Rational Points on Hypersurfaces in Projective Space

Jörg Jahnel

Mathematisches Institut der Universität Göttingen

19. 07. 2006

joint work with Andreas-Stephan Elsenhans

The Fundamental Problem

Problem (Diophantine equation)

Given $f \in \mathbb{Z}[X_0, \ldots, X_n]$, describe the set

$$\{(x_0, \ldots, x_n) \in \mathbb{Z}^{n+1} \mid f(x_0, \ldots, x_n) = 0\},$$

explicitly.

The Fundamental Problem

More realistic from computational point of view:

Problem (Diophantine equation – search for solutions)

Given $f \in \mathbb{Z}[X_0, \ldots, X_n]$ and $B > 0$, describe the set

$$\{(x_0, \ldots, x_n) \in \mathbb{Z}^{n+1} \mid f(x_0, \ldots, x_n) = 0, |x_i| \leq B\},$$

explicitly.

B is usually called the *search limit*.

Geometric Meaning

- Integral points on an n-dimensional hypersurface in $\mathbf{A}^{n+1}$.

Geometric Meaning

- Integral points on an n-dimensional hypersurface in $\mathbf{A}^{n+1}$.
- If f is homogeneous: Rational points on an $(n-1)$-dimensional hypersurface V_f in $\mathbf{P}^n$.

A statistical forecast

$$Q(B) := \{(x_0, \ldots, x_n) \in \mathbb{Z}^{n+1} \mid |x_i| \leq B\}$$

Thus,

$$\#Q(B) = (2B+1)^{n+1} \sim C_1 \cdot B^{n+1}.$$

On the other hand,

$$\max_{(x_0,\ldots,x_n)\in Q(B)} |f(x_0, \ldots, x_n)| \sim C_2 \cdot B^{\deg f}.$$

Assuming equidistribution of the values of f on $Q(B)$, we are therefore led to expect the asymptotics

$$\#\{(x_0, \ldots, x_n) \in V_f(\mathbb{Q}) \mid |x_0|, \ldots, |x_n| \leq B\} \sim C \cdot B^{n+1-\deg f}$$

for the number of solutions.

Examples

The statistical projection explains the following well-known examples.

- $n+1-\deg f < 0$: Very few solutions.
  Example: $x^k + y^k = z^k$ for $k \geq 4$.

Examples

The statistical projection explains the following well-known examples.

- $n+1-\deg f < 0$: Very few solutions.
  Example: $x^k + y^k = z^k$ for $k \geq 4$.
- $n+1-\deg f = 0$: A few solutions.
  Example: $y^2 z = x^3 + 8xz^2$.
  Elliptic curves.
  Another Example: $x^4 + 2y^4 = z^4 + 4w^4$.
  More generally, surfaces of type $K3$.

Examples

The statistical projection explains the following well-known examples.

- $n+1-\deg f<0$: Very few solutions.
  Example: $x^k+y^k=z^k$ for $k\geq 4$.
- $n+1-\deg f=0$: A few solutions.
  Example: $y^2z=x^3+8xz^2$.
  Elliptic curves.
  Another Example: $x^4+2y^4=z^4+4w^4$.
  More generally, surfaces of type $K3$.
- $n+1-\deg f>0$: Many solutions.
  Example: $x^2+y^2=z^2$.
  Conics.
  Another Example: $x^3+y^3+z^3+w^3=0$.
  Cubic surfaces.

A few complications

- Unsolvability
  - Unsolvability in reals,
    $x^2+y^2+z^2=0$.
  - p-adic unsolvability,
    $u^3+2v^3+7w^3+14x^3+49y^3+98z^3=0$.
  - Obstructions against the Hasse principle
    (Brauer-Manin obstruction, unknown obstructions?).

A few complications

- Unsolvability
  - Unsolvability in reals,
    $x^2+y^2+z^2=0$.
  - p-adic unsolvability,
    $u^3+2v^3+7w^3+14x^3+49y^3+98z^3=0$.
  - Obstructions against the Hasse principle
    (Brauer-Manin obstruction, unknown obstructions?).
- "Accumulating" subvarieties:
  $x^3+y^3=z^3+w^3$ defines a cubic surface V in $\mathbf{P}^3$.
  $$\#\{(x_0,\dots,x_n)\in V(\mathbb{Q})\mid |x_0|,\dots,|x_n|\leq B\}\sim C\cdot B$$
  is predicted.
  However, V contains the line given by $x=z$, $y=w$, on which there is quadratic growth, already.

The conjectures

Let V_f be a smooth hypersurface in $\mathbf{P}^n$.

