HTP over Algebraic Extensions of $\mathbb{Q}$: Normforms vs. Elliptic Curves

Alexandra Shlapentokh

East Carolina University

Number Theory and Computability, ICMS, June 2007
A Talk in Two Rounds

Round I: Normforms
Today

Round II: Elliptic Curves
Later
Table of Contents

1 A Brief History of Diophantine Undecidability over Algebraic Extensions of $\mathbb{Q}$
   - The Original Problem
   - Extensions to Number Fields
   - Extensions to Infinite Algebraic Extensions of $\mathbb{Q}$.

2 How Things are Done
   - Diophantine Sets, Definitions and Models

3 Constructing Diophantine Definitions
   - Vertical Methods
   - Norm Equations over Rings of Integers
   - Norm Equations over Big Rings
   - Norm Equations and Bounds
   - The Final Score
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?

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 Matijasevich.
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 $R$?

Arguably, the most important open problems in the area concern the Diophantine status of the ring of integers of an arbitrary number field and the Diophantine status of $\mathbb{Q}$. 
The Rings of Integers of Number Fields.

Theorem

HTP is unsolvable over the rings of integers of the following fields:

- Extensions of degree 4, totally real number fields (i.e. finite extensions of \( \mathbb{Q} \) all of whose embeddings into \( \mathbb{C} \) are real) 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)
A prime of a number field is a prime ideal of the rings of integers of the field or, alternatively, a non-archimedean valuation of a field.

A Ring in the Middle of a Number Field $K$

Let $\mathcal{V}$ be a set of primes of a number field $K$. Then define

$$O_{K,\mathcal{V}} = \{x \in K : \text{ord}_p x \geq 0 \ \forall p \notin \mathcal{V}\}.$$ 

If $\mathcal{V} = \emptyset$, then $O_{K,\mathcal{V}} = O_K$ – the ring of integers of $K$. If $\mathcal{V}$ contains all the primes of $K$, then $O_{K,\mathcal{V}} = K$. If $\mathcal{V}$ is finite, we call the ring small. If $\mathcal{V}$ is infinite, we call the ring big or large. Finally, if the natural density of $\mathcal{V}$ is equal to 1, we call the ring very large.
HTP over Small Subrings of Number Fields

Theorem

HTP is unsolvable over small subrings of \( \mathbb{Q} \).

Theorem

For any number field \( K \), if HTP is unsolvable over \( \mathcal{O}_K \), then HTP is unsolvable over any small subring of \( K \).

(Julia Robinson and others)
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 or 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 $1 - \frac{1}{[K : \mathbb{Q}]} - \varepsilon$.
- HTP is unsolvable over $O_{K,S}$.

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)
If the fields are “close” enough to the algebraic closure of \(\mathbb{Q}\), one starts to get decidability results not just for HTP but also for the first order theory. (See results by Rumely, Van den Dries, Macintyre, Jarden, Razon, Prestel, Green, Pop, Roquette, Moret-Bailly, and others.) So if we are looking for undecidability we should stay “far” away from the algebraic closure.
Denef’s Theorem for Infinite Extensions of $\mathbb{Q}$, 1980

**Theorem**

Let $K$ be a totally real field (possibly of infinite degree) such that for some elliptic curve $E$ defined over $\mathbb{Q}$, the rank of $E$ over $\mathbb{Q}$ is positive and the same as over $K$. Then the ring of integers of $K$ has a Diophantine definition of $\mathbb{Z}$. 
**Integral Closure**

Let $R_1 \subset R_2$ be integral domains. Then the integral closure of $R_1$ in $R_2$ is the set of elements of $R_2$ satisfying monic irreducible polynomials with coefficients in $R_1$.

