Counterexamples to the Hasse principle

Martin Bright

16 April 2008

1 The Hasse principle

If a polynomial equation defined over the rational numbers has no rational solutions, it can sometimes be very easy to prove this.

Example 1.1. The conic $x^2 + y^2 + z^2 = 0 \subset \mathbb{P}^2_{\mathbb{Q}}$ has no rational points. Why not? Because it has no real points.

Example 1.2. The conic $x^2 + y^2 = 3z^2 \subset \mathbb{P}^2_{\mathbb{Q}}$ has no rational points. For suppose that (x, y, z) were a solution, where we may assume that x, y, z are coprime integers. Then x^2, y^2, z^2 would all be congruent to 0 or 1 (mod 4); looking at the equation shows that they would all have to be 0 (mod 4), and therefore x, y, z all even, contradicting the assumption that they were coprime.

In both of these examples, we have proved that $X(\mathbb{Q}) = \emptyset$ by showing that $X(\mathbb{Q}_v) = \emptyset$ for some place v. In the first case it was $v = \infty$, the real place. In the second case we showed that $X(\mathbb{Q}_2)$ was empty: the argument applies equally well to a supposed solution over $\mathbb{Q}_2$.

Given a variety X over a number field k and a place v of k, it is a finite procedure to decide whether $X(k_v)$ is empty. Moreover, $X(k_v)$ is automatically non-empty for all but finitely many places v, which can be determined: this follows from the Weil conjectures. It is therefore a finite (and usually very straightforward) process to check whether $X(k_v)$ is non-empty for all v.

For some families of varieties, this is enough to ensure that $X(k)$ is non-empty. For example:

Theorem 1.3 (Hasse, Minkowski)**.** *Let k be a number field, and let $X \subset \mathbb{P}^n_k$ be defined by one quadratic form. If $X(k_v)$ is non-empty for all places v of k, then $X(k)$ is non-empty.*

Proof. See... □

Because of this theorem, we say that quadratic forms satisfy the *Hasse principle*. Some other families of varieties are also known to satisfy the Hasse principle: for example, Severi–Brauer varieties and del Pezzo surfaces of degree at least 5.

In order to state results about the Hasse principle more succinctly, it will be useful to define the set of *adelic points* of a variety X.

Definition 1.4. Let k be a number field. The ring of *adèles* of k is the restricted direct product $\mathbb{A}_k = \prod' k_v$ with respect to the rings of integers of the k_v. This is the subring of the direct product $\prod_v k_v$ consisting of those elements (x_v) such that x_v is an integer at all but finitely many places v. The set of *adelic points* of a variety X over k is the set $X(\mathbb{A}_k)$ of points of X with coordinates in the adèles of k.

Remark 1.5. The set of adelic points constists of those elements of the direct product $(P_v) \in \prod_v X(k_v)$ such that P_v has coordinates which are integers in k_v, for all but finitely many places v. If X is projective, then this is an equality: $X(\mathbb{A}_k) = \prod_v X(k_v)$. This is because any point of projective space over k_v can be written with coordinates which are integers in k_v.

Using this notation, we see that $X(\mathbb{A}_k)$ is non-empty precisely when all of the $X(k_v)$ are non-empty, that is, when X is everywhere locally soluble. So X satisfies the Hasse principle if the implication $X(\mathbb{A}_k) \neq \emptyset \implies X(k) \neq \emptyset$ holds.

If $X(k)$ is non-empty, we can further ask whether X satisfies weak approximation:

Definition 1.6. A smooth, geometrically irreducible, projective variety X over a number field k satisfies *weak approximation* if $X(k)$ is dense in $X(\mathbb{A}_k)$. Equivalently, given any open subsets $U_v \subseteq X(k_v)$ for finitely many places v, there exists a point in $X(k)$ lying in each U_v under the embedding $X(k) \subset X(k_v)$.

Unfortunately, not all varieties satisfy the Hasse principle.

Example 1.7 (Reichardt, Lind)**.** The curve of genus 1 defined by the equation

$$2Y^2 = X^4 - 17Z^4 \tag{1}$$

is a counterexample to the Hasse principle over $\mathbb{Q}$. In other words, this equation has solutions in $\mathbb{Q}_v$ for each place v, but has no rational solution.

