# Acquisition of Rational Points on Algebraic Curves

Pete L. Clark

February 2, 2006

§1: Introduction

Let $k$ be a field of char. 0 (e.g. $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}_p$).

Let $V_{/k}$ be an algebraic variety: an object given by a finite system of polynomial equations with coefficients in $k$.

(Assume $V_{/\overline{k}}$ nonsingular, projective, connected.)

Example: $k = \mathbb{Q}$,

$$F_N : X^N + Y^N = Z^N,$$

the **Fermat curve**.

Basic problem in arithmetic geometry: Understand the set $V(k)$ of $k$-rational points – solutions to the system of equations.

Q: What does it mean to "understand" $V(k)$?

“Sample” theorem (Wiles 1995): If $N \geq 3$, all $\mathbb{Q}$-rational solutions $(x, y, z)$ have $xyz = 0$.

Certainly the answer depends on $k$:
• $k = \mathbb{C}$, $V(\mathbb{C})$ a compact complex manifold: topological invariants, Hodge numbers, ....
• $k = \mathbb{R}$: $V(\mathbb{R})$ a compact real manifold; top. invariants, especially $H^0$.

• $k = \mathbb{Q}$. (Or any number field.)
a) Is $V(\mathbb{Q})$ finite?
b) If finite, find all the rational points.
c) If infinite, understand

(i) How they are distributed on $V$.
(ii) How many there are of any bounded height: $H(\frac{a}{b}) = \max(a, b)$).

d) If $V$ is an algebraic group, determine the group structure on $V(\mathbb{Q})$.

It would seem that no matter what $k$ is, we can agree that if

$$V(k) = \emptyset$$

there is nothing to understand.

But I don't agree!

Claim: We need to understand not just $V(k)$ but also $V(l)$ for all finite field extensions $l/k$.

Equivalently: understand $V(\overline{k})$ as a set with $\mathfrak{g}_k = Aut(\overline{k}/k)$-action.

**Proposed problem**: Go the other extreme; study the set $\mathcal{A}(V)$ of $l/k$ such that $V(l) \neq \emptyset$.

Objection 1: If $V(k) \neq \emptyset$, the problem is trivial.

Response: *Most* algebraic varieties over (e.g.) $\mathbb{Q}$ do not have $\mathbb{Q}$-rational points.

Objection 2: If $V(k) = \emptyset$, the problem is preposterously difficult:

For $k = \mathbb{Q}$, unknown whether there exists an algorithm to decide whether $V(\mathbb{Q}) = \emptyset$. For equations over $\mathbb{Z}$, there is no algorithm ("No" to Hilbert 10). Varying $k$ makes it hopeless.

Reponse: Agreed. Still, special cases make for interesting theorems and conjectures. Compare with:

Theorem: a) If $C_{/\mathbb{Q}}$ has genus 0 or 1, then there exists $k/\mathbb{Q}$ such that $\#C(k) = \infty$.
b) (Faltings) If $C$ has genus at least 2, then $\#C(k) < \infty$ for all $k/\mathbb{Q}$.

§2: Local versus global

Example: For any $g \geq 0$,

$$Y^2 = -(X^{2g+2} + 1)$$

gives a genus $g$ curve $C_{/\mathbb{Q}}$ with $C(\mathbb{Q}) = \emptyset$. Indeed, $C(\mathbb{R}) = \emptyset$.

(Obvious principle: if $\mathbb{Q} \hookrightarrow L$ and $V(L) = \emptyset$, then $V(\mathbb{Q}) = \emptyset$.)

Example: $2X^2 + 3Y^2 = Z^2$ has no $\mathbb{Q}$-points. Indeed, it has no points over $\mathbb{Z}/3\mathbb{Z}$.

This is also a case of our "obvious principle".

$$\mathbb{Z}_p = \lim_{n \leftarrow \infty} \mathbb{Z}/p^n\mathbb{Z}.$$

$$\mathbb{Q}_p = \mathbb{Z}_p \otimes \mathbb{Q}.$$

Recall: If $V$ is projective, $\mathbb{Q}$-valued points $\iff$ $\mathbb{Z}$-valued points; $\mathbb{Q}_p$-valued point $\iff$ $\mathbb{Z}_p$-valued point (clear denominators).

$V$ has $\mathbb{Q}_p$-valued points $\forall\ p \iff \forall\ N$ the system has solutions as a **congruence** modulo $N$.

Can compute a single $N$ such that if $V$ has points mod $N$ it has solutions over $\mathbb{Q}_p$ for all $p$ (**Hensel's Lemma**); and can deal with $\mathbb{R}$-points algorithmically.

Therefore, for $V_{/\mathbb{Q}}$, there's an algorithm to determine whether $\exists$ points **everywhere locally** (i.e., over $\mathbb{Q}_p$ and $\mathbb{R}$).

