Defining Multiplication on Indices of Points on an Elliptic Curve and Defining $\mathbb{Z}$ Using One Universal Quantifier

Alexandra Shlapentokh

Department of Mathematics,  
East Carolina University,  
Greenville, North Carolina, USA

February, 2009
You can’t always get what you want
You can’t always get what you want
You can’t always get what you want
But if you try sometimes you might find
You get what you need

Rolling Stones
Table of Contents

1 Prologue
2 Complications
3 Big and Small
4 Matters of the First Order or Back to the Future
5 Something New
6 Highlights
   - Index Multiplication
   - Defining $\mathbb{Z}$
   - Density
7 Consequences
8 Epilogue
Hilbert’s Question about Polynomial Equations

Is there an algorithm which can determine whether or not an arbitrary polynomial equation in several variables has solutions in integers? Using modern terms one can ask if there exists a program taking coefficients of a polynomial equation as input and producing “yes” or “no” answer to the question “Are there integer solutions?”.

This problem became known as Hilbert’s Tenth Problem
This question was answered negatively (with the final piece in place in 1970) in the work of Martin Davis, Hilary Putnam, Julia Robinson and Yuri Matiyasevich. Actually a much stronger result was proved. It was shown that the recursively enumerable subsets of \( \mathbb{Z} \) are the same as the Diophantine subsets of \( \mathbb{Z} \).
Diophantine Sets
If $R$ is a ring and $m \in \mathbb{Z}_{>0}$, then a subset $A \subset R^m$ is called Diophantine over $R$ if there exists a polynomial $p(T_1, \ldots, T_m, X_1, \ldots, X_k)$ with $R$-coefficients such that for any element $(t_1, \ldots, t_m) \in R^m$ we have that
\[
\exists x_1, \ldots, x_k \in \mathbb{Z} : p(t_1, \ldots, t_m, x_1, \ldots, x_k) = 0
\]
\[\uparrow\downarrow\]
$(t_1, \ldots, t_m) \in A$.

In this case we call $p(T_1, \ldots, T_m, X_1, \ldots, X_k)$ a Diophantine definition of $A$ over $\mathbb{Z}$.

Lemma
If $R$ is an integral domain with a not algebraically closed fraction field, then intersections and unions of Diophantine sets are Diophantine.

Lemma (Replacing Finitely Many by One)
If $R$ is as above and is recursive, then any finite system of equations over $R$ can be effectively replaced by a single polynomial equation over $R$ with the identical $R$-solution set.
A General Question

A Question about an Arbitrary Recursive Ring $R$

Is there an algorithm, which if given an arbitrary polynomial equation in several variables with coefficients in $R$, can determine whether this equation has solutions in $R$?

The most prominent open questions are probably the decidability of HTP for $R = \mathbb{Q}$ and $R$ equal to the ring of integers of an arbitrary number field.
Using Diophantine Definitions to Solve the Problem

Lemma

Let $R$ be a recursive ring containing $\mathbb{Z}$ and such that $\mathbb{Z}$ has a Diophantine definition $p(T, \bar{X})$ over $R$. Then HTP is not decidable over $R$.

Proof.

Let $h(T_1, \ldots, T_l)$ be a polynomial with rational integer coefficients and consider the following system of equations.

$$
\begin{align*}
  h(T_1, \ldots, T_l) &= 0 \\
  p(T_1, \bar{X}_1) &= 0 \\
  & \quad \vdots \\
  p(T_l, \bar{X}_l) &= 0 
\end{align*}
$$

(1)

It is easy to see that $h(T_1, \ldots, T_l) = 0$ has solutions in $\mathbb{Z}$ iff (1) has solutions in $R$. Thus if HTP is decidable over $R$, it is decidable over $\mathbb{Z}$. \qed
The Plan

So to show that HTP is undecidable over $\mathbb{Q}$ we just need to construct a Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}!!!
A Conjecture of Barry Mazur

The Conjecture on the Topology of Rational Points

Let $V$ be any variety over $\mathbb{Q}$. Then the topological closure of $V(\mathbb{Q})$ in $V(\mathbb{R})$ possesses at most a finite number of connected components.

