BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 51, Number 3, July 2014, Pages 447–461
S 0273-0979(2014)01443-0
Article electronically published on March 17, 2014

A HASSE PRINCIPLE FOR QUADRATIC FORMS OVER FUNCTION FIELDS

R. PARIMALA

Abstract. We describe the classical Hasse principle for the existence of nontrivial zeros for quadratic forms over number fields, namely, local zeros over all completions at places of the number field imply nontrivial zeros over the number field itself. We then go on to explain more general questions related to the Hasse principle for nontrivial zeros of quadratic forms over function fields, with reference to a set of discrete valuations of the field. This question has interesting consequences over function fields of p-adic curves. We also record some open questions related to the isotropy of quadratic forms over function fields of curves over number fields.

1. Introduction

In 1882, Minkowski, who was still a student at Königsberg, wrote a paper on rational quadratic forms ([22]) which was awarded the mathematics prize by the French Academy of Sciences. In this paper Minkowski established the foundations of the theory of integral quadratic forms, with the aim of determining the number of representations of a natural number as a sum of five squares. From this long article he extracted, in a letter to Adolf Hurwitz in 1890 ([23]), necessary and sufficient conditions for two rational forms to be isometric. This is achieved by associating to any nonsingular form f a set of invariants $C_p(f)$, one for each prime p, which can take values 1 or -1. If f is an integral form, these invariants $C_p(f)$ only depend on the reduction of f modulo an explicitly given, sufficiently high power of p. Two forms are isometric if and only if they have the same dimension and signature, the same discriminant up to squares, and the same invariants C_p.

Hensel, in 1897 ([15]) ushered in the fields of p-adic numbers, in analogy with the fields of formal power series, with a grand vision for the parallel development of algebraic number theory and analytic function theory. Hensel's 1913 book *Zahlentheorie* ([16]) in spite of its elementary character, defines p-adic numbers (in fact m-adic numbers for any integer $m > 1$), and it explains how to compute with them and how they can be used in the study of binary and ternary quadratic forms.

Hasse, after discovering Hensel's book in an antiquarian bookshop, decided to leave Göttingen and continue his studies in Marburg with Hensel. Hensel's questions led him to the proof of the local-global theorem for rational n-dimensional forms ([10]), saying that a rational quadratic form has a nontrivial zero if and only if it

Received by the editors August 26, 2013, and, in revised form, October 28, 2013.
2010 *Mathematics Subject Classification.* Primary ???
The author is partially supported by National Science Foundation grant DMS-1001872.
(Based on the AWM Noether lectures, delivered at the 2013 AMS-MAA joint meeting at San Diego).

has a nontrivial zero in any $\mathbb{Q}_p$ and in $\mathbb{R}$. This result was immediately followed by another ([11]), saying that two rational quadratic forms are equivalent if and only if they are equivalent over $\mathbb{R}$ and over all $\mathbb{Q}_p$. Hasse introduced what is now termed the Hasse invariant as a product of Hilbert symbols and proved that Minkowski's invariants C_p were equivalent to his own. Hasse's work was a significant milestone in the study of rational quadratic forms. The first generalization came the next year when Hasse proved the same theorems for quadratic forms over algebraic number fields ([12], [13]). A few years later an important result was achieved in a different direction, when Brauer, Hasse, and Noether proved (in a paper dedicated to Hensel) that a central simple algebra over an algebraic number field, which is a locally a matrix algebra, is in fact a matrix algebra ([1]).

These results can be expressed by saying that certain varieties defined over a number field k have a rational point provided they have points over all the completions of k. Theorems of this kind have come to be termed as *Hasse principles*. Such a Hasse principle for a general smooth projective variety fails, as is seen from examples of genus one curves admitting local points over k_vs but with no rational points. These examples go back to Reichardt [26] and Lind [21]. Manin introduced an obstruction, using the Brauer group, to the validity of the Hasse principle for the existence of rational points for varieties over number fields. This obstruction is now known as the *Brauer–Manin* obstruction. There has been extensive study of when this obstruction is the only obstruction to the Hasse principle (cf. [2], [25]).