- $n+1-\deg f<0$: Then, V_f is a variety of general type.

Conjecture (Lang)

All $\mathbb{Q}$-rational points on V_f are contained in finitely many closed subvarieties $V_1,\dots,V_l\subsetneq V_f$.

The conjectures

Let V_f be a smooth hypersurface in $\mathbf{P}^n$.

- $n+1-\deg f < 0$: Then, V_f is a variety of general type.

Conjecture (Lang)

All $\mathbb{Q}$-rational points on V_f are contained in finitely many closed subvarieties $V_1, \ldots, V_l \subsetneq V_f$.

- $n+1-\deg f = 0$: Then, V_f is a variety of intermediate type.

Conjecture (Batyrev-Manin)

For each $\varepsilon > 0$, there are finitely many closed subvarieties $V_1, \ldots, V_l \subsetneq V_f$ such that

$$\#\{(x_0, \ldots, x_n) \in V^\circ(\mathbb{Q}) \mid |x_0|, \ldots, |x_n| \leq B\} \ll C \cdot B^\varepsilon,$$

$V^\circ := V_f \setminus (V_1 \cup \cdots \cup V_l)$.

The conjectures II

- $n+1-\deg f > 0$: Then, V_f is a Fano variety.

Conjecture (Manin)

$$\#\{(x_0, \ldots, x_n) \in V^\circ(\mathbb{Q}) \mid |x_0|, \ldots, |x_n| \leq B\} \sim C \cdot B^k \log^{r-1} B,$$

$k := n+1-\deg f$, $r = \operatorname{rk} \operatorname{Pic} V$. C is an explicit constant (Peyre).

What is known?

- For curves, all the conjectures above are proven
(Lang's conjecture: Faltings,
Batyrev-Manin conjecture: Mordell-Weil,
Manin's conjecture: Fano curves are rational, i.e. isomorphic to $\mathbf{P}^1$).

What is known?

- For curves, all the conjectures above are proven
(Lang's conjecture: Faltings,
Batyrev-Manin conjecture: Mordell-Weil,
Manin's conjecture: Fano curves are rational, i.e. isomorphic to $\mathbf{P}^1$).
- Manin's conjecture is true for $n \gg 2^{\deg f}$ (circle method).
[Birch, B. J.: *Forms in many variables,* Proc. Roy. Soc. Ser. A **265** (1961/1962), 245–263]

What is known?

- For curves, all the conjectures above are proven
  (Lang's conjecture: Faltings,
  Batyrev-Manin conjecture: Mordell-Weil,
  Manin's conjecture: Fano curves are rational, i.e. isomorphic to $\mathbf{P}^1$).
- Manin's conjecture is true for $n \gg 2^{\deg f}$ (circle method).
  [Birch, B. J.: *Forms in many variables,* Proc. Roy. Soc. Ser. A **265** (1961/1962), 245–263]
- If Manin's conjecture is true for X and Y then for $X \times Y$, too (Franke, Manin, Tschinkel).

What is known? II

- Manin's conjecture is established in many particular cases of low dimension, e.g.
  - generalized flag varieties (Franke, Manin, Tschinkel),
  - projective smooth toric varieties (Batyrev and Tschinkel),
  - certain toric fibrations over generalized flag varieties (Strauch and Tschinkel),
  - smooth equivariant compactifications of affine spaces (Chambert-Loir and Tschinkel),
  - $\mathbf{P}^2_{\mathbb{Q}}$ blown-up in four points in general position (Salberger, la Brèteche).

What is known? II

- Manin's conjecture is established in many particular cases of low dimension, e.g.
  - generalized flag varieties (Franke, Manin, Tschinkel),
  - projective smooth toric varieties (Batyrev and Tschinkel),
  - certain toric fibrations over generalized flag varieties (Strauch and Tschinkel),
  - smooth equivariant compactifications of affine spaces (Chambert-Loir and Tschinkel),
  - $\mathbf{P}^2_{\mathbb{Q}}$ blown-up in four points in general position (Salberger, la Brèteche).

- The simplest case where Manin's conjecture is *open* are smooth cubic surfaces. (There is, however, a lot of numerical evidence in this case [Peyre-Tschinkel, Heath-Brown].)

Numerical evidence for Manin's Conjecture

Experimental Result (E.+J.)
There is numerical evidence for Manin's Conjecture in the case of the hypersurfaces in $\mathbf{P}^4_{\mathbb{Q}}$ given by $ax^e = by^e + z^e + v^e + w^e$ for $e = 3$ and 4.

This requires algorithms to

- solve Diophantine equations,

Numerical evidence for Manin's Conjecture

Experimental Result (E.+J.)