A Nasty Consequence

There is no Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$.

Actually if the conjecture is true, no infinite and discrete (in the archimedean topology) set has a Diophantine definition over $\mathbb{Q}$.
Another Plan: Diophantine Models

What is a Diophantine Model of $\mathbb{Z}$?

Let $R$ be a recursive ring whose fraction field is not algebraically closed and let $\phi : \mathbb{Z} \rightarrow R^k$ be a recursive injection mapping Diophantine sets of $\mathbb{Z}$ to Diophantine sets of $R^k$. Then $\phi$ is called a Diophantine model of $\mathbb{Z}$ over $R$. 


Another Plan: Diophantine Models

Sending Diophantine Sets to Diophantine Sets Makes the Map Recursive

Actually the recursiveness of the map will follow from the fact that the \( \phi \)-image of the graph of addition is Diophantine. Indeed, if the \( \phi \)-image of the graph of addition is Diophantine, it is recursively enumerable. So we have an effective listing of the set

\[
D_+ = \{(\phi(m), \phi(n), \phi(m + n)), m, n \in \mathbb{Z}\}.
\]

Assume we have computed \( \phi(k - 1) \). Now start listing \( D_+ \) until we come across a triple whose first two entries are \( \phi(k - 1) \) and \( \phi(1) \). Then third element of the triple must be \( \phi(k) \).

Making Addition and Multiplication Diophantine is Enough

It is enough to require that the \( \phi \)-images of the graphs of \( \mathbb{Z} \)-addition and \( \mathbb{Z} \)-multiplication are Diophantine over \( R \).
Defining Multiplication on Indices of Points on an Elliptic Curve and Defining $\mathbb{Z}$ Using One Universal Quantifier

Complications

Diophantine Model of $\mathbb{Z}$ Implies Undecidability

If $R$ has a Diophantine model of $\mathbb{Z}$, then $R$ has undecidable Diophantine sets. Indeed, let $A \subset \mathbb{Z}$ be an undecidable Diophantine set. Suppose we want to determine whether an integer $n \in A$. Instead of answering this question directly we can ask whether $\phi(n) \in \phi(A)$. By assumption $\phi(n)$ is algorithmically computable. So if $\phi(A)$ is a computable subset of $R$, we have a contradiction.

So all we need is a Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$!!!
An Old Plan

Using Elliptic Curves of Rank One

Let $E$ be a rank one elliptic curve over $\mathbb{Q}$. To simplify the situation, assume the torsion group is trivial. Let $P$ be a generator. Consider a map sending $n \neq 0$ to $[n]P$. It is easy to see that under this map the graph of addition is Diophantine. Unfortunately, it is not clear what happens to the graph of multiplication.
A Theorem of Cornelissen and Zahidi

Theorem

If Mazur’s conjecture on topology of rational points holds, then there is no Diophantine model of \( \mathbb{Z} \) over \( \mathbb{Q} \).
A Ring in between

Let $K$ be a number field and let $\mathcal{W}$ be a set of primes of $K$. Let $O_{K,\mathcal{W}}$ be the following subring of $K$.

$$\{x \in K : \text{ord}_p x \geq 0 \ \forall p \notin \mathcal{W}\}$$

If $\mathcal{W} = \emptyset$, then $O_{K,\mathcal{W}} = O_K$ – the ring of integers of $K$. If $\mathcal{W}$ contains all the primes of $K$, then $O_{K,\mathcal{W}} = K$. If $\mathcal{W}$ is finite, we call the ring small (or the ring of $\mathcal{W}$-integers). If $\mathcal{W}$ is infinite, we call the ring large, and if the natural density of $\mathcal{W}$ is one, we call the ring “very large”.
Defining Multiplication on Indices of Points on an Elliptic Curve and Defining $\mathbb{Z}$ Using One Universal Quantifier

Big and Small

Diophantine Properties of Small Rings

**Lemma**

The set of non-zero elements of a big or a small ring is Diophantine over the ring.