Let k be a p-adic field. Then every quadratic form in five variables over k has a nontrivial zero. It has been recently settled that every quadratic form in at least nine variables over the function field of a curve over k has a nontrivial zero ([14], [19], [24]). However, analogous questions for function fields of curves over number fields are wide open. More precisely, let k be a totally imaginary number field. Thanks to the Hasse–Minkowski theorem, every five dimensional quadratic form over k has a nontrivial zero. Let F be the function field of a smooth projective curve over k. The completion of F at a divisorial discrete valuation (cf. Section 8) of F has a global field as its residue field. In particular, every nine dimensional form over the completion F_v has a nontrivial zero. If the Hasse principle were true for quadratic forms over F with respect to its divisorial discrete valuations, it would follow that every nine dimensional quadratic form over F admits a nontrivial zero.

Thus, the Hasse principle questions for function fields of varieties over number fields have deep consequences concerning the arithmetic of quadratic forms over these fields. Beginning with the results of Hasse and Minkowski, we trace in this article the history of the Hasse principle for existence of nontrivial zeros of quadratic forms over function fields.

2. Notation

Let k be a field of characteristic not 2. A *quadratic form* q on a finite dimensional vector space V over k is a map $q : V \to k$ satisfying

(1) $q(\lambda v) = \lambda^2 q(v) \ \forall\, \lambda \in k, v \in V$.
(2) The map $b_q : V \times V \to k$, given by

$$b_q(v, w) = \frac{q(v+w) - q(v) - q(w)}{2},$$

is bilinear.

The form q is said to be *nondegenerate* if the associated bilinear form b_q is nondegenerate. For a choice of basis $\{e_i\}_{1\leq i\leq n}$ for V, b_q is represented by a symmetric $n\times n$ matrix

$$A(q) = \left(b_q\left(e_i, e_j\right)\right)_{1\leq i\leq n}.$$

Nondegeneracy of q is the same as invertibility of $A(q)$. The quadratic form q is represented with respect to this basis by a homogeneous polynomial $\sum_{1\leq i\leq j\leq n} a_{ij}X_iX_j$ of degree 2 with $a_{ij} = 2b_q\left(e_i, e_j\right)$ for $i\neq j$ and $a_{ii} = b_q\left(e_i, e_i\right)$. Two quadratic forms (V_1, q_1) and (V_2, q_2) are *isomorphic* if there is an isomorphism of the underlying vector spaces $\varphi : V_1 \cong V_2$ with $q_2\left(\varphi(v)\right) = q_1(v)$. This is equivalent to the existence of an invertible $n\times n$ matrix T such that

$$A\left(q_1\right) = T^t A\left(q_2\right) T. \tag{1}$$

Over fields of characteristic not 2, the study of quadratic forms up to isomorphism is equivalent to the study of symmetric matrices up to congruence (see equation (1)). Further, one can choose an orthogonal basis such that the form is *diagonal*:

$$q = \sum_{1\leq i\leq n} b_i X_i^2, b_i\in k.$$

If the form is nondegenerate, all b_i are nonzero and such a form is denoted by $\langle b_1, b_2, \ldots, b_n\rangle$. The *orthogonal sum* of two quadratic forms (V_1, q_1) and (V_2, q_2) is the form $q_1\perp q_2 : V_1\oplus V_2\to k$ defined by

$$\left(q_1\perp q_2\right)\left(v_1, v_2\right) = q_1\left(v_1\right) + q_2\left(v_2\right), v_1\in V_1, v_2\in V_2.$$

The matrix associated to $q_1\perp q_2$ is the block matrix

$$\begin{pmatrix} A\left(q_1\right) & 0\\ 0 & A\left(q_2\right)\end{pmatrix}.$$

A scalar $\lambda\in k$ is *represented* by q if there is a nonzero vector $v\in V$ such that $q(v) = \lambda$.