---

**Big and Small Rings in Infinite Extensions**

Let $K_\infty$ be an infinite algebraic extension of $\mathbb{Q}$. Let $K$ be any number field contained in $K_\infty$. Let $\mathcal{W}_K$ be a set of primes of $K$ and let $R$ be the integral closure of $O_{K,\mathcal{W}_K}$ in $K_\infty$. Then we call $R$ **big** or **large** if $\mathcal{W}_K$ is infinite, and we call $R$ **small** otherwise. We denote $R$ by $O_{K_\infty,\mathcal{W}_{K_\infty}}$. 
Big and Small Rings in Totally Real Infinite Extensions

Theorem

Every totally real subfield of a cyclotomic extension with finitely many ramified primes contains a small subring, not equal to the ring of integers, where HTP is unsolvable. (S. 1994)

Theorem

Every totally real subfield $K_{\infty}$ of a cyclotomic extension with finitely many ramified primes contains a big subring $R$ where HTP is unsolvable. Further for any $\varepsilon > 0$ it can be arranged that $R$ is the integral closure of a ring $O_{K, W_K}$, where $K$ is a number field contained in $K_{\infty}$ and the natural density of $W_K$ is greater than $1 - \varepsilon$. (S. 2004)
Big Rings in the Extensions of Degree 2 of Totally Real Infinite Extensions

**Theorem**

Let $K_{\infty}$ be a totally real subfield of a cyclotomic extension with finitely many ramified rational primes and a finite ramification degree for 2. Let $G_{\infty}/K_{\infty}$ be any extension of degree 2. Let $K \neq \mathbb{Q}$ be a totally real number field contained in $G_{\infty}$. Then for some large subring $O_{K, \mathcal{R}_K}$ of $K$ we have that HTP is unsolvable in the integral closure of $O_{G_{\infty}, \mathcal{R}_{G_{\infty}}}$ in $G_{\infty}$. 
Small Rings in the Extensions of Degree 2 of Totally Real Infinite Extensions

**Theorem**

Let $K_\infty$ be a totally real subfield of a cyclotomic extension with finitely many ramified rational primes. Let $G_\infty/K_\infty$ be any extension of degree 2. Let $K$ be a number field contained in $G_\infty$. Then for any small subring $O_{K,S_K}$ of $K$, not equal to the ring of integers of $K$, we have that HTP is unsolvable in $O_{G_\infty,S_{G_\infty}}$.

(S. 2006)
A Corollary

Theorem

Let $A_\infty$ be an abelian (possibly infinite) extension of $\mathbb{Q}$ with finitely many ramified primes. Then the following statements are true.

- If the ramification degree of 2 is finite, then for any number field $A$ contained in $A_\infty$ and not equal to $\mathbb{Q}$, there exists an infinite set of $A$-primes $\mathcal{W}_A$ such that HTP is unsolvable in the integral closure of $O_{A,\mathcal{W}_A}$ in $A_\infty$.

- For any number field $A \subset A_\infty$ and any finite non-empty set $S_A$ of its primes, we have that HTP is unsolvable over the integral closure of $O_{A,S_A}$ in $A_\infty$.

(S. 2006)
Ring of Integers of Totally Real Extensions

**Theorem**

Let $K_\infty$ be a totally real possibly infinite algebraic extension of $\mathbb{Q}$. Let $U_\infty$ be a finite extension of $K_\infty$ such that there exists an elliptic curve $E$ defined over $U_\infty$ with $E(U_\infty)$ finitely generated and of a positive rank. Then HTP is unsolvable over the ring of integers of $K_\infty$.

**Theorem**

Let $K_\infty, U_\infty$ and $E$ be as above. Let $G_\infty$ be an extension of degree two of $K_\infty$. If $G_\infty$ has no real embeddings into it algebraic closure, assume additionally that $K_\infty$ has a totally real extension of degree two. Then HTP is unsolvable over the ring of integers of $G_\infty$.

(S. 2007)
Very Big Subrings of Infinite Extensions

Theorem

Let $K_{\infty}$ be an algebraic extension of $\mathbb{Q}$ such that there exists an elliptic curve $E$ defined over $K_{\infty}$ with $E(K_{\infty})$ of rank 1 and finitely generated. Fix a Weierstrass equation for $E$ and a number field $K$ containing all the coefficients of the Weierstrass equation and the coordinates of all the generators of $E(K_{\infty})$. Assume that $K$ has two non-dyadic relative degree one primes $p$ and $q$ such that integrality is definable at $p$ and $q$ over $K_{\infty}$ (this term will be explained later). Then there exists a set $\mathcal{W}_K$ of $K$-primes of natural density 1 such that HTP is not solvable over $O_{K_{\infty},\mathcal{W}_K}$, the integral closure of $O_K,\mathcal{W}_K$ in $K_{\infty}$.