**Corollary**

Let $R$ be a big or a small ring. Let $A \subset \mathbb{Q}^m$ be Diophantine over $\mathbb{Q}$. Then $A \cap R^m$ is Diophantine over $R$.

**Theorem (Julia Robinson)**

If $K$ is a number field and $\mathfrak{p}$ is a finite prime of $K$, then the valuation ring of $\mathfrak{p}$ is Diophantine over $K$.

**Corollary**

If $K$ is a number field and $\mathbb{Z}$ is Diophantine over $O_K$, then $\mathbb{Z}$ is Diophantine over any small subring of $K$. 
The Rings of Integers of Number Fields

Theorem

\( \mathbb{Z} \) is Diophantine and HTP is unsolvable over the rings of integers of the following fields:

- Extensions of degree 4, totally real number fields and their extensions of degree 2. (Denef, 1980 & Denef, Lipshitz, 1978)
  Note that these fields include all Abelian extensions.

- Number fields with exactly one pair of non-real embeddings (Pheidas, S. 1988)

- Any number field \( K \) such that there exists an elliptic curve \( E \) of positive rank defined over \( \mathbb{Q} \) with \( [E(K) : E(\mathbb{Q})] < \infty \). (Poonen, S. 2003)

- Any number field \( K \) such that there exists an elliptic curve of rank 1 over \( K \) and an Abelian variety over \( \mathbb{Q} \) keeping its rank over \( K \). (Cornelissen, Pheidas, Zahidi, 2005)
Theorem

Let $K$ be a number field satisfying one of the following conditions:

- $K$ is a totally real field.
- $K$ is an extension of degree 2 of a totally real field.
- There exists an elliptic curve $E$ defined over $\mathbb{Q}$ such that $[E(K) : E(\mathbb{Q})] < \infty$.

Let $\varepsilon > 0$ be given. Then there exists a set $S$ of non-archimedean primes of $K$ such that

- The natural density of $S$ is greater than $1 - \frac{1}{[K : \mathbb{Q}]} - \varepsilon$.
- $\mathbb{Z}$ is Diophantine over $O_{K,S}$.
- $\text{HTP}$ is unsolvable over $O_{K,S}$.

Theorem

Let $K$ be a number field with a rank one elliptic curve. Then there exist recursive sets of $K$-primes $T_1$ and $T_2$, both of natural density zero and with an empty intersection, such that for any set $S$ of primes of $K$ containing $T_1$ and avoiding $T_2$, Hilbert’s Tenth Problem is unsolvable over $O_{K,S}$. (Poonen 2003: the case of $K = \mathbb{Q}$; Poonen, S. 2005: the general case)
Remark

Over very large subrings the undecidability of HTP was shown by constructing a model of \( \mathbb{Z} \): over \( \mathbb{Q} \) it was accomplished by approximating integers and over number fields by constructing a “model of a model” of \( \mathbb{Z} \). In neither case was the multiplication on indices shown to be Diophantine over the rings.
## Previous First-Order Definability Results

<table>
<thead>
<tr>
<th>Theorem (Julia Robinson, 1949 and 1959)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Z}$ is first-order definable over any number field $K$.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Theorem (Cornelissen and Zahidi, 2007)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assuming a conjecture concerning elliptic curves over $\mathbb{Q}$, there exists a first-order model of $\mathbb{Z}$ over $\mathbb{Q}$ using just one universal quantifier.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Theorem (Poonen, 2008)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- For any number field $K$, the ring of integers of $K$ is first-order definable over $K$ using just two universal quantifiers.</td>
</tr>
<tr>
<td>- For any $\varepsilon &gt; 0$, there exists a set of rational primes $\mathcal{W}<em>Q$ of natural density greater than $1 - \varepsilon$ such that $\mathbb{Z}$ is definable using just one quantifier over $O</em>{Q,\mathcal{W}_Q}$.</td>
</tr>
</tbody>
</table>
Defining Multiplication on Indices of Points on an Elliptic Curve and Defining $\mathbb{Z}$ Using One Universal Quantifier