There is numerical evidence for Manin's Conjecture in the case of the hypersurfaces in $\mathbf{P}^4_{\mathbb{Q}}$ given by $ax^e = by^e + z^e + v^e + w^e$ for $e = 3$ and 4.

This requires algorithms to

- solve Diophantine equations,
- compute Peyre's constant,

Numerical evidence for Manin's Conjecture

Experimental Result (E.+J.)

There is numerical evidence for Manin's Conjecture in the case of the hypersurfaces in $\mathbf{P}^4_{\mathbb{Q}}$ given by $ax^e = by^e + z^e + v^e + w^e$ for $e = 3$ and 4.

This requires algorithms to

- solve Diophantine equations,
- compute Peyre's constant,
- detect accumulating subvarieties.

An algorithm to solve Diophantine equations I

The following example was our starting point.

Example (Sir P. Swinnerton-Dyer, 2002)

The equation

$$x^4 + 2y^4 = z^4 + 4w^4$$

defines a $K3$ surface S in $\mathbf{P}^3$.

$(1 : 0 : 1 : 0)$ and $(1 : 0 : (-1) : 0)$ are $\mathbb{Q}$-rational points on S, the two *obvious* points.

Is there another $\mathbb{Q}$-rational point on S?

An algorithm to solve Diophantine equations II

Algorithm (A naive algorithm)

Write $x^4 + 2y^4 - 4w^4 = z^4$ and let x, y, and w run in a triple loop.

Complexity: $C \cdot B^3$.

Realistic search bound: 50 000.
(We did a trial run with search bound 10 000.)

An algorithm to solve Diophantine equations III

Algorithm (A better algorithm)

The two sets $\{x^4 + 2y^4 \mid |x|, |y| \leq B\}$ and $\{z^4 + 4w^4 \mid |z|, |w| \leq B\}$ have $\sim B^2$ elements each. List them and form their intersection.

Facts

- *Complexity:* $O(B^2 \log B)$ *(use sorting, D. Bernstein),*
  $O(B^2)$ *(assuming uniform hashing, E.+J.).*
- *Memory Usage:* $O(B^2)$ *(naively),*
  $O(B)$ *(D. Bernstein's Algorithm*
  – generates the sets in sorted order.)

Detection of solutions of Diophantine equations – Hashing

Our method works for Diophantine equations of the form

$$f(x_1, \ldots, x_k) = g(y_1, \ldots, y_l).$$

Detection of solutions of Diophantine equations – Hashing II

Writing

We store the vectors $(x_1, \ldots, x_k)$ in a hash table (with space for up to 2^{27} entries).

The *hash function* $H: \mathbb{Z} \to [0, 2^{27} - 1]$ is given by a selection of bits, i.e. $H(z) :=$ a selection of bits of $(z \bmod 2^{64})$.

For each vector $(x_1, \ldots, x_k)$, the expression $H(f(x_1, \ldots, x_k))$ defines its position in the hash table.

Besides $(x_1, \ldots, x_k)$, we also write a *control value* $K(f(x_1, \ldots, x_k))$, $K(z) :=$ a selection of the remaining bits of $(z \bmod 2^{64})$.

Reading

Then, we search for vectors $(y_1, \ldots, y_l)$ such that hash value and control value do fit.

Detection of solutions of Diophantine equations – Hashing III

Remarks

- Assuming uniform hashing (which implies there are not too many solutions), the expected running time is $O(B^{\max(k,l)})$.

  Congruence conditions might help to reduce the O-factor.

Detection of solutions of Diophantine equations – Hashing III

Remarks

- Assuming uniform hashing (which implies there are not too many solutions), the expected running time is $O(B^{\max(k,l)})$.

  Congruence conditions might help to reduce the O-factor.
- The algorithm actually detects *pseudo-solutions* where a coincidence of the control values and an "almost coincidence" of the hash values occurs.

  Some *post processing* with an exact multiprecision calculation is necessary (ARIBAS, GMP).

How to reduce memory usage when hashing?

Idea (Paging)

Choose $m \in \mathbb{Z}$ sufficiently large. Form the sets

$$L_c := \{f(x_1, \dots, x_k) \mid |x_1|, \dots, |x_k| \leq B, f(x_1, \dots, x_k) \equiv c \pmod{m}\}$$

and

$$R_c := \{g(y_1, \dots, y_l) \mid |y_1|, \dots, |y_l| \leq B, g(y_1, \dots, y_l) \equiv c \pmod{m}\}.$$

Memory usage: $B^{\max(k,l)}/m$ (assuming equidistribution).

Optimization through congruence conditions I

x and z are odd. y and w are even.