(S. 2007)
Diophantine Sets

Let \( R \) be an integral domain. 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 coefficients in \( R \) such that for any \( m \)-tuple \( (t_1, \ldots, t_m) \in R^m \) we have that

\[
\exists x_1, \ldots, x_k \in R : p(t_1, \ldots, t_m, x_1, \ldots, x_k) = 0
\]

\[\iff (t_1, \ldots, t_m) \in A.\]

In this case we call \( p(T_1, \ldots, T_m, X_1, \ldots, X_k) \) a Diophantine definition of \( A \) over \( R \).
Diophantine Sets

Other Descriptions

Diophantine sets can also described as projections of algebraic sets or sets existentially definable in the language of rings.
Diophantine Subsets of $\mathbb{Z}$

MDRP Theorem

The recursively enumerable subsets of $\mathbb{Z}$ are the same as the Diophantine subsets of $\mathbb{Z}$.

Corollary

There are undecidable Diophantine subsets of $\mathbb{Z}$. 
Definition

Let $R_1, R_2$ be two recursive rings and let $\phi : R_1 \rightarrow R_2^m$, $m \in \mathbb{Z}_{>0}$ be an injective recursive map sending Diophantine sets of $R_1^k$, $k \in \mathbb{Z}_{>0}$ to Diophantine sets of $R_2^{k+m}$. Then $\phi$ is called a Diophantine model of $R_1$ over $R_2$.

Remark

If $R_1 \subset R_2$ and $\phi$ is the inclusion map, then $R_1$ has a Diophantine definition over $R_2$. Conversely, if $R_1$ has a Diophantine definition over $R_2$, then $R_2$ has a Diophantine model of $R_1$ with $\phi$ being the inclusion map.
Diophantine Models and Diophantine Undecidability

**Proposition**

Suppose $R_1$ has undecidable Diophantine sets and $R_2$ has a Diophantine model of $R_1$. Then $R_2$ also has undecidable Diophantine sets.

**Corollary**

If $R$ is a countable ring with a Diophantine model of $\mathbb{Z}$, then $R$ has undecidable Diophantine sets and therefore HTP is unsolvable over $R$.

**Remark**

Most of the known Diophantine undecidability results over algebraic extensions of $\mathbb{Q}$ are obtained by constructing a Diophantine definition of $\mathbb{Z}$. However, there are notable exceptions to this pattern, where a Diophantine model which is not a Diophantine definition is constructed.
A Vertical Problem

Definition
Let $R_1$, $R_2$ be integral domains such that $F_2$, the fraction field of $R_2$, is an algebraic extension of $F_1$, the fraction field of $R_1$. Assume also that $R_2$ is the integral closure of $R_1$ in $F_2$. Then call the problem of constructing a Diophantine definition of $R_1$ over $R_2$ a **vertical** problem.

There are two vertical methods: the weak one and the strong one, both due to Denef and Lipshitz.
The Strong Vertical Method

**Lemma**

Let $R$ be the ring of integers of some algebraic extension of $\mathbb{Q}$. Let $x, w \in R$, let $n \in \mathbb{Z}$ and assume that the following congruence holds:

$$x \equiv n \mod w \text{ in } R,$$

where for every $\sigma$, embedding of $\mathbb{Q}(x, w)$ into the algebraic closure of $\mathbb{Q}$, we have that $|\sigma(x)| < \frac{1}{2} |\sigma(w)|$ and $n < \frac{1}{2} |\sigma(w)|$. Then $x = n$.

**Proof.**

From Congruence (1) we have that

$$N_{\mathbb{Q}(x,w)/\mathbb{Q}}(x - n) \equiv 0 \mod N_{\mathbb{Q}(x,w)/\mathbb{Q}}(w).$$

But

$$|N_{\mathbb{Q}(x,w)/\mathbb{Q}}(x - n)| = \prod_{\sigma} |\sigma(x - n)| < \prod_{\sigma} |\sigma(w)| = |N_{\mathbb{Q}(x,w)/\mathbb{Q}}(w)|.$$ 

Thus, $x - n = 0$. 