Matters of the First Order or Back to the Future

Previous First-Order Definability Results

Theorem (Cornelissen and S., 2008)

Let $K \neq \mathbb{Q}$ be a number field of one of the following types:

- $K$ is totally real;
- $K$ is an extension of degree two of a totally real number field;
- There exists an elliptic curve defined over $\mathbb{Q}$ and of positive rank over $\mathbb{Q}$ such that this curve preserves its rank over $K$;

Then for every $\varepsilon > 0$, there exists a set of primes $\mathcal{W}_K$ of $K$ of natural density exceeding $1 - \varepsilon$, such that $\mathbb{Z}$ can be defined as a subset of $O_K, \mathcal{W}_K$ by a formula with only one $\forall$-quantifier.
Previous First-Order Definability Results

Theorem (Cornelissen and S., 2008)

Let $K$ be a number field, including $\mathbb{Q}$. Assume there exists an elliptic curve defined over $K$ of rank 1 over $K$. Then for every $\varepsilon > 0$, there exists a set of primes $\mathcal{W}_K$ of $K$ of natural density exceeding $1 - \varepsilon$, such that $\mathbb{Z}$ can be defined as a subset of $O_{K,\mathcal{W}_K}$ by a formula with only two $\forall$-quantifiers.

Remark

Observe that the fact that $\mathbb{Z}$ can be defined over a number field using two quantifiers does not imply directly that $\mathbb{Z}$ can be defined over a subring of the field using two quantifiers: in translating a definition over the field to a ring, one has to represent an algebraic number as a ratio of two elements of the ring. Thus a “mechanical” translation of Poonen’s result over number fields would produce a definition with four universal quantifiers.
New Results: Defining Multiplication of Indices

**Theorem**

Let $K$ be a number field. Let $E$ be an elliptic curve defined and of rank one over $K$. Let $P$ be a generator of $E(K)$ modulo the torsion subgroup, and fix an affine Weierstrass equation for $E$ of the form $y^2 = x^3 + ax + b$, with $a, b \in O_K$, where $O_K$ is the ring of integers of $K$. Let $(x_n, y_n)$ be the coordinates of $[n]P$ with $n \neq 0$ derived from this Weierstrass equation. Then there exists a set of $K$-primes $\mathcal{W}_K$ of natural density one, and a positive integer $m_0$ such that the following set $\Pi \subset O_{K,\mathcal{W}_K}^{12}$ is Diophantine over $O_{K,\mathcal{W}_K}$.

$$(U_1, U_2, U_3, X_1, X_2, X_3, V_1, V_2, V_3, Y_1, Y_2, Y_3) \in \Pi \iff \exists \text{ unique } k_1, k_2, k_3 \in \mathbb{Z}_{\neq 0} \text{ such that }$$

$$\left(\frac{U_i}{V_i}, \frac{X_i}{V_i}\right) = (x_{m_0k_i}, y_{m_0k_i}), \text{ for } i = 1, 2, 3, \text{ and } k_3 = k_1k_2.$$
New Results: Defining $\mathbb{Z}$ Using Just One Universal Quantifier

**Theorem**

Let $K$ be a number field. Let $E$ be an elliptic curve defined and of rank one over $K$. Then there exists a set $\mathcal{W}_K$ of primes of $K$ of natural density one such that $\mathbb{Z}$ is first-order definable over $O_{K, \mathcal{W}_K}$ using just one universal quantifier.
Proof Overview for Index Multiplication

Simplifying Assumptions

- We set $K = \mathbb{Q}$ and assume $E_{\text{tor}}(\mathbb{Q})$ is trivial.

- For a generator $P$ of $E(\mathbb{Q})$, for $n \in \mathbb{Z} \neq 0$, we let $[n]P = (x_n, y_n) = \left( \frac{U_n}{V_n}, \frac{X_n}{Y_n} \right) \in \mathbb{Q}^2$, where $V_n > 0$, $Y_n > 0$, $(U_n, V_n) = 1$, $(X_n, Y_n) = 1$.

