Rational Points and Analytic Number Theory

D.R. Heath-Brown
Mathematical Institute, Oxford

1 Introduction

There are a number of distinct ways in which analytic number theory can be used to provide information about rational points on algebraic varieties. Conversely, there are also a number of ways in which hoped-for results on the distribution of rational points could be used in classical problems from analytic number theory. Thus the analytic number theorist hopes not only to contribute to the theory of rational points, but also to get something back in return!

2 Contributions from Analytic Number Theory

The best known application of analytic methods to the distribution of rational points is the Hardy-Littlewood circle method. We shall not go into this in detail here, but refer the reader instead to the talk by Trevor Wooley. Given a projective variety V defined over $\mathbb{Q}$, the goal is to estimate the number $N(B)$ of rational points on V which have height at most B. When the method succeeds it usually establishes an estimate of the form

$$N(B) \sim \sigma_\infty \prod_p \sigma_p \, B^m, \quad (B \to \infty) \tag{1}$$

for an appropriate integer exponent m. Here σ_p is the p-adic density of points on V, and σ_∞ is the corresponding real density. The method tends to work when the dimension of the variety is reasonably large compared with its degree, and much of the research on the circle method is designed to weaken this constraint. The form of the asymptotic formula (1) is closely related to the Hasse Principle. Indeed one can usually show that the factors σ_∞ and σ_p are all positive when the variety has points everywhere locally. Under these circumstances the asymptotic formula (1) shows in particular that there are infinitely many rational points. Moreover when the circle method works it can usually be adapted to prove a weak approximation result as well.

It is therefore natural to ask what happens for varieties which do not satisfy weak approximation. Should we still expect (1) to hold? Since we expect that whenever we can apply the circle method we can also establish weak approximation, it follows that we should not expect the circle method to succeed on such varieties. As a test case consider the variety defined by

$$\begin{cases} L_1(x_1, x_2)L_2(x_1, x_2) = x_3^2 + x_4^2, \\ L_3(x_1, x_2)L_4(x_1, x_2) = x_5^2 + x_6^2, \end{cases} \tag{2}$$

where the L_i are suitable linear forms. It is known that weak approximation may fail for such varieties, as indeed may the Hasse Principle. None the less we can still establish an asymptotic formula for $N(B)$, which takes the shape

$$N(B) \sim \kappa\sigma_\infty \prod_p \sigma_p \; B^2. \tag{3}$$

The novelty here lies in the factor κ. This is a rational number in the range $\kappa \in [0, 2]$. Moreover it is constructed out of p-adic densities for certain "descent varieties" related to (2). One can show that the Hasse Principle fails exactly when $\kappa = 0$. The asymptotic formula (3) is proved essentially by passing to the "descent varieties" and using a variant of the circle method on these. In fact the classical circle method does not quite work and a delicate alternative method has to be used. Full details are given in the author's work [2].

A second area where discussion of rational points encounters issues in analytic number theory is in treatments of the Hasse Principle assuming Schinzel's Hypothesis. Schinzel's Hypothesis concerns the representation of primes by polynomials in one variable. The only instance of the hypothesis which is known to be true is Dirichlet's theorem on primes represented as a linear polynomial $aX + b$. The classical proof of the Hasse Principle for quadratic forms in 4 variables uses Dirichlet's theorem, and one can view more recent developments as an extension of this idea. Thus Colliot-Thélène and Sansuc [1] used Schinzel's Hypothesis to prove the following result. Let $a_1, \ldots, a_r$ be non-zero rationals, and let $P_1, \ldots, P_r$ be irreducible polynomials over $\mathbb{Q}$. Then the system of equations

$$0 \neq P_i(t) = x_i^2 - a_i y_i^2, \quad (1 \leq i \leq r),$$

satisfies the Hasse Principle, and weak approximation.

In some problems one can use versions of Schinzel's Hypothesis which refer to polynomials in 2 or more variables. Here there has been recent progress in prime number theory, which enables us to handle primes represented by binary cubic forms, for example. As an application one can show the following, due to Heath-Brown and Moroz [3].

Theorem *Let a and b be coprime rational integers satisfying one of the following congruence conditions:*

$$a \text{ or } b = \pm 2 \text{ or } \pm 3 \pmod 9,$$

or

$$a = \pm b \pmod 9.$$

Then there is a nontrivial rational point on the surface

$$x_0^3 + 2x_1^3 + ax_2^3 + bx_3^3 = 0.$$

This is one of the few completely unconditional results in the area. The proof depends on a result of Satgé [4, Proposition 3.3] which states that the curve

$$x_0^3 + 2x_1^3 = pZ^3$$

has a non-trivial rational point for any prime $p \equiv 2 \pmod 9$. Satgé's argument uses a Heegner point construction. For the result above it therefore suffices

to show that the binary form $ax_2^3 + bx_3^3$ takes a prime value $p \equiv 2 \pmod 9$. Progress in prime number theory is such that this has now been established. With the above congruence constraints on a and b there are always suitable rational values of x_2 and x_3, with denominators 1 or 3. Indeed we can find infinitely many primes of the required form, although the application requires only one such prime.