Proof. Clearly there are real solutions. There are also solutions in $\mathbb{Q}_p$ for all $p \geq 3$ where the equation (1) has smooth reduction modulo p, since the Hasse bound says that any smooth curve of genus 1 over $\mathbb{F}_p$ has at least $p+1-2\sqrt{p} > 0$ points, and any of these lifts by Hensel's Lemma to a point over $\mathbb{Q}_p$. It only remains to check the finitely many primes of bad reduction (which are 2 and 17), and in each case a point is easily found.

We now show that there can be no rational solution to (1). If there were, then without loss of generality we could write it as (X, Y, Z) with X, Y, Z integers and X, Z coprime, and further assume that $Y > 0$. Now, what primes may divide Y? If q is odd and $q \mid Y$, then $X^4 \equiv 17Z^4 \pmod{q}$ and so 17 is a square modulo q. By quadratic reciprocity, this means that q is a square modulo 17.

Now 2 and -1 are also squares modulo 17, so we deduce that all primes dividing Y are squares modulo 17, and hence so is Y. We can therefore write $Y \equiv Y_0^2 \pmod{17}$. Substituting into (1), we get that $2Y_0^4 \equiv X^4 \pmod{17}$ and hence that 2 is a fourth power modulo 17. But this is not true, and so there can be no rational solution. □

Remark 1.8. The equation (1) is not homogeneous, so does not define a projective variety. There are two ways round this: either give the variable Y weight 2, so that the equation defines a smooth variety in a weighted projective space; or take one affine piece, say by setting Z equal to 1, form the projective closure of this affine curve, and then blow up to resolve the singular points at infinity.

The two procedures lead to isomorphic curves. In our case, none of this matters, since it is immediately clear that any rational solution must have all of X, Y, Z nonzero.

Most of the arguments in this proof are entirely local arguments: they involve making deductions about $X(\mathbb{Q}_v)$ for various places v. But there is one step which is not local, and that is the use of quadratic reciprocity. The theorem of quadratic reciprocity gives a link between behaviour at one prime and behaviour at another prime, and so shows that the possible locations of our hypothetical rational solution in the $X(\mathbb{Q}_v)$ are not independent of each other. We will see this technique repeated in the following examples.

Example 1.9 (Birch–Swinnerton-Dyer [1])**.** The non-singular del Pezzo surface of degree 4 defined by the equations

$$\begin{cases} uv = x^2 - 5y^2 \\ (u+v)(u+2v) = x^2 - 5z^2 \end{cases} \tag{2}$$

is a counterexample to the Hasse principle.

Proof. Let X denote this surface. We begin by showing that X has points everywhere locally. To do this, note that the points $(u, v, x, y, z) = (1 : 1 : 1 : 0 : \sqrt{-1})$, $(10, -10, 5, 5, \sqrt{5})$ and $(5, 0, 0, 0, \sqrt{-5})$ all lie on X, and that, for any place $v \neq 2$, at least one of them is defined over $\mathbb{Q}_v$. As for $\mathbb{Q}_2$, the point $(-25, 5, 0, 5, 2\sqrt{-15})$ lies in $X(\mathbb{Q}_2)$.

To show that X has no rational points, we begin by supposing that there exists a rational solution (u, v, x, y, z), where we may assume that u, v are coprime integers (but the other coordinates need not be integers).

Firstly we look at $X(\mathbb{Q}_5)$. x is a 5-adic integer, since otherwise uv would not be; similarly y is a 5-adic integer. Now suppose that 5 divided uv; then 5 would divide x, and therefore 5 would divide $(u+v)(u+2v)$. But 5 can divide at most one of u, v, so we have a contradiction and deduce that 5 divides neither u nor v. Similarly, 5 divides neither $(u+v)$ nor $(u+2v)$.

Now we use quadratic reciprocity, in the following disguise: if an integer n can be written as $n = x^2 - 5y^2$ for rational numbers x, y then any prime $p \equiv \pm 2 \pmod 5$ can divide n only to an even power. We deduce that uv (and hence u and v individually) are only divisible by such primes to even power, and therefore that u and v are both congruent to $\pm 1 \pmod 5$. Similarly, both $(u+v)$ and $(u+2v)$ are congruent to $\pm 1 \pmod 5$. But these statements cannot both be true, and so no rational solution exists. □

We conclude with one further example which, though not a counterexample to the Hasse principle, is a counterexample to weak approximation.