- We assume that every non-trivial multiple of the generator $P$ has an odd primitive divisor, i.e. for every $n \in \mathbb{Z} \neq 0, \pm 1$ there exists a prime $p \neq 2$ such that $p | V_n$ but $p \nmid V_m$ for any $m$ with $|m| < |n|$.

- Coordinates of $P$ are integers.
Defining Multiplication on Indices of Points on an Elliptic Curve and Defining \( \mathbb{Z} \) Using One Universal Quantifier

**Highlights**

**Index Multiplication**

**Proof Overview for Index Multiplication**

**Properties of Denominators**

- Assuming \( n, m \in \mathbb{Z} \neq 0 \), we have that \( n|m \iff V_n|V_m \).
- The primes dividing \( V_{(m,n)} \) are the same as the primes dividing \( (V_m, V_n) \). Thus, \( (m, n) = 1 \iff (V_m, V_n) = 1 \).
- If \( p \neq q \) are primes, and \( \text{ord}_p V_n < 0 \) then \( \text{ord}_p V_{qn} = \text{ord}_p V_n \) while \( \text{ord}_p V_{pn} > \text{ord}_p V_n \).
Defining Multiplication on Indices of Points on an Elliptic Curve and Defining $\mathbb{Z}$ Using One Universal Quantifier

Highlights

Index Multiplication

Proof Overview for Index Multiplication

What Not to Invert

$\mathcal{V} = \{\text{The largest odd primitive prime factor } p_{\ell^i} \text{ of } V_{\ell^i}\}$, where $\ell$ runs through all the prime numbers and $i \in \mathbb{Z}_{>0}$.

What to Invert

ALL THE OTHER PRIMES

Divisibility in the Bigger Ring

Let $R \subset \mathbb{Q}$ be the resulting ring. Observe that we still have for $n, m \in \mathbb{Z}_{\neq 0}$ the fact that $n|m \iff V_n |_R V_m$. (Here “$|_R$” signifies division in $R$.) It is enough to show that $V_{\ell^i} |_R V_n \iff \ell^i | n$.

Indeed, if $V_{\ell^i} |_R V_n$, then $p_{\ell^i} | V_n$, and therefore, $p_{\ell^i}$ divides $(V_n, V_{\ell^i}) = V_{(n, \ell^i)} = V_{\ell^j}$, where $0 \leq j \leq i$. But if $0 \leq j < i$, then $p_{\ell^i} \nmid V_{\ell^j}$ by definition of $p_{\ell^i}$. Conversely, if $\ell^i | n$, then $V_{\ell^i} | V_n \Rightarrow V_{\ell^i} |_R V_n$. 
**Indices We Can Multiply Directly**

**Lemma**

If $m, n \in \mathbb{Z}_{\neq 0}$ and $(m, n) = 1,$ $(n, V_m)_R = 1,$ $(m, V_n)_R = 1$ then 
$V_m V_n |_R V_{mn}$ and $V_{mn} |_R V_m V_n.$

**Remark**

$(V_m, V_n)_R = 1 \iff (V_m, V_n) = 1 \iff (m, n) = 1.$ (Here $(V_m, V_n)_R = 1$ means $V_m, V_n$ relatively prime in $R$) If a prime $q | (m, n),$ then $p_q | V_m$ and $p_q | V_n$ and $p_q |_R (V_m, V_n).$

**Proof.**

We will consider the case of $m = t$ and $n = q,$ where $t$ and $q$ are prime numbers with $(q, V_t)_R = 1$ and $(t, V_q)_R = 1.$ First of all we have that $V_t | V_{tq}$ and $V_q | V_{tq}$ and $(V_t, V_q)_R = (V_t, V_q) = 1.$ Thus $V_t V_q | V_{tq}.$ In general, $V_{tq} \not| V_t V_q$ but since we inverted all the primes of $V_{tq}$ which do not come from $V_t$ or $V_q$ we have that the only non-inverted primes which divide $V_{tq}$ are $p_q$ and $p_t$ – the primitive divisors of $V_t$ and $V_q.$ Now the conditions $(q, V_t)_R = 1$ and $(t, V_q)_R = 1$ insure that $\text{ord}_{p_t} V_t = \text{ord}_{p_t} V_{qt}$ and $\text{ord}_{p_q} V_q = \text{ord}_{p_q} V_{qt}.$
Indices We Can Multiply Directly

Lemma

For any \( m, n \in \mathbb{Z} \neq 0 \) with \((V_m, V_n)_R = 1\) we have that \( V_m V_n |_R V_k \) and \( V_k |_R V_m V_n \Rightarrow |k| = |mn|\).