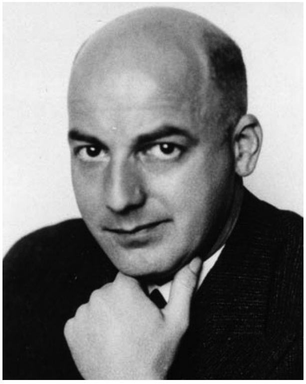
Example 2.1. The form $X_1^2 + X_2^2$ over $\mathbb{Q}$ represents 5 but not 3.

A form q is *isotropic* if there is a nonzero vector $v\in V$ such that $q(v) = 0$. The form is *anisotropic* if it is not isotropic.

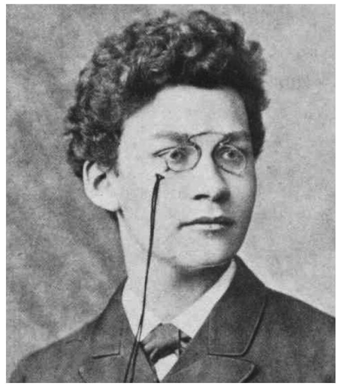
Example 2.2. A typical isotropic form is $X_1^2 - X_2^2$, is called the hyperbolic plane, and is denoted by h.

3. Rational quadratic forms and a theorem of Minkowski and Hasse

Let $\mathbb{Q}$ be the field of rational numbers. A basic question is to determine when a quadratic form over $\mathbb{Q}$ has a nontrivial zero. Let q be a quadratic form over $\mathbb{Q}$ of dimension n, represented by $a_1X_1^2 + \cdots + a_nX_n^2, a_i\in\mathbb{Q}^\star$. By changing a_i in their square classes, which does not affect the isomorphism class of q, we may assume that the a_i are integers. Since multiplying q by a nonzero scalar $\lambda\in\mathbb{Q}$ does not affect the isotropy of q, we assume after scaling, that $\gcd_i\left(a_i\right) = 1$. Such a form is called a *primitive quadratic form.* We also assume that the a_i are square-free integers.



Helmut Hasse
(1898–1979)



Hermann Minkowski
(1864–1909)

Given a nontrivial zero $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ of q over $\mathbb{Q}$, one can find a zero $(\mu_1, \mu_2, \ldots, \mu_n)$ of q with $\mu_i \in \mathbb{Z}, 1 \leq i \leq n$, and $\gcd_i(\mu_i) = 1$. Such a zero is called a *primitive* zero of q. An element $(\lambda_1, \lambda_2, \ldots, \lambda_n) \in \mathbb{Z}^n$ is called a *primitive congruence solution modulo* m if $\gcd_i(\lambda_i)$ is coprime to m and $\sum_{1 \leq i \leq n} a_i \lambda_i^2 \equiv 0 \mod m$.

Let q be a primitive quadratic form over $\mathbb{Q}$ defined by $q = \sum_{1 \leq i \leq n} a_i X_i^2$. The following is a set of necessary conditions for q to be isotropic.

- q is isotropic over $\mathbb{R}$, the field of real numbers, i.e., there is a change in the signs of the a_i. (Such a form is called an *indefinite* quadratic form.)
- q has primitive congruence solutions modulo m for every integer $m \geq 2$.

Example 3.1. $q = X^2 + Y^2 - 7Z^2$. The form q is indefinite but has no primitive congruence solutions modulo 4. Hence q is not isotropic over $\mathbb{Q}$.

The first sufficient conditions for a quadratic form q over $\mathbb{Q}$ to represent zero nontrivially were due to Legendre for the case when the dimension of q is 3, towards the end of the eighteenth century ([29, Chapter IV, Appendix I]). The sufficient conditions for a general quadratic form q over $\mathbb{Q}$ were due to Hasse and Minkowski.

Theorem 3.2 (Hasse and Minkowski)**.** *A primitive quadratic form q over $\mathbb{Q}$ has a nontrivial zero provided it is indefinite and admits primitive congruence solutions modulo n for every integer $n \geq 2$.*

The Hasse–Minkowski theorem actually provides an efficient recipe to verify isotropy. Let $q = \sum_{1 \leq i \leq n} a_i X_i^2$, with $a_i \in \mathbb{Z}$ square-free and $\gcd_i(a_i) = 1$.