HTP over Algebraic Extensions of $\mathbb{Q}$: Normforms vs. Elliptic Curves

Constructing Diophantine Definitions

Vertical Methods

The Weak Vertical Method

The Main Idea

If an *element above* is equivalent to an *element below* modulo sufficiently *large element below*, then the *element above* is really *below*.
The Weak Vertical Method for Integers and Extensions of Degree 2

Proposition

Assume the following.

- \( K_\infty \) is an algebraic extension of \( \mathbb{Q} \).
- \( G_\infty \) is an extension of degree 2 of \( K_\infty \).
- \( x \in O_{G_\infty} \)
- \( \alpha \in O_{G_\infty}, G_\infty = K_\infty(\alpha), 1 < \alpha^2 = a \in K_\infty \).
- \( x = y_1 + y_2\alpha, y_1, y_2 \in K_\infty \).
- \( z, w \in O_{K_\infty} \).
- \( x \equiv z \mod w \) in \( O_{G_\infty} \).
- For any embedding \( \sigma : G_\infty \rightarrow \tilde{\mathbb{Q}} \) (the algebraic closure of \( \mathbb{Q} \)) we have that \( |\sigma(2\alpha y_2)| < |\sigma(w)| \).

Then \( x \in K_\infty \).
**Proof**

Let $M$ be a number field such that $M \subset K_{\infty}$ and $a = \alpha^2, y_1, y_2, z, w \in M$. Then

$$N_{M(\alpha)/Q}(w) > N_{M(\alpha)/Q}(2\alpha y_2).$$

Let

$$\bar{x} = y_1 - \alpha y_2$$

be the conjugate of $x$ over $K_{\infty}$ and note that

$$\bar{x} \equiv z \mod w \text{ in } O_{G_{\infty}}$$

also. Therefore

$$2\alpha y_2 = x - \bar{x} \equiv 0 \mod w.$$  

(Observe that since $x, \bar{x} \in O_{G_{\infty}}$ we also have $2\alpha y_2$ in $O_{G_{\infty}}$.) Hence, either

$$y_2 = 0 \text{ or } N_{M/Q}(w) \leq N_{M/Q}(2\alpha y_2).$$

The second option leads to a contradiction.
Ingredients of the Vertical Methods

Let $R_1$, $R_2$ be integral domains such that $F_2$, the fraction field of $R_2$, is an algebraic extension of $F_1$, the fraction field of $R_1$. Assume also that $R_2$ is the integral closure of $R_1$ in $F_2$.

- We need a polynomial equation $P(t_1, \ldots, t_m, x_1, \ldots, x_k)$ with coefficients in $R_2$ such that if

$$P(t_1, \ldots, t_m, x_1, \ldots, x_k) = 0$$

has solutions in $R_2$, it is the case that $t_1, \ldots, t_m \in R_1$.

(WVM)

- We need to be able to bound the absolute value and/or the height of all the conjugates $t_1, \ldots, t_m$ in a “Diophantine manner”. (Both WVM and SVM)

- We need to be able to generate integers from $t_1, \ldots, t_m$.

(WVM)

- Solutions to the polynomial equation must have “rank 1”.

(SVM)
Using Norm Equations of Units to Generate Integers

A vertical problem
Let $L \subset K \subset M$ be number field extensions. Let $R_L$ be a subring of $L$ (big or small) and let $R_K$ and $R_M$ be the integral closures of $R_L$ in $K$ and $M$ respectively. We consider the problem of existentially defining $R_L$ in $R_K$ using norm equations.

Lemma
$R_M$-solutions to the equation $N_{M/K}(x) = 1$ form a multiplicative group. Thus, if $x$ is a solution, $x^n$ is also a solution for any $n \in \mathbb{Z}$.

Producing Integers
\[
\frac{x^n - 1}{x - 1} \equiv n \mod (x - 1) \text{ in } \mathbb{Z}[x] \subseteq R_M.
\]
What We Need

Remark

For the SVM, one needs the solution group to be of rank 1. For the WVM, one needs all the solutions to be "essentially" in L.
Dirichlet Unit Theorem

**Theorem**

Let $K$ be a number field with $r_K$ real embeddings and $2s_k$ complex embeddings into its algebraic closure. Then the rank of the integral unit group of $K$ is $r_K + s_k - 1$.

