii).

References

[1] B. J. Birch, *Homogeneous forms of odd degree in a large number of variables.* Mathematika **4** (1957), 102–105.

[2] B. J. Birch, *Forms in many variables.* Proc. Roy. Soc. Ser. A **265** (1962), 245–263.

[3] J. Bourgain, A. Gamburd and P. Sarnak, *Sieving and expanders.* C. R. Math. Acad. Sci. Paris **343** (2006), 155–159.

[4] S. K. K. Choi and J. Y. Liu, *Small prime solutions of quadratic equations II.* Proc. Amer. Math. Soc. **133** (2005), 945–951.

[5] R. Dietmann, *Systems of cubic forms.* J. London Math. Soc. (2) **77** (2008), 666–686.

[6] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions.* Ann. of Math. (2) **167** (2008), 481–547.

[7] L. K. Hua, *Additive theory of prime numbers.* Amer. Math. Soc., Providence, RI, 1965.

[8] O. T. O'Meara, *Introduction to quadratic forms.* Springer-Verlag, Berlin, 1971.

[9] W. M. Schmidt, *The density of integer points on homogeneous varieties.* Acta Math. **154** (1985), 243–296.

[10] T. D. Wooley, *Forms in many variables.* Analytic number theory (Kyoto, 1996), pp. 361–376, London Math. Soc. Lecture Note Ser. vol. 247, Cambridge Univ. Press, Cambridge, 1997.

[11] T. D. Wooley, *Linear spaces on cubic hypersurfaces, and pairs of homogeneous cubic equations.* Bull. London Math. Soc. **29** (1997), 556–562.

[12] T. D. Wooley, *An explicit version of Birch's theorem.* Acta Arith. **85** (1998), 79–96.

[13] H. G. Zhou and T. Z. Wang, *Small solutions of cubic equations with prime variables in arithmetic progressions.* Acta Arith. **126** (2007), 169–193.

J. Brüdern
Institut für Algebra und Zahlentheorie
Universität Stuttgart
D-70511 Stuttgart, Germany
e-mail: `bruedern@mathematik.uni-stuttgart.de`

R. Dietmann
Department of Mathematics
Royal Holloway, University of London
Egham TW20 0EX, United Kingdom
e-mail: `Rainer.Dietmann@rhul.ac.uk`

J. Y. Liu
School of Mathematics
Shandong University
Jinan 250100, China
e-mail: jyliu@sdu.edu.cn

T. D. Wooley
School of Mathematics
University of Bristol
University Walk, Clifton
Bristol BS8 1TW, United Kingdom
e-mail: matdw@bristol.ac.uk