Proof.

First \((V_m, V_n)_R = 1\) implies that \((m, n) = 1\). Therefore, we have that \(mn|k\). Next, if for some prime \( \ell \) and some positive integer \( i \) it is the case that \( \ell^i | k \), then \( p_{\ell^i} | V_k \) and consequently \( p_{\ell^i} | V_m \) or \( p_{\ell^i} | V_n \) and thus \( \ell^i | m \) or \( \ell^i | n \). Consequently, \( k | mn \).

Squaring Is Enough

It is enough to define squares: \( \frac{1}{2}((a + b)^2 - a^2 - b^2) = ab \).
Definitions Multiplication on Indices of Points on an Elliptic Curve and Defining \( \mathbb{Z} \) Using One Universal Quantifier

**Highlights**

**Index Multiplication**

**Indices We Cannot Multiply Directly**

**Lemma**

For any even \( k \in \mathbb{Z} \neq 0 \) there exists an \( m \in \mathbb{Z} \neq 0 \) such that \( k \) and \( m \) and \( k + m \) can be multiplied directly.

**Proof.**

Let \( k = 2q \), where \( q \) is a prime number. We are looking for an odd prime number \( t \neq q \) such that \((V_{2q}, t)_R = 1\), \((2q, V_t)_R = 1\), \((V_{2q + t}, 2q)_R = 1\), and \((V_{2q}, 2q + t) = 1\). Suppose we have that \( q = p_\ell^i \) for some prime \( \ell \) and some positive integer \( i \). Then we need to arrange the following:

\[
\begin{align*}
&\quad t \neq p_q \land t \neq 2 \text{ to assure } (V_{2q}, t)_R = 1 \\
&\quad t \neq \ell \text{ to assure } (V_t, 2q)_R = 1. \text{ Note that } 2 \text{ is inverted in our ring.} \\
&\quad 2q + t \not\equiv 0 \mod p_q \land 2q + t \not\equiv 0 \mod p_2 \text{ to assure } (V_{2q}, t + 2q)_R = 1 \\
&\quad 2q + t \not\equiv 0 \mod \ell \text{ to assure } (V_{t+2q}, 2q)_R = 1
\end{align*}
\]

If \( \ell = 2 \), or \( p_2 = q \) or \( \ell = q \), the corresponding equivalencies are automatically true given the first “non-equalities”. Otherwise, since we assumed that all primitive divisors are odd, we can simultaneously solve \( 2q + t \not\equiv 0 \mod \ell, 2q + t \not\equiv 0 \mod p_2 \), and \( 2q + t \not\equiv 0 \mod p_q \).
Defining the Square of the Index

**Lemma**

Let \((U_i, V_i, X_i, Y_i) \in \mathbb{R}^4, i = 1, \ldots, 8\) be such that

\[
(U_i, V_i)_R = 1, (X_i, Y_i)_R = 1, \left(\frac{U_i}{V_i}, \frac{X_i}{Y_i}\right) = (x_{k_i}, y_{k_i}) \in E(\mathbb{Q}), k_i \neq 0 \tag{2}
\]

\[
k_1 \equiv 4 \mod 16; k_2 \equiv 1 \mod 2; k_3 = k_1 + k_2 \tag{3}
\]

\[
(V_1, V_2)_R = (V_1, V_3)_R = 1 \tag{4}
\]

\[
V_1 V_2 \mid_R V_4 \text{ and } V_4 \mid_R V_1 V_2, \tag{5}
\]

\[
V_1 V_3 \mid_R V_5 \text{ and } V_5 \mid_R V_1 V_3 \tag{6}
\]

\[
k_6 = k_5 - k_4; k_6 \equiv 0 \mod 16; k_7 = k_1 - 1; k_8 = k_6 - 1 \tag{7}
\]

\[
V_7 \mid_R V_8, \tag{8}
\]