**Proposition**

Let $M/K$ be a number field extension. Then the rank of the group \( \{ x \in O_M : N_{M/K}(x) = 1 \} \) is the difference between the ranks of the unit groups of $M$ and $K$. 
Solution Groups of Rank 1

Proposition

Let $K$ be a totally real number field of degree $n$, and let $M$ be an extension of degree $2$ of $K$ with $2n - 2$ non-real embeddings and $2$ real embeddings into its algebraic closure. Alternatively, let $K$ be a number field of degree $n$ with exactly one pair of non-real embeddings into its algebraic closure, and let $M$ be a totally complex extension of degree $2$ of $K$. Then the rank of the solution group $N_{M/K}(x) = 1, x \in \mathcal{O}_M$ is $1$.

Proof.

The assertion follows from the comparison of the ranks of the unit groups of $M$ and $K$.

These norm equations were used to construct a Diophantine definition of $\mathbb{Z}$ over rings of integers of totally real fields and fields with one pair of non-real embeddings.
Norm Equations with Solutions Below over Integral Units

Proposition (Denef, Lipshitz, 1979)

Let $M$ be a totally real number field. Let $G$ be an extension of degree 2 of $M$ generated by $\alpha \in O_G$ such that $\alpha^2 = a \in M$ and $G$ is not totally real. Next let $b \in O_M$ be such that for any embedding $\sigma : M \rightarrow \bar{\mathbb{Q}}$ we have that $\sigma(a)\sigma(b) < 0$. Let $\beta \in \bar{\mathbb{Q}}$ be such that $\beta^2 = b$ and let $H = M(\beta)$. Let $\varepsilon \in O_{GH}$ and assume that

$$N_{GH/G}(\varepsilon) = 1$$

Then for some positive integer $k$ we have that $\varepsilon^k \in O_H$. Further there are solutions to this norm equation which are not roots of unity.
This can be used to produce a Diophantine definition of $O_G$ over $O_M$. Given the lemma above, “almost all” solutions $(x, y) \in O_G^2$ to the equation $x^2 - by^2 = 1$ are actually in $O_M$. 
Proof

Let

\[ A_{GH} = \{ \varepsilon \in O_{GH} : N_{GH/G}(\varepsilon) = 1 \}. \]

Let

\[ A_H = \{ \varepsilon \in O_H : N_{H/M}(\varepsilon) = 1 \}. \]

Let \([M : \mathbb{Q}] = n\), \([G : \mathbb{Q}] = 2n\) and \([GH : \mathbb{Q}] = 4n\). Let \(s_G > 0\) be the number of pairs non-real embeddings of \(G\) into \(\bar{\mathbb{Q}}\). Let \(r_G\) be the number of real embeddings of \(G\) into \(\bar{\mathbb{Q}}\). (Thus \(r_G + 2s_G = 2n\)).

Given our assumptions, all of the embeddings of \(GH\) into \(\bar{\mathbb{Q}}\) are non-real and there are \(2n\) conjugate pairs of these embeddings.

The rank of \(A_{GH}\) is

\[ (2n - 1) - (r_G + s_G - 1) = r_G + 2s_G - r_G - s_G = s_G. \]

The rank of \(A_H\) is \(r_G/2 + 2s_G - 1 - (n - 1) = s_G\). So the ranks of \(A_{GH}\) and \(A_H\) are the same. Further, since \(H\) and \(G\) are linearly disjoint over \(K\), we also have that \(A_H \subseteq A_{GH}\) and thus the proposition holds.
Let $K \neq \mathbb{Q}$ be a totally real field and let $M$ be a totally complex extension of degree 2 of $K$. Then the unit groups of $M$ and $K$ have the same rank and therefore for some $\ell \in \mathbb{Z}_{>0}$, for any integral unit $\varepsilon \in \mathcal{O}_M$ we have that $\varepsilon^\ell \in \mathcal{O}_K$. So in this case, over rings of integers, one can use the WVM without norm equations. Another way to look at this situation is to note that the only integral solutions to $N_{M/K}(x) = 1, x \in \mathcal{O}_M$ are possibly roots of unity.
Divisors of Number Field Elements