Proposition 3.3. *For a primitive quadratic form $q = \sum_{1 \leq i \leq n} a_i X_i^2$, where $n \geq 3$ and a_i square-free integers, to be isotropic, it suffices to verify the following:*

- *There is a change in the signs of the a_i.*
- *There is a primitive congruence solution modulo p^2 for the finite set of odd primes p dividing any of the a_i.*
- *There is a primitive congruence solution modulo 16.*

We shall prove this using Hensel's lemma and the Hasse–Minkowski theorem in Section 5.

4. p-ADIC FIELDS

We now begin by describing Newton's method for finding rational approximations to real numbers to motivate Hensel's construction of the field of p-adic numbers.

Consider the equation $x^2 = 7$. This equation has no solutions in $\mathbb{Q}$. We construct a solution in $\mathbb{R}$ as a limit of approximate solutions in $\mathbb{Q}$.

- 0^{th} approximation:
  $X_0 = 2$.
- 1^{st} approximation:
  To correct X_0, we write $X_1 = X_0 + h_1$.
  $X_1^2 = 7$ gives us that $X_0^2 + 2X_0h_1 + h_1^2 = 7$. Solving the equation ignoring the h_1^2 term, we get
  $$h_1 = \frac{3}{4}, \quad X_1 = \frac{11}{4}.$$
- 2^{nd} approximation:
  To correct X_1, we write $X_2 = X_1 + h_2$ and solve for $X_2^2 = 7$ ignoring the h_2^2 term, and we end up with
  $$h_2 = -\frac{9}{88}, \quad X_2 = \frac{233}{88}.$$

Continuing this process, we get a sequence of rational numbers

$$\begin{aligned} X_0 &= 2, \\ X_1 &= \frac{11}{4} = 2.75, \\ X_2 &= \frac{233}{88} = 2.64772727\cdots, \\ X_3 &= \frac{108497}{41008} = 2.6457520483\cdots, \\ &\cdots, \end{aligned}$$

converging to $\sqrt{7} = 2.6457513110\cdots$ in $\mathbb{R}$.

The field $\mathbb{R}$ of real numbers is the *completion* of $\mathbb{Q}$ with respect to the usual distance metric. We shall describe the p-adic metric which gives rise to the field of p-adic numbers as the completion of $\mathbb{Q}$ for the p-adic metric.

To compare whether two integers x and y are equal, we look at the difference $x - y$.

- If $|x - y|$ is less than $\frac{1}{n}$ for every integer $n \geq 1$, then $x = y$.
- For a given prime p, if $x - y$ is divisible by p^n for every integer $n \geq 1$, then $x = y$.

Thus high divisibility by prime powers is another test for the equality of x and y. Let us look at $x^2 = 7$ again. We construct a sequence $\{X_n\}$ of integers such that $X_n^2 - 7$ is divisible by 3^{n+1}.

- 0^{th} approximation:
  $X_0 = 2$. Then $X_0^2 - 7$ is divisible by 3.
- 1^{st} approximation:
  $X_1 = X_0 + 3h_1$. Pick h_1 so that $X_1^2 - 7$ is divisible by 3^2, i.e., $4 + 12h_1 + 9h_1^2 - 7$ is divisible by 9. Pick $h_1 = 1, X_1 = 5$.

- 2^{nd} approximation:
  $X_2 = X_1 + 3^2 h_2$. Pick h_2 so that $X_2^2 - 7$ is divisible by 3^3. Pick $h_2 = 1, X_2 = 14$.

Iterating this process, we get a sequence $\{X_n\}$ of integers:

$$\begin{aligned} X_0 &= 2, \\ X_1 &= 2 + 3 = 5, \\ X_2 &= 2 + 3 + 3^2 = 14, \\ X_3 &= 2 + 3 + 3^2 + 2 \times 3^3 = 68, \\ &\cdots, \\ X_n &= 2 + 3h_1 + 3^2 h_2 + \cdots + 3^{n-1} h_{n-1}, \\ &\cdots, \end{aligned}$$

where $0 \leq h_i \leq 2$ for each i, satisfying $3^{n+1} | (X_n^2 - 7)$ for each n.