3 Potential Applications to Analytic Number Theory

When analytic number theorists attack problems on rational points they often run into other, related, questions. Consider the counting function

$$N(F; B) = \#\{\mathbf{x} \in \mathbb{Z}^n : \ F(\mathbf{x}) = 0 \ \max_{1 \le i \le n} |x_i| \le B\}.$$

For the diagonal cubic hypersurface corresponding to $F(\mathbf{x}) = a_1 x_1^3 + \ldots + a_n x_n^3$ we can give an asymptotic formula for $N(F; B)$ as soon as $n \ge 8$, thanks to work on the circle method by Vaughan [5]. However we would like to handle smaller values of n. To deal with the case $n = 7$ it would suffice to prove the following conjecture.

Conjecture *We have*

$$N(F_0; B) \ll B^\theta$$

for some constant $\theta < 7/2$, *where*

$$F_0(\mathbf{x}) = x_1^3 + x_2^3 + x_3^3 - x_4^3 - x_5^3 - x_6^3.$$

This estimate is known to hold for any $\theta > 7/2$, by a classical result of Hua, and is believed to hold for any $\theta > 3$. From a geometrical viewpoint there is no obvious reason why the form F_0 should be related to F. Nor is it immediately apparent from a geometric viewpoint how an upper estimate for $N(F_0; B)$ can lead to an asymptotic formula for $N(F; B)$. However these relationships are quite simple from the viewpoint of the circle method, which is what makes it such a distinctive and useful tool.

One may also ask what happens for the form

$$F_0(\mathbf{x}) = x_1^d + x_2^d + x_3^d - x_4^d - x_5^d - x_6^d.$$

Again we conjecture that any $\theta > 3$ is admissible. In fact one can take $\theta = \theta_d < 7/2$ if d is large enough, but attempts to reduce the permissible size of d encounter some purely geometric questions. Typical of these is—what low degree curves are contained in the variety $F_0(\mathbf{x}) = 0$? For example when $d \ge 5$ the only lines are those that lie in trivial planes of the type $x_1 = x_4, x_2 = x_5, x_3 = x_6$. It would be good, for example, to know that there were no curves of degree at most 4, other than those lying in such planes. We should remark that a resolution of the problems described by Salberger in his lecture would also result in significant progress in reducing the exponent θ.

As an example of a potential application to other areas of the subject, consider the variety $V(k, s) \subset \mathbb{P}^{2s-1}$ defined by the equations

$$x_1^j + \cdots + x_s^j = y_1^j + \cdots + y_s^j, \quad (1 \le j \le k).$$

This is a cone with vertex $(1,\dots,1)$. The counting function $N(B)$ for this variety is the subject of Vinogradov's Mean Value Theorem. Upper bounds for $N(B)$ have various applications in analytic number theory, to the estimation of exponential sums in the first instance, and thence to bounds on the Riemann Zeta-function and the error term in the Prime Number Theorem. A great deal of effort has gone into improving the original upper bounds established by Vinogradov. It is not hard to show that

$$N(B) \gg \max\{B^s, B^{2s-k(k+1)/2}\}$$

for all $s, k \geq 1$. Moreover, if $s \leq k$ then all points have $x_1, \dots, x_s$ a permutation of $y_1, \dots, y_k$, so that $N(B) \sim c(k,s)B^s$ in this case. Moreover Vaughan and Wooley [6] have established the same asymptotic formula for $s = k+1$. On the other hand we know that

$$N(B) \sim c(k,s)B^{2s-k(k+1)/2}$$

for

$$s \geq s_0(k) = k^2(\log k + 2\log\log k + O(1))$$

(see Wooley [7]). It would be good to know how $N(B)$ behaves for values of s of intermediate size. It seems likely that a better understanding of the geometry of $V(k,s)$ would help. As an example, when $k = 4$ and $s = 6$ we ask the following. Let L be a linear space of projective dimension l, and C an irreducible component of $V(4,6) \cap L$. Assume that C is not contained in the 'diagonal' set where $(x_1, \dots, x_6)$ is a permutation of $(y_1, \dots, y_6)$. Then is $\dim C \leq (2l-1)/3$?

References

[1] J.-L. Colliot-Thélène, and J.-J. Sansuc, Sur le principe de Hasse et l'approximation faible, et sur une hypothèse de Schinzel, *Acta Arith.,* 41 (1982), 33-53.

[2] D.R. Heath-Brown, Linear relations amongst sums of two squares, (to appear).

[3] D.R. Heath-Brown and B.Z. Moroz, On the representation of primes by cubic polynomials in two variables, *Proc. London Math. Soc.,* (to appear).

[4] P. Satgé, Un analogue du calcul de Heegner, *Invent. Math.,* 87 (1987), 425-439.

[5] R. C. Vaughan, On Waring's problem for cubes, *J. Reine Angew. Math.,* 365 (1986), 122-170.

[6] R.C. Vaughan and T.D. Wooley, A special case of Vinogradov's mean value theorem, *Acta Arith.,* 79 (1997), 193-204.

[7] T.D.Wooley, Some remarks on Vinogradov's mean value theorem and Tarry's problem, *Monatsh. Math.,* 122 (1996), 265-273.