- Case 1: $5|y, w \quad (\Longrightarrow 5\nmid x, z)$.
  Then, $x^4 \equiv z^4 \pmod{625}$.
  We write pairs (x, z) and hash $x^4 - z^4$. We read $4w^4 - 2y^4$.
- Case 2: $5|x, y \quad (\Longrightarrow 5\nmid z, w)$.
  Then, $z^4 + 4w^4 \equiv 0 \pmod{625}$.
  Here, we write pairs (z, w) and hash $z^4 + 4w^4$. We read $x^4 + 2y^4$.

These congruences are particularly strong. They reduce the number of writing steps to 0.512% and the number of reading steps to 4%.

Optimization through congruence conditions II

Further congruences:

- Some congruences modulo small powers of 2:
  In Case 1, we always have $32|4w^4 - 2y^4$. But $32|x^4 - z^4$ implies $x \equiv \pm z \pmod{8}$. This saves on writing.
  No such optimization for Case 2.

- Some congruences modulo 81:
  In Case 1, $2y^4 - 4w^4$ represents $(0 \bmod 3)$ only trivially. Therefore, we do not need to write (x, z) when $x^4 \equiv z^4 \pmod{3}$ but $x^4 \not\equiv z^4 \pmod{81}$.
  In Case 2, there is a similar congruence which saves on the reading step.

A new solution – Answer to Sir P. Swinnerton-Dyer's question I

Calculation

```
==> 1484801**4 + 2 * 1203120**4.
-: 90509_10498_47564_80468_99201

==> 1169407**4 + 4 * 1157520**4.
-: 90509_10498_47564_80468_99201
```

Theorem (E.+J.)

Up to changes of sign, $(1\,484\,801 : 1\,203\,120 : 1\,169\,407 : 1\,157\,520)$ *is the only non-obvious* $\mathbb{Q}$*-rational point of height* $\leq 10^8$ *on Sir P. Swinnerton-Dyer's surface* S*.*

This means, on S *there exist precisely ten* $\mathbb{Q}$*-rational points of height* $\leq 10^8$*.*

A new solution – Answer to Sir P. Swinnerton-Dyer's question II

Remarks

- The new solution was found on December 2, 2004 by an intermediate version of our programs for search bound $2.5 \cdot 10^6$.
- The final version of the programs (for search bound 10^8) took almost exactly 100 days of CPU time on an AMD Opteron 248 processor. This time is composed almost equally of 50 days for Case 1 and 50 days for Case 2.
- The main computation was executed in parallel on two machines in February and March, 2005.

A new solution – Answer to Sir P. Swinnerton-Dyer's question III

Question

What is the asymptotics of $\#\{(x, y, z, w) \in S(\mathbb{Q}) \mid H_{\text{naive}}(p) \leq B\}$ for $B \to \infty$?

A wild guess:

$$\#\{(x, y, z, w) \in S \mid H_{\text{naive}}(p) \leq B\} \sim (\log B)^\alpha$$

(similarly to abelian surfaces where $\alpha = \text{rk}(S(\mathbb{Q}))/2$.)

An even wilder guess: $\alpha = 1/2$.

Manin's Conjecture – Peyre's constant I

Recall, we consider the hypersurfaces in $\mathbf{P}^4_{\mathbb{Q}}$ given by

$$ax^e - by^e = z^e + v^e + w^e$$

for $e = 3$ and 4.

Remarks

- Search for $\mathbb{Q}$-rational points is obviously of complexity $O(B^3)$.
- When considering $O(B)$ varieties (differing only by a and b), simultaneously, then the running-time is *still* $O(B^3)$.

  We considered the varieties with $a, b = 1, \ldots, 100$ (5 000 cubics, 10 000 quartics) with a search bound of 5 000 (cubics) and 100 000 (quartics).

Manin's Conjecture – Peyre's constant II

Conjecture (Manin's Conjecture – Version for hypersurfaces in $\mathbf{P}^n$)

Let the smooth variety $V_f \subset \mathbf{P}^n$ be given by $f = 0$. Then,

$$\#\{(x_0, \dots, x_n) \in V^\circ(\mathbb{Q}) \mid |x_0|, \dots, |x_n| \le B\} \sim C \cdot B^k \log^{r-1} B,$$

for $k = n + 1 - \deg(f)$ and $r = \operatorname{rk} \operatorname{Pic} V$.