If the series $2 + 3h_1 + 3^2 h_2 + \cdots + 3^{n-1} h_{n-1} + \cdots$ is to converge with respect to an absolute value, it should treat integers divisible by high powers of 3 as small! This is the 3-adic absolute value $||\cdot||_3$ on $\mathbb{Q}$.

For any nonzero integer a, define the *p-adic valuation* ν_p as follows:

Let p^n be the highest power of p dividing a. Set $\nu_p(a) = n$. For a rational number $\frac{a}{b}$, where $a, b \in \mathbb{Z}$, both nonzero, set $\nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b)$.

$$\left|\left|\frac{a}{b}\right|\right|_p = \left(\frac{1}{p}\right)^{\nu_p\left(\frac{a}{b}\right)}.$$

$||\cdot||_p$ is the *p-adic absolute value* on $\mathbb{Q}$, which defines a metric on $\mathbb{Q}$ called the *p-adic metric*. For an integer $a \neq 0$, $||a||_p$ is small if a high power of p divides a.

Definition 4.1. The field $\mathbb{Q}_p$ of *p-adic numbers* is the completion of $\mathbb{Q}$ with respect to the p-adic metric.

Every series $a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \cdots$, where $a_i \in \mathbb{Z}$, converges in $\mathbb{Q}_p$.

Example 4.2.

$$1 + p + p^2 + p^3 + \cdots + p^n + \cdots = \frac{1}{1-p} \in \mathbb{Q}_p.$$

The solution $X = 2 + 3h_1 + 3^2 h_2 + \cdots + 3^n h_n + \cdots$ constructed above defines a 3-adic number X whose square is 7 in $\mathbb{Q}_3$.

5. Complete fields and Hensel's lemma

We relate congruence solutions modulo p^n to solutions in p-adic completions. This is achieved via *Hensel's lemma*, which asserts lifting of congruence solutions to solutions in the completion.

Definition 5.1. A *discrete valuation* on a field k is an onto function $\nu : k^\star \to \mathbb{Z}$ satisfying

$$\begin{aligned} \nu(ab) &= \nu(a) + \nu(b), \\ \nu(a+b) &\geq \min\{\nu(a), \nu(b)\}. \end{aligned}$$

The *valuation ring* of ν is the ring

$$\mathcal{O} = \{x \in k^\star | \nu(x) \geq 0\} \cup \{0\}.$$

The ring $\mathcal{O}$ is a local domain with maximal ideal generated by any element $\pi \in \mathcal{O}$ with $\nu(\pi) = 1$. Such an element π is called a *parameter* for ν. The *residue field* of the valuation ν is $\kappa(\nu) = \mathcal{O}/(\pi)$.

The valuation ν gives rise to an absolute value on k as follows. Fix a real number λ with $0 < \lambda < 1$, and set

$$|| \, x \, ||_\nu = \lambda^{\nu(x)}, x \in k \setminus \{0\},$$
$$|| \, 0 \, ||_\nu = 0.$$

This is a *non-archimedean absolute value*, i.e.,

$$|| \, x + y \, ||_\nu \leq \max\{|| \, x \, ||_\nu, || \, y \, ||_\nu\}$$

(better than the usual triangle inequality). Let k_ν denote the *completion* of k with respect to the metric induced by the norm $|| \cdot ||_\nu$.

Example 5.2. The p-adic valuation ν_p on $\mathbb{Q}$ is a discrete valuation. The completion of $\mathbb{Q}$ with respect to ν_p is the field $\mathbb{Q}_p$ of p-adic numbers.

Remark 5.3. Any discrete valuation on $\mathbb{Q}$ is a p-adic valuation.

Example 5.4. Let $\mathbb{F}_q(t)$ denote the rational function field in one variable over the finite field $\mathbb{F}_q$. Define $\nu_t : \mathbb{F}_q(t)^\star \to \mathbb{Z}$ as follows.