Then \(k_6 = k_1^2\). Conversely, if \(k_1 \equiv 4 \mod 16\) then there exist

\((U_i, V_i, X_i, Y_i) \in \mathbb{R}^4, i = 2, \ldots, 8\) such that all the equations and conditions above can be satisfied.
Defining Multiplication on Indices of Points on an Elliptic Curve and Defining $\mathbb{Z}$ Using One Universal Quantifier

Highlights

Index Multiplication

Defining the Square of an Index

Proof.

$$(V_1 V_2 | R V_4) \land (V_4 | R V_1 V_2) \land (V_1 V_3 | R V_5) \land (V_5 | R V_1 V_3)$$ imply

$$|k_4| = |k_1 k_2| \quad \text{and} \quad |k_5| = |k_1(k_1 + k_2)|.$$  Thus, $$k_6 = k_5 - k_4 = \pm k_1^2$$ or $$k_6 = \pm (k_1^2 + 2k_1 k_2).$$  Since $$k_1 \equiv 4 \mod 16$$ and $$k_2$$ is odd, $$k_1^2 + 2k_1 k_2 \not\equiv 0 \mod 16$$ which is required for $$k_6$$, and we must conclude that $$k_6 = \pm k_1^2.$$  Finally, if $$k_6 = -k_1^2$$, then $$k_8 = -1 - k_1^2$$ and, consequently, since $$|k_1| \geq 4$$, it is the case that $$k_1 - 1$$ does not divide $$k_8$$, implying $$V_7$$ does not divide $$V_8$$ as required. Thus $$k_6 = k_1^2.$$  

If $$k_1 \equiv 4 \mod 16$$ then we can find a $$k_2 \in \mathbb{Z}_{\text{odd}}$$ so that all the equations are satisfied.
More Properties of Denominators

For any sufficiently large in absolute value $l \in \mathbb{Z}_{\neq 0}$, for any $k \in \mathbb{Z}_{\neq 0}$ we have that the reduced denominator of $x_l$ divides the reduced numerator of
\[
\left( \frac{x_l}{x_{kl}} - k^2 \right)^2 \text{ in } \mathbb{Z}.
\]

For any $n \in \mathbb{Z}_{>0}$ there exists $l \in \mathbb{Z}_{>0}$ such that $n$ divides the reduced denominator of $x_l$ in $\mathbb{Z}$. 
Let \( z \in R \) be such that \( \exists k \in \mathbb{Z} \neq 0 \forall b \in R \exists i, j \in \mathbb{Z} \neq 0 \) satisfying the equations below.

\[
b^2 \text{ divides the reduced denominator of } x_i \text{ in our ring. } \quad (9)
\]

\[
 j = ik \quad (10)
\]

The reduced denominator of \( x_i \)

divides the reduced numerator of \( (z - \frac{x_i}{x_j})^2 \) in our ring. \quad (11)

(Here, as above, \( x_k, x_i, x_j \) are the \( x \)-coordinates of \([k]P\), \([i]P\) and \([j]P\) respectively.) Then \( z \in \mathbb{Z} \).

Conversely, if \( z \) above is a square of a non-zero integer, then we can find a \( k \in \mathbb{Z} \neq 0 \) such that for every \( b \) in our big ring there exist \( i \) and \( j \) so that equations above are satisfied.
Highlights

Defining $Z$

Proof.

From equations we conclude that in our ring $b$ divides the reduced numerator of \( \left( \frac{x_i}{x_j} - k^2 \right) \) as well as the reduced numerator of \((z - \frac{x_i}{x_j}) = (z - \frac{x_i}{x_{ik}})\). Thus, $b$ divides the reduced numerator of $z - k^2$. Since we can pick $b$ to be divisible by $q^m$, where $q$ is a prime which is not inverted in our ring and $m$ is an arbitrary positive integer, the only way the divisibility condition can hold is for $z = k^2$.