Here, C is an explicit constant (due to E. Peyre),
[Peyre, E.: *Hauteurs et mesures de Tamagawa sur les variétés de Fano*, Duke Math. J. **79** (1995), 101–218, Définition 2.3]

Manin's Conjecture – Peyre's constant III

Definition (Peyre's constant)

For $n \ge 4$, *Peyre's constant* is the Tamagawa-type number

$$C = \prod_{p \in \mathbb{P} \cup \{\infty\}} \left(1 - \frac{1}{p}\right) \tau_p$$

where

$$\tau_p = \lim_{m \to \infty} \frac{\#V(\mathbb{Z}/p^m\mathbb{Z})}{p^{m \dim(V)}} \qquad \text{for } p \in \mathbb{P}$$

and

$$\tau_\infty = \frac{1}{2} \int\limits_{\substack{f(x_0,\dots,x_n)=0 \\ |x_i| \le 1}} \frac{1}{\frac{\partial f}{\partial x_j}} \, dx_0 \dots \widehat{dx_j} \dots dx_n.$$

An algorithm to *count* solutions I

To compute Peyre's constant, the main work to be done is to *count* solutions of the same equation $f(x_0, \dots, x_n) = 0$ but over finite fields $\mathbb{F}_p$ instead of $\mathbb{Z}$.

Consider an equation of the form

$$(+) \qquad \sum_{i=0}^{n} f_i(x_i) = 0.$$

Denote by $d^{(i)}(k) := \#\{x \in \mathbb{F}_p \mid f_i(x) = k\}$ the numbers of representations. Then, the number of solutions of $(+)$ is equal to

$$(d^{(0)} * d^{(1)} * \dots * d^{(n)})(0).$$

Use FFT convolution to compute $d^{(0)} * d^{(1)} * \dots * d^{(n)}$.

An algorithm to *count* solutions II

Remarks (Complexity)

- We need to compute n convolutions of vectors of length p.
- A convolution takes $O(p \log p)$ steps.

An algorithm to compute Peyre's constant

Algorithm (FFT point counting on

$$V^e_{a,b}\colon ax^e = by^e + z^e + v^e + w^e,$$

$e = 3, 4$ over $\mathbb{F}_p$)

- Initialize a vector $X[0 \dots p]$ with zeroes.

An algorithm to compute Peyre's constant

Algorithm (FFT point counting on

$$V^e_{a,b}\colon ax^e = by^e + z^e + v^e + w^e,$$

$e = 3, 4$ over $\mathbb{F}_p$)

- Initialize a vector $X[0 \dots p]$ with zeroes.
- Let r run from 0 to $p-1$ and increase $X[r^e \bmod p]$ by 1.

An algorithm to compute Peyre's constant

Algorithm (FFT point counting on

$$V^e_{a,b}\colon ax^e = by^e + z^e + v^e + w^e,$$

$e = 3, 4$ over $\mathbb{F}_p$)

- Initialize a vector $X[0 \dots p]$ with zeroes.
- Let r run from 0 to $p-1$ and increase $X[r^e \bmod p]$ by 1.
- Calculate $\tilde{Y} := X * X * X$ by FFT convolution.

An algorithm to compute Peyre's constant

Algorithm (FFT point counting on

$$V^e_{a,b}\colon ax^e = by^e + z^e + v^e + w^e,$$

$e = 3, 4$ over $\mathbb{F}_p$)

- Initialize a vector $X[0 \dots p]$ with zeroes.
- Let r run from 0 to $p-1$ and increase $X[r^e \bmod p]$ by 1.
- Calculate $\tilde{Y} := X * X * X$ by FFT convolution.
- Normalize by putting $Y[i] := \tilde{Y}[i] + \tilde{Y}[i+p] + \tilde{Y}[i+2p]$ for $i = 0, \dots, p-1$.
  (Now, $Y[i]$ is the number of solutions of $z^e + v^e + w^e \equiv i \pmod{p}$.)

Algorithm to compute Peyre's constant II

- Initialize N as zero.

Algorithm to compute Peyre's constant II

- Initialize N as zero.
- (Counting points with $x \neq 0$)
  Let j run from 0 to $p-1$ and increase N by $Y[(a - bj^4) \bmod p]$.

Algorithm to compute Peyre's constant II

- Initialize N as zero.
- (Counting points with $x \neq 0$)
  Let j run from 0 to $p-1$ and increase N by $Y[(a - bj^4) \bmod p]$.
- (Adding points with $x = 0$ and $y \neq 0$)
  Increase N by $Y[(-b) \bmod p]$.

Algorithm to compute Peyre's constant II

- Initialize N as zero.
- (Counting points with $x \neq 0$)
  Let j run from 0 to $p-1$ and increase N by $Y[(a - bj^4) \bmod p]$.
- (Adding points with $x = 0$ and $y \neq 0$)
  Increase N by $Y[(-b) \bmod p]$.
- (Adding points with $x = y = 0$)
  Increase N by $(Y[0] - 1)/(p - 1)$.