For $f(t) \in \mathbb{F}_q[t]$, write

$$f(t) = t^n \left(a_0 + a_1 t + \cdots + a_m t^m\right), a_i \in \mathbb{F}_q, a_0 \neq 0.$$

Set $\nu_t(f) = n$ and extend ν_t to $\mathbb{F}_q(t) \setminus \{0\}$ by setting $\nu_t\left(\frac{f}{g}\right) = \nu_t(f) - \nu_t(g)$ for $f, g \in \mathbb{F}_q[t]$, both nonzero. The function ν_t is a discrete valuation on $\mathbb{F}_q(t)$ with t as a parameter. The completion of $\mathbb{F}_q(t)$ at ν_t is isomorphic to $\mathbb{F}_q((t))$, the field of *Laurent series* in t. (A Laurent series is a formal sum $a_m t^{-m} + a_{m-1} t^{-(m-1)} + \cdots + a_1 t^{-1} + a_0 + b_1 t + b_2 t^2 + \cdots + b_n t^n + \cdots$, where $a_i, b_i \in \mathbb{F}_q$.)

The set of discrete valuations of $\mathbb{F}_q(t)$ is in bijection with monic irreducible polynomials in $\mathbb{F}_q[t]$ together with $\frac{1}{t}$.

Let (k, ν) be a complete discrete valued field with ring of integers $\mathcal{O}_\nu$, a parameter π and residue field κ of characteristic p. A quadratic form $q = \sum_{1 \leq i \leq n} a_i X_i^2, a_i \in k$, is *primitive* if $a_j \in \mathcal{O}_\nu$ for each j and π does not divide a_i for some i. We may also assume that π^2 does not divide a_i for any i. A zero $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ of q is *primitive* if $\lambda_j \in \mathcal{O}_\nu$ for each j and at least one λ_i is a unit in $\mathcal{O}_\nu$. A tuple $(\lambda_1, \lambda_2, \ldots, \lambda_n) \in k^n$ is said to be a *primitive zero modulo* π^m of q if $\lambda_j \in \mathcal{O}_\nu$ for each j, at least one λ_i is a unit in $\mathcal{O}_\nu$ and $\sum_{1 \leq i \leq n} a_i \lambda_i^2 \equiv 0 \mod \pi^m$. Define

$$\epsilon_p = \begin{cases} 1 & \text{if char}\, \kappa \neq 2, \\ 2\nu(2) + 1 & \text{if char}\, \kappa = 2. \end{cases}$$

Lemma 5.5 (Hensel's square criterion)**.** *Let $\lambda \in \mathcal{O}_v$ be a unit, and let* $\operatorname{char} \kappa = p$. *Then λ is a square provided λ is a square modulo π^{ϵ_p}.*

Theorem 5.6 (Hensel)**.** *Let $q = \sum_{1 \leq i \leq n} a_i X_i^2$ be a primitive quadratic form over k with $\nu(a_i) \leq 1$ for every i. Suppose that q has a primitive zero modulo $\pi^{\epsilon_p + 1}$. Then q has a nontrivial zero in k.*

Proof. This is a consequence of Hensel's square criterion. Let $\overline{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ be a primitive zero modulo π^{ϵ_p+1}. Since q is a primitive form and $\overline{\lambda}$ is a primitive zero modulo π^{ϵ_p+1}, a_i and λ_j are units in $\mathcal{O}_v$ for some i and j.

Case I. $i = j$.

Assume without loss of generality that a_1 and λ_1 are units. Set $c = a_2\lambda_2^2 + \cdots + a_n\lambda_n^2$. Then c is a unit as $a_1\lambda_1^2 + c \equiv 0 \mod \pi^{\epsilon_p+1}$. Also note that $\lambda_1^2 \equiv -ca_1^{-1} \mod \pi^{\epsilon_p}$.