If $V(\mathbb{Q}) \neq \emptyset$ we say $V$ has **global points**. Clearly global points $\Longrightarrow$ everywhere local points.

**Hasse Principle**: **hope** that the converse holds.

## §3: Curves $C_{/k}$ of genus zero

Every genus zero curve is canonically a plane conic, i.e., the zero locus of a quadratic form $Q(X, Y, Z)$. Diagonalize and rescale: $C \cong C_{(a,b)}$,

$$C_{(a,b)} : aX^2 + bY^2 = Z^2.$$

$C$ has points over certain quadratic extensions, but not necessarily over $k$.

$C(k) \neq \emptyset \iff C \cong \mathbb{P}^1$.

**Theorem** (Hasse-Minkowski)
a) If $k = \mathbb{R}$ or $\mathbb{Q}_p$, there is a unique genus zero curve without rational points.
b) If $k = \mathbb{Q}$ and $C$, $C'$ are two conics, then $C \cong C' \iff \forall p \leq \infty, C_{/\mathbb{Q}_p} \cong C'_{/\mathbb{Q}_p}$.
c) $\#\{p \leq \infty \mid C(\mathbb{Q}_p) = \emptyset\} = 2n$.

Thus: $\forall p \leq \infty,\ C(\mathbb{Q}_p) \neq \emptyset \Longrightarrow C(\mathbb{Q}) \neq \emptyset$.

One can use this theorem to determine the set $\mathcal{A}(C_{/\mathbb{Q}})$.

Hasse Principle holds for **quadric hypersurfaces** and all **Severi-Brauer varieties** (and other "sufficiently Fano" varieties).

§4: Curves of genus one: elliptic curves

Let $C_{/k}$ be a curve of genus one.

**Assume** there exists $O \in C(k)$. Then $L(3[O])$ embeds $C$ into $\mathbb{P}^2$ as a Weierstrass cubic

$$y^2z+a_1xyz+a_3yz^2 = x^3+a_2x^2z+a_4xz^2+a_6z^3;$$

$O$ becomes "the point at $\infty$": $\{z = 0\} \cap C$.
$C(k)$ has natural group law with $e = [O]$:
$P, Q, R$ colinear $\Longrightarrow [P] + [Q] + [R] = [O]$.

**Theorem** (Mordell-Weil) Let $(C, O)_{/\mathbb{Q}}$ be an elliptic curve. Then $C(\mathbb{Q})$ is a finitely generated abelian group.

Rank and torsion are much studied. **If** we had an algorithm to determine whether a genus one curve $C_{/\mathbb{Q}}$ has a rational point, would have an algorithm for computing the Mordell-Weil group.

Example (Selmer):

$$C_{3,4,5} : 3x^3 + 4y^3 + 5z^3 = 0$$

has $\mathbb{Q}_p$-points for all $p \leq \infty$ but no $\mathbb{Q}$-rational points. (Goodbye Hasse Principle.)

Thus in genus one, the study of $\mathcal{A}(C_{/\mathbb{Q}})$ cannot be reduced to purely local considerations.

$\underline{|\,|\,|}$ is waiting in the wings...

§5 $g = 1$: **Invariants**

A genus 0 curve has points over a quadratic extension. For $g \geq 2$, there exists $l/k$ with $[l : k] \leq 2g - 2$ such that $C(l) \neq \emptyset$.

Nothing like this holds for genus one curves (the canonical divisor is trivial).

Definition: For any variety $V_{/k}$, the **m-invariant** is the least degree of $l/k$ such that $V(l) \neq \emptyset$.

Definition: For any variety $V_{/k}$, the **index** is the gcd over all degrees $[l : k] \mid V(l) \neq \emptyset$.

$i(V) =$ least pos. degree of a 0-cycle on $V$.

$= (V = C)$ least pos. degree of a divisor.

$m$-inv = least degree of *effective* zero-cycle.

$m$-invariant seems most basic: there are curves with index 1 but arbitrarily large $m$-invariant.

**Key fact**: For genus one curves, $i(C) = m(C)$.

(Cassels) $\forall\ n \in \mathbb{Z}^+$, $\exists$ a genus one curve $C_{/\mathbb{Q}}$ with $n \leq m(C) \leq n^2$.

Q (Lang & Tate, 1958): Are there genus one curves $C_{/\mathbb{Q}}$ of every positive index?

**Theorem 1** *For any number field $k$ and any $n \in \mathbb{Z}^+$, $\exists$ infinitely many genus one curves $C_{/k}$ with index $n$.*

§6: Solvable and abelian points

$\mathbb{Q}^{ab}$ := maximal abelian extension of $\mathbb{Q}$.

$\mathbb{Q}^{solv}$ := maximal solvable extension of $\mathbb{Q}$.