Algorithm to compute Peyre's constant II

- Initialize N as zero.
- (Counting points with $x \neq 0$)
  Let j run from 0 to $p-1$ and increase N by $Y[(a - bj^4) \bmod p]$.
- (Adding points with $x = 0$ and $y \neq 0$)
  Increase N by $Y[(-b) \bmod p]$.
- (Adding points with $x = y = 0$)
  Increase N by $(Y[0] - 1)/(p-1)$.
- Return N as the number of all $\mathbb{F}_p$-valued points on $V^e_{a,b}$.

Algorithm to compute Peyre's constant III

Remarks

- For the running-time, step 3 is dominant. Therefore, the running-time of the algorithm is $O(p \log p)$.

Algorithm to compute Peyre's constant III

Remarks

- For the running-time, step 3 is dominant. Therefore, the running-time of the algorithm is $O(p \log p)$.
- To count, for fixed e and p, $\mathbb{F}_p$-rational points on $V^e_{a,b}$ with varying a and b, one needs to execute the first four steps only once. Afterwards, one may perform steps 5 through 9 for all pairs (a, b) of elements from a system of representatives for $\mathbb{F}_p^*/(\mathbb{F}_p^*)^e$ (i.e. at most e^2 times). Note that steps 5 through 9 alone are of complexity $O(p)$.

Algorithm to compute Peyre's constant III

Remarks

- For the running-time, step 3 is dominant. Therefore, the running-time of the algorithm is $O(p \log p)$.
- To count, for fixed e and p, $\mathbb{F}_p$-rational points on $V^e_{a,b}$ with varying a and b, one needs to execute the first four steps only once. Afterwards, one may perform steps 5 through 9 for all pairs (a, b) of elements from a system of representatives for $\mathbb{F}_p^*/(\mathbb{F}_p^*)^e$ (i.e. at most e^2 times). Note that steps 5 through 9 alone are of complexity $O(p)$.
- For $p \equiv 2 \pmod 3$, one has $\#V^3_{a,b}(\mathbb{F}_p) = p^3 + p^2 + p + 1$.
  Analogously, for $p \equiv 3 \pmod 4$, $\#V^4_{a,b}(\mathbb{F}_p) = p^3 + p^2 + p + 1$.

Algorithm to compute Peyre's constant III

Remarks

- For the running-time, step 3 is dominant. Therefore, the running-time of the algorithm is $O(p \log p)$.
- To count, for fixed e and p, $\mathbb{F}_p$-rational points on $V^e_{a,b}$ with varying a and b, one needs to execute the first four steps only once. Afterwards, one may perform steps 5 through 9 for all pairs (a, b) of elements from a system of representatives for $\mathbb{F}_p^*/(\mathbb{F}_p^*)^e$ (i.e. at most e^2 times). Note that steps 5 through 9 alone are of complexity $O(p)$.
- For $p \equiv 2 \pmod 3$, one has $\#V^3_{a,b}(\mathbb{F}_p) = p^3 + p^2 + p + 1$. Analogously, for $p \equiv 3 \pmod 4$, $\#V^4_{a,b}(\mathbb{F}_p) = p^3 + p^2 + p + 1$.
- We ran this algorithm for all primes $p \leq 10^6$ (such that $p \equiv 1 \pmod 3$ and $p \equiv 1 \pmod 4$, respectively,) and stored the cardinalities in a file. This took several days of CPU time.

Algorithm to compute Peyre's constant IV

Examples

- $$x^4 = y^4 + z^4 + v^4 + w^4$$
defines a smooth quartic threefold V in $\mathbb{F}_p$, $p = 269\,117$. We find
$$\#V(\mathbb{F}_p) = p^3 + p^2 + p + 1 + 7\,028p.$$
- $$11x^4 = 13y^4 + z^4 + v^4 + w^4$$
defines a smooth quartic threefold V in $\mathbb{F}_p$, $p = 269\,089$. We find
$$\#V(\mathbb{F}_p) = p^3 + p^2 + p + 1 - 840p.$$

Note that both examples are within the Weil bound which says $\#V(\mathbb{F}_p) = p^3 + p^2 + p + 1 + C$ with $|C| \leq 60p^{3/2}$ in the case of a smooth quartic threefold.

Algorithm to compute Peyre's constant V

Algorithm (Compute an approximate value for $\tau^3_{a,b,fin}$ ($\tau^4_{a,b,fin}$))

- Let p run over all prime numbers such that $p \equiv 2 \pmod 3$ ($p \equiv 3 \pmod 4$) and $p \leq N$ and calculate the product of all values of $(1 - 1/p^4)$.