By Hensel's square criterion, $-ca_1^{-1}$ is a square in k, say $\theta^2 = -ca_1^{-1}$ for some $\theta \in k$. Then $(\theta, \lambda_2, \lambda_3, \ldots, \lambda_n)$ is a nontrivial zero of q in k.

Case II. a_i and λ_i are not units simultaneously for $1 \leq i \leq n$.

Assume without loss of generality that λ_1 is a unit and $a_1 = \pi a_1'$ with a_1' a unit. Set $c = a_2\lambda_2^2 + \cdots + a_n\lambda_n^2$. Then $\pi a_1'\lambda_1^2 + c \equiv 0 \mod \pi^{\epsilon_p+1}$, which implies that π divides c. Set $c = \pi c'$. Then $a_1'\lambda_1^2 + c' \equiv 0 \mod \pi^{\epsilon_p}$. Hence c' must be a unit. By Hensel's square criterion, $-c'a_1'^{-1}$ is a square in k, say $\theta^2 = -c'a_1'^{-1}$ for some $\theta \in k$. Then $(\theta, \lambda_2, \lambda_3, \ldots, \lambda_n)$ is a nontrivial zero of q in k. □

Remark 5.7. Let p be an odd prime, and let $q = \sum_{1\leq i\leq n} a_i X_i^2$ be a primitive quadratic form where $n \geq 3$ with each $a_i \in \mathbb{Z}$ and coprime to p. Then q has a nontrivial zero in $\mathbb{Q}_p$.

Proof. A simple counting argument which goes back to Euler yields the fact that forms of rank at least 3 are isotropic over finite fields. Thus q has a primitive zero modulo p, say $(\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n)$. Now we are back in Case I of the proof of the previous theorem. □

Proof of Proposition 3.3. Remark 5.7 tells us that q has nontrivial zeros in $\mathbb{Q}_p$ for odd primes p which do not divide any of the a_i. The hypotheses of Proposition 3.3 imply that q has primitive zeros modulo p^{ϵ_p+1} for each prime p dividing any of the a_i and for $p = 2$. The theorem of Hensel (Theorem 5.6) implies that q has a nontrivial zero in each corresponding $\mathbb{Q}_p$. Thus we have primitive zeros modulo p^m for every prime p and every integer $m \geq 1$. This in turn gives primitive zeros modulo N for every integer $N \geq 2$ by the Chinese remainder theorem. Since q is given to be an indefinite form, there is a nontrivial zero of q in $\mathbb{R}$. By the Hasse–Minkowski theorem (Theorem 3.2), we can conclude that there exists a nontrivial zero of q in $\mathbb{Q}$.

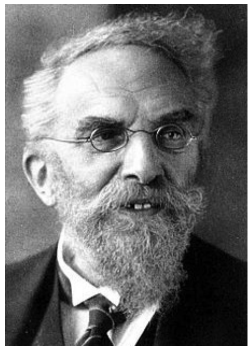
The Hasse–Minkowski theorem can also be stated as follows:

Theorem 5.8 (Hasse and Minkowski)**.** *Let q be a primitive quadratic form over $\mathbb{Q}$. If q is indefinite and isotropic over $\mathbb{Q}_p$ for every prime p, then q is isotropic over $\mathbb{Q}$.*

6. Hensel's vision

In his 1908 paper, *Neue Grundlagen der Arithmetik* in Crelle's journal, Hensel defined the p-adic numbers and proved the result that later became known as Hensel's lemma.

Even earlier, Hensel announced these results at the 1897 German Mathematical Association annual meeting along with a grand vision for the parallel development of algebraic number theory (i.e., the study of number fields) and analytic function theory (i.e., the study of function fields). The number field/function field analogy has seen tremendous development over the last century.



Kurt Hensel
(1861–1941)

Über eine neue Begründung der Theorie der algebraischen Zahlen.

Von **K. Hensel** in Berlin.

Die Analogie zwischen den Resultaten der Theorie der algebraischen Functionen einer Variabeln und der der algebraischen Zahlen hat mir schon seit mehreren Jahren den Gedanken nahe gelegt, die Zerlegung der algebraischen Zahlen mit Hülfe der idealen Primfactoren durch eine einfachere Behandlungsweise zu ersetzen, welche der Entwickelung der algebraischen Functionen in Potenzreihen für die Umgebung einer beliebigen Stelle völlig entspricht.