Abel, Galois: $\mathbb{Q}^{solv}$ is not algebraically closed.

A field $k$ is **pseudoalgebraically closed** (PAC) if every geometrically irreducible variety over $k$ – equivalently, every algebraic curve – has a $k$-rational point.

Conjecture: $\mathbb{Q}^{solv}$ is PAC.

Theorem (Ciperiani-Wiles): Every* genus one curve $C_{/\mathbb{Q}}$ has a point over $\mathbb{Q}^{solv}$.

Theorem (Frey): $\mathbb{Q}^{ab}$ is *not* PAC.

**Theorem 2** *There exists a plane cubic* $C_{/\mathbb{Q}}$ *with* $C(\mathbb{Q}^{ab}_{11}) = \emptyset$.

## §7: A conjectural anti-Hasse principle

People say: “In general, the Hasse principle does not hold for curves of genus $g \geq 1$.”

Q: What does this mean?

A1: There exist counterexamples with $g \geq 1$.

Challenge: For each $g \geq 2$, find a curve $C_{/\mathbb{Q}}$ violating the Hasse Principle. Find infinitely many. (Hyperelliptic curves?)

No *ad hoc* list of counterexamples will condemn a *principle*.

For every $g$, many genus $g$ curves $C_{/\mathbb{Q}}$ do *not* have points everywhere locally. Thus – in a rather legalistic way! – “many” curves **satisfy** the Hasse Principle.

A curve $C$ over a number field $k$ is a **potential Hasse principle violation** (PHPV) if there exists some number field $l/k$ such that $C_{/l}$ violates the Hasse principle.

**Conjecture 1** *(Anti-Hasse Principle) Let $C_{/k}$ be a curve defined over a number field, of positive genus, and without $k$-rational points. Then there exists some finite field extension $l/k$ such that $C_{/l}$ is PHPV.*

Very roughly, we believe that counterexamples to the Hasse Principle are plentiful on the moduli space of curves of genus $g$.

## §8: Refinements and special cases

For $V_{/\mathbb{Q}}$, the local m-invariant $m_{loc}(V)$ is the lcm of $m(V_{/\mathbb{Q}_p})$, $p \leq \infty$.

Lemma: $\exists$ $\infty$ly many $k/\mathbb{Q}$ of degree $m_{loc}(V)$ such that $V_{/k}$ has points everywhere locally.

**Conjecture 2** *(Refined anti-Hasse Principle) Under the hypotheses of Conjecture 1, $\exists$ $\infty$ly many $k/\mathbb{Q}$ of degree $m_{loc}$ such that $C_{/k}$ violates the Hasse principle.*

Proposition: If $m(C) > m_{loc}(C)$, $C$ is PHPV.

**Theorem 3** *For any $E_{/\mathbb{Q}}$, there exist $C_{/\mathbb{Q}}$, with Jacobian $E$, such that $C$ violates the Hasse principle over a quadratic field.*

Remark: Actually have more results on curves of genus one (period-index problem, large $\underline{|\ |\ |}$), but let's move on to curves of higher genus.

§9: Applications to Shimura curves

Idea: find examples of anti-Hasse Principle "in nature."

Many of the most studied algebraic curves over $\mathbb{Q}$ have "trivial" $\mathbb{Q}$-rational points, e.g. the Fermat curves $F_N$ have (1 : 0 : 1) and classical modular curves $X_0(N), \ldots$ have cusps.

Shimura curves: Let $D$ be a squarefree positive integer. There is a curve $X^D_{/\mathbb{Q}}$, given over $\mathbb{C}$ as the quotient of $\mathcal{H}$ by a Fuchsian group constructed from the positive norm units of a maximal order in the quaternion algebra $B_{/\mathbb{Q}}$ of discriminant $D$.

Shimura constructed a canonical $\mathbb{Q}$-rational model. There is a *moduli interpretation*: roughly, $X^D$ is a moduli space for abelian surfaces admitting $B$ as an algebra of endomorphisms.

As in the classical case (which we can view as $D = 1$), there are modular coverings $X_0^D(N)$, $X_1^D(N)$.

We'll assume: $N$ squarefree and prime to $D$.

Theorem (Shimura): $X^D(\mathbb{R}) = \emptyset$.

Some curves have genus zero, e.g. $X^6$, $X^{10}, X^{22}$; of course our conjecture does not apply to these. $g(X_0^D(N))$ approaches $\infty$ with $\min(D, N)$.