Algorithm to compute Peyre's constant V

Algorithm (Compute an approximate value for $\tau^3_{a,b,fin}$ ($\tau^4_{a,b,fin}$))

- Let p run over all prime numbers such that $p \equiv 2 \pmod 3$ ($p \equiv 3 \pmod 4$) and $p \leq N$ and calculate the product of all values of $(1 - 1/p^4)$.
- Compute the factor corresponding to $p = 3$ ($p = 2$).

Algorithm to compute Peyre's constant V

Algorithm (Compute an approximate value for $\tau^3_{a,b,fin}$ ($\tau^4_{a,b,fin}$))

- Let p run over all prime numbers such that $p \equiv 2 \pmod 3$ ($p \equiv 3 \pmod 4$) and $p \leq N$ and calculate the product of all values of $(1 - 1/p^4)$.
- Compute the factor corresponding to $p = 3$ ($p = 2$).
- Let p run over all prime numbers such that $p \equiv 1 \pmod 3$ ($p \equiv 1 \pmod 4$) and $p \leq N$. If $p|ab$ then start a separate function for the case of bad reduction.
  Otherwise, compute the e-th power residue-symbols of a and b and look up the precomputed factor for this $\mathbb{F}_p$-isomorphism class of varieties in the list.

Algorithm to compute Peyre's constant V

Algorithm (Compute an approximate value for $\tau^3_{a,b,fin}$ ($\tau^4_{a,b,fin}$))

- Let p run over all prime numbers such that $p \equiv 2 \pmod 3$ ($p \equiv 3 \pmod 4$) and $p \leq N$ and calculate the product of all values of $(1 - 1/p^4)$.
- Compute the factor corresponding to $p = 3$ ($p = 2$).
- Let p run over all prime numbers such that $p \equiv 1 \pmod 3$ ($p \equiv 1 \pmod 4$) and $p \leq N$. If $p|ab$ then start a separate function for the case of bad reduction.
  Otherwise, compute the e-th power residue-symbols of a and b and look up the precomputed factor for this $\mathbb{F}_p$-isomorphism class of varieties in the list.
- Multiply the two products from steps i) and iii) and the factor from step ii) with each other. Correct the product by taking the bad primes $p \equiv 2 \pmod 3$ ($p \equiv 3 \pmod 4$) into consideration.

Investigation of the cubic threefolds I

We determined all $\mathbb{Q}$-rational points of height less than 5 000 on the cubic threefolds $V^3_{a,b}$ given by

$$ax^3 = by^3 + z^3 + v^3 + w^3$$

for $a, b = 1, \ldots, 100$ and $b \leq a$.

Points lying on a $\mathbb{Q}$-rational line in $V_{a,b}$ were excluded from the count. The smallest number of points found is 3 930 278 for $(a, b) = (98, 95)$. The largest numbers of points are 332 137 752 for $(a, b) = (7, 1)$ and 355 689 300 in the case that $a = 1$ and $b = 1$.

On the other hand, for each threefold $V^3_{a,b}$ where $a, b = 1, \ldots, 100$ and $b + 3 \leq a$, we calculated the number of points expected (according to Manin-Peyre) and the quotients

$$\#\{\text{ points of height} < B \text{ found }\} \,/\, \#\{\text{ points of height} < B \text{ expected }\}.$$

Let us visualize the quotients by two histograms.

Investigation of the cubic threefolds II

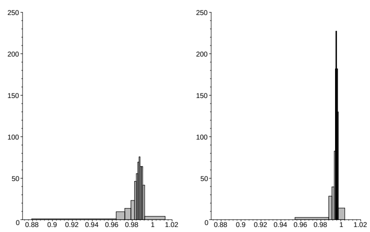

Figure: Distribution of the quotients for $B = 1\,000$ and $B = 5\,000$.

Investigation of the cubic threefolds III

Table: Parameters of the distribution in the cubic case

	$B = 1\,000$	$B = 2\,000$	$B = 5\,000$
mean value	0.981 79	0.988 54	0.993 83
standard deviation	0.012 74	0.008 23	0.004 55

Investigation of the quartic threefolds I

We determined all $\mathbb{Q}$-rational points of height less than 100 000 on the quartic threefolds $V^4_{a,b}$ given by

$$ax^4 = by^4 + z^4 + v^4 + w^4$$

for $a, b = 1, \ldots, 100$.