**Definition**

Let $K$ be a number field and let $x \in K$. Let $\mathcal{P}(K)$ be the set of all non-archimedean primes of $K$ (ideals of $O_K$ or non-archimedean valuations of $K$). Then the divisor of $x$ is

$$\prod_{p \in \mathcal{P}(K)} p^{\text{ord}_p x}$$

Over $\mathbb{Q}$ this is equivalent to writing the prime factorization of the numerator and denominator of a reduced fraction representing a rational number: $\frac{18}{25} = \frac{3^2 \cdot 2}{5^2}$. 
Norms of Divisors

Let $K/E$ be a number field extension, let $p_K$ be a prime of $K$ and let $p_E = p_K \cap \mathcal{O}_E$ be the prime below $p_K$ in $E$. Then the residue field of $p_K$ is a finite extension of the residue field of $p_E$ and the degree $f$ of this extension is called the relative degree of $p_K$ over $p_E$. We also define the $N_{K/E}p_K = p_E^f$. If we have a divisor of $K$, i.e. a finite product of primes of $K$, we define the norm of the divisor to be the product of the norms of the constituent factors:

$$N_{K/E} \prod q_i^{a_i} = \prod N_{K/E}(q_i)^{a_i}.$$

Proposition

Let $x \in K$. Then the divisor of $N_{K/E}(x)$ is equal to the $K/E$-norm of the divisor of $x$. 
**Lemma**

Let $M/K$ be a finite extension of number fields. Let $x \in M$ be a solution to $N_{M/K}(x) = 1$ and let $p$ be a prime of $M$ such that $\text{ord}_p x \neq 0$. Then $p$ lies above a prime of $K$ which splits into distinct factors in the extension $M/K$.

**Proof.**

Let the divisor of $x$ be of the form $\frac{p_1^{a_1} \cdots p_k^{a_k}}{q_1^{b_1} \cdots q_m^{b_m}}$. Then the divisor of the $K$-norm of $x$ will be of the form $\frac{\mathfrak{P}_1^{f(p_1)a_1} \cdots \mathfrak{P}_k^{f(p_k)a_k}}{\mathfrak{Q}_1^{f(q_1)b_1} \cdots \mathfrak{Q}_m^{f(q_m)b_m}}$, where $\mathfrak{P}_i$ is the $K$-prime below $p_i$, $\mathfrak{Q}_i$ is the $K$-prime below $q_i$, and $f(p_i)$, $f(q_i)$ are the relative degrees of $p_i$ and $q_i$ respectively over $K$.

Now if the $K$-norm of $x$ is $1$, the divisor above must be a trivial divisor. This means that for each $p_i$ there exists a $q_j$ such that $\mathfrak{P}_i = \mathfrak{Q}_j$. Therefore this $K$-prime has at least two factors in $M$. $\blacksquare$
Proposition

Let $M/K$ be a finite extension of number fields. Let $\mathcal{W}_K$ be a set of primes of $K$. Let $\mathcal{W}_M$ be the set of all $M$-factors of primes in $\mathcal{W}_K$. (This assumption implies that $O_{M,\mathcal{W}_M}$ is the integral closure of $O_{K,\mathcal{W}_K}$ in $M$.) Let $x \in O_{M,\mathcal{W}_M}$ be a solution to $N_{M/K}(x) = 1$ and let $q_M$, a prime of $M$ be such that $\text{ord}_{q_M} x \neq 0$. Then $q_M \in \mathcal{W}_M$.

Proof.

If $\text{ord}_{q_M} x \neq 0$, then $\text{ord}_{q_M}$ has a conjugate $t_M$ over $K$ such that either $\text{ord}_{t_M} x < 0$ or $\text{ord}_{q_M} x < 0$. Thus, both $q_M, t_M \in \mathcal{W}_M$ since $\mathcal{W}_M$ is closed under conjugation over $K$.