**Theorem 4** *For all $D > 546$, $\exists\ m$ such that $X^D_{/\mathbb{Q}(\sqrt{m})}$ violates the Hasse Principle.*

**Theorem 5** *There exists a constant $C$ such that: if $D \cdot N > C$, there exist number fields $k = k(D,N)$ and $l = l(D,N)$ such that $X_0^D(N)_{/k}$ and $X_1^D(N)_{/l}$ violate the Hasse principle.*

**Theorem 6** *Maintain the notation of the previous theorem; assume $D \cdot N > C$.*
*a) We may choose $k$ such that $[k : \mathbb{Q}] \mid 4$.*
*b) The degree $[l : \mathbb{Q}]$ necessarily tends to $\infty$ with $N$ (uniformly in $D$).*

Remark: Jordan ($\sim$ 1985) showed $X^{39}/_{\mathbb{Q}(\sqrt{-23})}$ violated the Hasse principle. Skorobogatov-Yafaev (2004) used descent theory to produce HPV's for $X_0^D(N)_{/\mathbb{Q}(\sqrt{m})}$. Their method requires conditions on **class numbers**, so seems very hard to get $\infty$ly many examples their way.

Some ingredients of the proof:

Definition: The **gonality** $d(C)$ of an algebraic curve $C_{/k}$ is the least degree of a $k$-morphism $C \to \mathbb{P}^1$.

**Theorem 7** *Let $C_{/k}$ be an algebraic curve defined over a number field. Suppose:*
*a) $C(k) = \emptyset$.*
*b) $d(C) > 2m > 2$ for a multiple $m$ of $m_{loc}(C)$.*
*Then there exist $\infty$ly many extensions $l/k$ with $[l : k] = m$ such that $C_{/l}$ violates the Hasse principle.*

The proof uses work of G. Frey and, especially, G. Faltings' **enormous theorem** on subvarieties of abelian varieties.

Remark: For a *general* curve, $d(C) \approx g(C)$. More essential is $m_{loc}(C) \ll g(C)$; it's not clear how common this condition is in general.

**Theorem 8** *(Ogg) The gonality of* $X_0^D(N)_{/\mathbb{Q}}$ *approaches infinity with* $\min(D, N)$*.*

Ogg proves the result by reducing modulo $p$ (for suitable $p$) and counting points!

For the $X_1^D(N)$ case, I used a much stronger gonality theorem of Abramovich: for all Shimura curves $X$, $d_{\mathbb{C}}(X) \geq \frac{21}{200}(g(X) - 1)$. This uses serious differential geometry.

**Theorem 9** *a)* $\forall$ $D$*,* $m_{loc}(X^D) = 2$*.*
*b)* $\forall$ $D$ *and* $N$*,* $m_{loc}(X_0^D(N))$ *is either* $2$ *or* $4$*.*

This, of course, exploits the geometry of Shimura curves; essentially new only at $p \mid N$.

The case of $X_1^D(N)$ follows from $X_0^D(N)$ essentially for free (because $X_1^D(N) \to X_0^D(N)$ is "not too ramified").

Remark: Note that we have made an end-run around the computation of $m(X_0^D(N))$. Many fascinating questions about quadratic points on $X_0^D(N)$ remain.

(Sample conjecture: for min$(D, N) \gg 0$, all quadratic points on $X_0^D(N)$ are CM points.)

**Theorem 10** *For all $D$, the curve $X^{D+} = X^D/w_D$ has points everywhere locally.*

**Conjecture 3** *For $D \gg 0$, the $X^{D+}(\mathbb{Q})$ consists only of CM points.*

The conjecture implies that for $\infty$ly many $D$, $X^{D+}_{/\mathbb{Q}}$ violates the Hasse principle.

Generalizations: (1) OK for Shimura curves over totally real fields. (2) Can also apply

**Theorem 11** *Let* $\{X_n\}_{n=1}^{\infty}$ *be a sequence of curves over* $\mathbb{Q}$ *with* $g(X_n) > 1$*. Suppose:*
*a)* $X_n(\mathbb{Q}) = \emptyset\ \forall n$*.*
*b)* $X_n$ *has semistable reduction. .*
*c)* $\lim_{n\to\infty} \frac{d_K(X_n)}{\log g(X_n)} = \infty$*.*
*d)* $\exists\ A \in \mathbb{Z}^+$ *such that* $\forall$ *places* $v$ *and all* $n$*, the Galois action on the irreducible components of the special fiber* $(X_n)_{/k_v}$ *of the minimal model trivializes over an extension of degree* $A$*.*
*Then* $n \gg 0 \Longrightarrow X_n$ *is PHPV.*

Next up: Study the case of $y^2 = P_4(x)$ (genus one, index 2).

Challenge problem:

$$C = X^{14} : (x^2 - 13)^2 + 7^3 + 2y^2 = 0.$$

Not hard to see that $C_{/\sqrt{m}}$ has points everywhere locally $\iff m < 0,\ (m, 7) = 1$; this set has density $\frac{3}{7}$. Show: global points only occur with density 0.