It turns out that on 5 015 of these varieties, there are no $\mathbb{Q}$-rational points occurring at all as the equation is unsolvable in $\mathbb{Q}_p$ for $p = 2$, 5, or 29. In this situation, Manin's conjecture is true, trivially.

For the remaining varieties, the points lying on a known $\mathbb{Q}$-rational conic in $V_{a,b}$ were excluded from the count.

Investigation of the quartic threefolds II

Table: Numbers of points of height $< 100\,000$ on the quartics.

a	b	# points	# not on conic	# expected (by Manin-Peyre)
29	29	2	2	135
58	87	288	288	272
58	58	290	290	388
87	87	386	386	357
⋮	⋮	⋮	⋮	⋮
34	1	9 938 976	5 691 456	5 673 000
17	64	5 708 664	5 708 664	5 643 000
1	14	7 205 502	6 361 638	6 483 000
3	1	12 657 056	7 439 616	7 526 000

Investigation of the quartic threefolds III

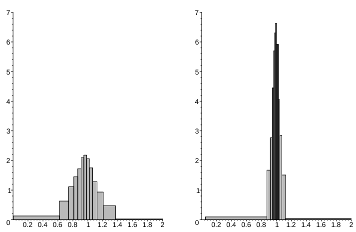

Figure: Distribution of the quotients for $B = 1\,000$ and $B = 10\,000$.

Investigation of the quartic threefolds IV

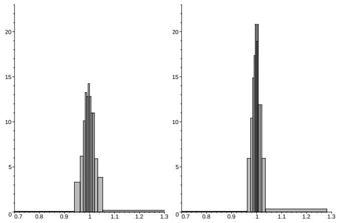

Figure: Distribution of the quotients for $B = 50\,000$ and $B = 100\,000$.

Investigation of the quartic threefolds V

Table: Parameters of the distribution in the quartic case

	$B = 1\,000$	$B = 10\,000$	$B = 100\,000$
mean value	0.9853	0.9957	0.9982
standard deviation	0.3159	0.1130	0.0372

Remark

In the cubic case, the standard deviation was by far smaller than in the case of the quartics. This is not very surprising as on a cubic there tend to be much more rational points than on a quartic. Thus, in the case of the cubic the sample is more reliable.

Investigation of the quartic threefolds VI

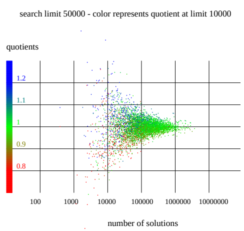

Figure: number of solutions and quotients for $B = 50\,000$.

Summary

Summary

- *To search systematically for solutions of Diophantine equations like* $x^4 + 2y^4 = z^4 + 4w^4$ *or* $7x^3 = 11y^3 + z^3 + v^3 + w^3$ *(*$n \geq 4$ *variables), there are faster ways than the obvious* $(n-1)$*-times iterated loop. (Essentially in* $O(B^{\lceil n/2 \rceil})$ *steps).*

Summary

Summary

- *To search systematically for solutions of Diophantine equations like $x^4 + 2y^4 = z^4 + 4w^4$ or $7x^3 = 11y^3 + z^3 + v^3 + w^3$ ($n \geq 4$ variables), there are faster ways than the obvious $(n-1)$-times iterated loop. (Essentially in $O(B^{\lceil n/2 \rceil})$ steps).*
- *To count solutions over $\mathbb{F}_p$ (not determining all of them) is even faster ($O(np \log p)$ steps).*

Summary

Summary

- *To search systematically for solutions of Diophantine equations like $x^4 + 2y^4 = z^4 + 4w^4$ or $7x^3 = 11y^3 + z^3 + v^3 + w^3$ ($n \geq 4$ variables), there are faster ways than the obvious $(n-1)$-times iterated loop. (Essentially in $O(B^{\lceil n/2 \rceil})$ steps).*
- *To count solutions over $\mathbb{F}_p$ (not determining all of them) is even faster ($O(np \log p)$ steps).*
- *These two observations together may be used to test Manin's conjecture, numerically.*

Summary

Summary

- *To search systematically for solutions of Diophantine equations like $x^4 + 2y^4 = z^4 + 4w^4$ or $7x^3 = 11y^3 + z^3 + v^3 + w^3$ ($n \geq 4$ variables), there are faster ways than the obvious $(n-1)$-times iterated loop. (Essentially in $O(B^{\lceil n/2 \rceil})$ steps).*
- *To count solutions over $\mathbb{F}_p$ (not determining all of them) is even faster ($O(np \log p)$ steps).*
- *These two observations together may be used to test Manin's conjecture, numerically.*

Remark (Conclusion)

The results suggest that Manin's conjecture should be true for the two families of threefolds considered.