Example 1.10 (Swinnerton-Dyer [3])**.** The singular cubic surface defined by the equation

$$t(x^2 + y^2) = (4z - 7t)(z^2 - 2t^2) \tag{3}$$

has real locus with two connected components. Rational points are dense in one component; the other contains no rational points.

Proof. To see the two connected components of the real locus, we look at the affine piece $t \neq 0$, given by the equation

$$x^2 + y^2 = (4z - 7)(z^2 - 2). \tag{4}$$

This is the surface of revolution about the z-axis of the elliptic curve

$$u^2 = (4z - 7)(z^2 - 2). \tag{5}$$

Since the right-hand side of this equation is positive only for $|z| \leq \sqrt{2}$ and $z \geq 7/4$, these two ranges for z give two connected components of the curve, and hence two connected components of the surface (4).

Firstly, we will show that rational points are dense in the component $z \geq 7/4$. The point $(x_0, y_0, z_0) = (1, 1, 2)$ lies in the surface. Consider the circle given by the intersection of the surface with the plane $z = z_0$. This is a plane conic with a rational point, and so has an isomorphism (given by projection away from the rational point) to $\mathbb{P}^1_{\mathbb{Q}}$. On $\mathbb{P}^1_{\mathbb{Q}}$, rational points are dense in the real points; we deduce that the same is true for the circle.

On the other hand, we can produce many more points to which this argument can be applied. The intersection of our surface with the plane $\{x = y\}$ is the elliptic curve $2v^2 = (4z - 7)(z^2 - 2)$, and our point corresponds to the point $(1, 2)$ on this curve. It turns out that the point has infinite order, and so its multiples are dense in the real component of this curve which contains it. We thus get a set of points of the affine surface (4) with z-coordinates dense in $\{z \geq 7/4\}$, and so a dense set of rational points on that connected component of the surface.

Secondly, we must prove that there are no rational solutions with $|z/t| \leq \sqrt{2}$. We may assume that z, t are coprime integers and that $t > 0$. Multiplying the original equation (3) through by t gives

$$t(7t - 4z)(2t^2 - z^2) = (tx)^2 + (ty)^2 \tag{6}$$

and, on this component, each of the left-hand terms t, $7t - 4z$ and $2t^2 - z^2$ is non-negative.

Quadratic reciprocity again appears in this proof in the guise of a fact about quadratic forms: if n is a positive integer which can be written as $n = x^2 + y^2$, then any prime congruent to 3 (mod 4) must divide n to an even power. Applying this to (6) shows that, if $p \equiv 3 \pmod 4$, then the power of p dividing the left-hand side must be even. We claim that, in fact, the power of p dividing each of t, $7t - 4z$ and $2t^2 - z^2$ must be even. To prove this, we must look at their possible common factors and show that no such p can divide more than one of them.

- Since $(t, z) = 1$, we have $(t, 7t - 4z) = (t, 4)$ so the only prime dividing both t and $7t - 4z$ can be 2.
- $(t, 2t^2 - z^2) = (t, z^2) = 1$ so no prime can divide both t and $2t^2 - z^2$.
- Suppose that $p \mid (7t - 4z, 2t^2 - z^2)$ and $p \equiv 3 \pmod 4$. If p were to divide z, then p would also have to divide t, which we have already seen is impossible. So p divides neither t nor z, but does divide $(8t + 7z)(7t - 4z) - 28(2t^2 - z^2) = 17tz$, and therefore $p = 17$, but $17 \equiv 1 \pmod 4$.

Therefore none of t, $7t-4z$, $2t^2-z^2$ is congruent to 3 (mod 4). But, if t were even, then z would have to be odd, and therefore $2t^2-z^2 \equiv 3 \pmod 4$; whereas, if t were odd, then t would have to be congruent to 1 (mod 4) and therefore $7t-4z \equiv 3 \pmod 4$, giving a contradiction in either case. So there can be no rational solutions to (6), so none to (3) with $t \neq 0$ and $|z/t| \leq \sqrt{2}$. □

2 Hilbert symbols

The Hilbert symbol is a piece of notation closely related to the Legendre symbol for quadratic residues, which will be useful for reformulating the arguments of the previous section in a more unified way. An excellent reference in Chapter III of Serre's book [2].