Assume now that $z = k^2$ where $k \in \mathbb{Z} \neq 0$. Let $b$ be any rational number in our ring. Let $i > 0$ be such that $b^2$ divides the reduced denominator of $x_i$ and $i$ is sufficiently large so that the relevant congruence holds for $l = j = ik$. Then all the equations will be satisfied.
### The Density of the Set of the Largest Primitive Divisors

**Notation**

Let $K$ be a number field, let $E$ be an elliptic curve of positive rank defined over $K$. Let $P \in E(K)$ be a point of infinite order. Let $p_n$ be a primitive divisor of the largest norm of $[n]P$.

**Theorem (Poonen)**

Let $A = \{p_{\ell} : \ell \text{ a rational prime number} \}$. Then the natural density of $A$ is 0.

**Proposition**

Let $B = \{p_{\ell^i} : \ell \text{ a rational prime number}, i \in \mathbb{Z}_{>1} \}$. Then the natural density of $B$ is 0.
Defining Multiplication on Indices of Points on an Elliptic Curve and Defining $\mathbb{Z}$ Using One Universal Quantifier

Consequences

A Class Diophantine Model

**Definition**

Let $R$ be a countable recursive ring, let $D \subset R^k$, $k \in \mathbb{Z}_{>0}$ be a Diophantine subset, and let $\approx$ be a (Diophantine) equivalence relation on $D$, i.e. assume that the set $\{(\bar{x}, \bar{y}) : \bar{x}, \bar{y} \in D, \bar{x} \approx \bar{y}\}$ is a Diophantine subset of $R^{2k}$. Let $D = \bigcup_{i \in \mathbb{Z}} D_i$, where $D_i$ is an equivalence class of $\approx$, and let $\phi : \mathbb{Z} \longrightarrow \{D_i, i \in \mathbb{Z}\}$ be defined by $\phi(i) = D_i$. Finally assume that the sets

$$Plus = \{ (\bar{x}, \bar{y}, \bar{z}) : \bar{x} \in D_i, \bar{y} \in D_j, \bar{z} \in D_{i+j} \}$$

and

$$Times = \{ (\bar{x}, \bar{y}, \bar{z}) : \bar{x} \in D_i, \bar{y} \in D_j, \bar{z} \in D_{ij} \}$$

are Diophantine over $R$.

Then we will say that $R$ has a class Diophantine model of $\mathbb{Z}$. 
A Class Diophantine Model of $\mathbb{Z}$

**Corollary**

In the notation above, for $n \neq 0$ let

$$\phi(n) = [(U_{m_0n}, X_{m_0n}, V_{m_0n}, Y_{m_0n})],$$

the equivalence class of

$$(U_{m_0n}, X_{m_0n}, V_{m_0n}, Y_{m_0n})$$

under the equivalence relation described below, where $U_{m_0n}, X_{m_0n}, V_{m_0n}, Y_{m_0n} \in O_K, \mathbb{W}_K, V_{m_0n} Y_{m_0n} \neq 0,$

and $(x_{m_0n}, y_{m_0n}) = \left( \frac{U_{m_0n}}{V_{m_0n}}, \frac{X_{m_0n}}{Y_{m_0n}} \right)$. Let $\phi(0) = \{(0, 0, 0, 0)\}$.

Then $\phi$ is a class Diophantine model of $\mathbb{Z}$. (Here if $V \hat{V} \hat{Y} Y \neq 0$

we set $(U, X, V, Y) \approx (\hat{U}, \hat{X}, \hat{V}, \hat{Y})$ if and only if $\frac{\hat{U}}{\hat{V}} = \frac{U}{V}$ and

$$\frac{\hat{X}}{\hat{Y}} = \frac{X}{Y}.$$
Defining Multiplication on Indices of Points on an Elliptic Curve and Defining $\mathbb{Z}$ Using One Universal Quantifier

Epilogue