Corollary

If $q_M$ is such that $\text{ord}_{q_M} x \neq 0$, then $q_M$ lies above a prime of $\mathcal{W}_K$ which splits in $M$. 
A Norm Equation System

Consider the following diagram:

where

- $K$ is a totally real number field,
- $M$ is a totally real cyclic extension of $\mathbb{Q}$ of prime degree $p > 2$,
- $L$ is a totally complex extension of degree 2 of $\mathbb{Q}$,
- $K$ and $ML$ are linearly disjoint over $\mathbb{Q}$,
- $p_K$ is a prime of $K$ splitting completely (into distinct factors) in the extension $MLK/K$,
- $\mathcal{V}_K$ is a set of primes of $K$ inert in the extension $MK/K$,
- $\mathcal{W}_K = \mathcal{V}_K \cup \{p\}$,
- $\mathcal{W}_{MLK}$ is the set of all $MLK$-factors of primes in $\mathcal{W}_K$.

Finally, consider all the solutions to the system

$$\begin{cases} 
N_{MLK/LK}(x) = 1 \\
N_{MLK/MK}(x) = 1 
\end{cases}$$

with $x \in O_{\mathcal{W}_{MLK}}$. 
If $q_{L,K}$ is a prime of $L,K$ lying above a prime $q_K \in \mathcal{V}_K$, then $q_{L,K}$ is inert in the extension $M_{L,K}/L,K$. (This follows by a counting argument from the fact that $M_{L,K}/K$ is Galois and $(p, 2) = 1$.)

Therefore no prime of $\mathcal{V}_{M_{L,K}}$, the set of all $M_{L,K}$-primes above primes in $\mathcal{V}_K$, can appear in the divisor of $x$.

It can be shown that the system does have solutions whose divisor is composed solely of the factors of $p_K$.

Since $M_{L,K}$ has no real embeddings and $M_K$ is totally real, we know that $N_{M_{L,K}/M_K}(x) = 1$ has no integral solutions except possibly for roots of unity.

If we have two solutions $x_1, x_2$ to our system and they have the same divisors, then $\frac{x_1}{x_2}$ is an integral solution and therefore must be a root of unity. In other words, a solution is almost completely determined by its divisor.
So by carefully selecting \( V_K \) we can arrange that all the solutions to System (3) in \( O_{W_{MLK}} \) have divisors consisting of factors of a single prime \( p_K \) and these solutions are completely determined by their divisors.

\[
\begin{align*}
N_{MLK/LK}(x) &= 1 \\
N_{MLK/MK}(x) &= 1
\end{align*}
\tag{3}
\]

Suppose now \( K \) has a cyclic subextension \( E \) and \( p_K \) lies above a prime \( p_E \) which is inert in the extension \( K/E \) but splits completely in the extension \( MLE/E \). Then it turns out that the solutions to the system above are exactly the same as the solutions to the system below, i.e. the solutions “above” are really “below”.

\[
\begin{align*}
N_{MLE/LE}(x) &= 1 \\
N_{MLE/ME}(x) &= 1
\end{align*}
\]

with \( x \in O_{W_{MLE}} \).
Lemma

Let $K$ be a number field of degree $n$. Let $x, y \in O_K$, assume $y$ is not a unit and $x(x + 1) \ldots (x + n)$ divides $y$ in $O_K$. Then for some positive constant $c$, depending on $K$ only, for every $\sigma$, embedding of $K$ into its algebraic closure, $|\sigma(x)| < |N_{K/\mathbb{Q}}(y)|^c$.

Proof.

Linear Algebra
Let $K$ be a number field, let $M/K$ be a finite extension and let $x \in O_M$ be a solution to $N_{M/K}(x) = 1$. As we discussed before, for any positive integer $n$ we also have that $x^n$ is a solution to this norm equation. Further, given any integer $z \in O_K$ for some $n \in \mathbb{Z}_{>0}$ we will have that $z$ divides $x^n - 1$. This works very nicely with the way we can generate integers from powers of $x$.

\[
\frac{x^{nk} - 1}{x^n - 1} \equiv k \mod x^n - 1
\]

So if we write down $z \equiv \frac{x^{nk} - 1}{x^n - 1} \mod (x^n - 1)$ we are on our way towards using the WVM.
Advantages and Disadvantages of Norm Equations

- Over number fields, the method depends on the ranks of the unit groups and, at least in its present form, cannot be pushed beyond the totally real fields, their extensions of degree 2 and fields with one pair of non-real embeddings.

- For infinite extensions, the method requires cyclic extensions and does not work for rings of integers.

- At the same time we can easily describe the classes of fields and rings for which the norm method does work.