Definition 2.1. Let K be a field, and let a and b be two non-zero elements of K. We define the *Hilbert symbol* to be

$$(a,b)_K := \begin{cases} 1 & \text{if the conic } ax^2+by^2=z^2 \text{ has a solution in } \mathbb{P}^2(K); \\ -1 & \text{otherwise.} \end{cases}$$

If k is a number field and v a place of k, then we write $(a,b)_v$ for $(a,b)_{k_v}$.

This slightly mysterious definition is given some algebraic meaning by the following proposition.

Proposition 2.2. *Let K be a field and $a,b \in K^\times$. Then $(a,b)_K = 1$ if and only if a is a norm from $K(\sqrt{b})$.*

Proof. See [2, Chapter III, Proposition 1]. □

There are some useful properties of the Hilbert symbol which are true over any field, and some further ones which are only true for local fields.

Proposition 2.3. *Let K be a field. The Hilbert symbol over K has the following properties:*

1. *Symmetry: $(a,b)_K = (b,a)_K$ for all $a,b \in K^\times$.*
2. *$(a,c^2)_K = 1$ for all $a,c \in K^\times$.*
3. *A weak form of bilinearity: if $(a,b)_K = 1$ then $(aa',b)_K = (a',b)_K$ for all $a' \in K^\times$.*
4. *$(a,-a) = 1$ for all $a \in K^\times$.*
5. *$(a,1-a) = 1$ for all $a \in K^\times \setminus \{1\}$.*

Proof. Some of these are obvious; for the rest, see [2, Chapter III, Proposition 2]. □

Proposition 2.4. *Let k be a number field. Then*

1. *For each place v of k, the Hilbert symbol defines a non-degenerate bilinear form on $k_v^\times/(k_v^\times)^2$.*

2. *For $a, b \in k^\times$, we have*

$$\prod_v (a,b)_v = 1$$

where the product is taken over all places of k.

Proof. For $k = \mathbb{Q}$, see [2, Chapter III, Theorems 2 and 3]. □

In the case $k = \mathbb{Q}$, there are simple explicit formulae giving the Hilbert symbol for any place of $\mathbb{Q}$.

Proposition 2.5. 1. *Let $a, b \in \mathbb{R}^\times$. Then*

$$(a,b)_\infty = (a,b)_\mathbb{R} = \begin{cases} 1 & \textit{if } a > 0 \textit{ or } b > 0; \\ -1 & \textit{if } a < 0 \textit{ and } b < 0. \end{cases}$$

2. *Let p be an odd prime; let $a, b \in \mathbb{Q}_p^\times$, and write $a = p^\alpha u$ and $b = p^\beta v$ with $u, v \in \mathbb{Z}_p^\times$. Write $\epsilon(p) = (p-1)/2$. Then*

$$(a,b)_p = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha.$$

In particular, $(u,v)_p = 1$ if $u, v \in \mathbb{Z}_p^\times$.

3. *Let $a, b \in \mathbb{Q}_2^\times$ and write $a = 2^\alpha u$ and $b = 2^\beta v$ with $u, v \in \mathbb{Z}_2^\times$. For $x \in \mathbb{Z}_2^\times$, write $\epsilon(x) = (x-1)/2$ and $\omega(x) = (x^2-1)/8$. Then*

$$(a,b)_2 = (-1)^{\epsilon(u)\epsilon(v) + \alpha\omega(v) + \beta\omega(u)}.$$

Proof. See [2, Chapter III, Theorem 1]. □

References

[1] B. J. Birch and H. P. F. Swinnerton-Dyer. The Hasse problem for rational surfaces. *J. Reine Angew. Math.*, 274/275:164–174, 1975. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III.

[2] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[3] H. P. F. Swinnerton-Dyer. Two special cubic surfaces. *Mathematika*, 9:54–56, 1962.