"The analogy between the results of the theory of algebraic functions of one variable and of algebraic numbers has struck me for several years, and could suggest replacing the decomposition of algebraic numbers into ideal prime factors with a simpler way of treatment, which is completely equivalent to the expansion of algebraic functions into power series in the neighborhood of a point." (Jahresbericht der Deutschen Mathematiker-Vereinigung **6**, 83–88.)

For a prime p and $q = p^r$, let $\mathbb{F}_q$ denote the finite field with q elements. A *global field* k is a finite extension of $\mathbb{Q}$ (a *number field*) or a finite extension of $\mathbb{F}_p(t)$ (a *function field*). A *local field* is a completion of a global field at a place, i.e., at a discrete valuation or at an archimedean absolute value. It is isomorphic to $\mathbb{R}$ or $\mathbb{C}$ (*archimedean* completions) or a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$ (*non-archimedean* completions).

Let k be a global field, and let Ω_k be the set of all discrete valuations of k. Let V_k denote the set of all places of k.

Example 6.1.

- $V_{\mathbb{F}_q(t)} = \Omega_{\mathbb{F}_q(t)}$ is in bijection with the set of monic irreducible polynomials in $\mathbb{F}_q[t]$ together with $\frac{1}{t}$.
- $V_{\mathbb{Q}}$ is in bijection with the set of primes together with the real place ∞.

The Hasse–Minkowski theorem holds for all global fields.

Theorem 6.2. *Let q be a quadratic form over a global field k. If q is isotropic over k_ν for every place $\nu \in V_k$, then q is isotropic over k.*

The above theorem for quadratic forms in three variables over number fields goes back to Hilbert ([17]).

7. Hasse principle for varieties

Let k be any field with $\operatorname{char}(k) \neq 2$. The equation $\sum_{1\leq i\leq n} a_i X_i^2 = 0$, where $a_i \in k^\star$ and $n \geq 3$, defines a *quadric hypersurface* $X \subset \mathbb{P}_k^{n-1}$ which is a smooth projective variety over k. The variety X has a k-rational point provided the defining quadratic form is isotropic. Let $X(k)$ denote the set of k-rational points of X. The Hasse–Minkowski theorem can be reformulated as

Theorem 7.1. *Let X be a smooth projective quadric over a global field k. If $X(k_\nu) \neq \emptyset$ for all $\nu \in V_k$, then $X(k) \neq \emptyset$.*

For a variety Y defined over a global field k, we say that Y satisfies the *Hasse principle* or a *local-global principle* if whenever $Y(k_\nu) \neq \emptyset$ for all $\nu \in V_k$, $Y(k) \neq \emptyset$. Quadrics are examples of varieties over number fields which satisfy the Hasse principle. These are projective homogeneous spaces. More generally, one has

Theorem 7.2 (Harder [9])**.** *Let G be a connected linear algebraic group defined over a number field k, and let X be a projective homogeneous space under G over k. Then X satisfies Hasse principle for the existence of rational points.*

8. Hasse principle for function fields and the u-invariant

It is natural to look for a Hasse principle for quadrics defined over a more general field with respect to a set of discrete valuations of the field. This has interesting consequences for determining the u-invariant.

Let E be any field with $\operatorname{char}(E) \neq 2$. The dimension of a quadratic form (V, q) is the dimension of the underlying vector space V. If q is nondegenerate, the number of variables in the polynomial representing q with respect to a basis of V is equal to the dimension of q.

Definition 8.1. The *u-invariant* of a field E is defined as

$$u(E) = \sup\{\dim(q) \mid q \text{ anisotropic quadratic form over } E\}$$

Example 8.2. Let F be a field with $\operatorname{char}(F) \neq 2$. Let $k = F((t))$ be the field of Laurent series over F. Since every power series of the form $1 + a_1 t + a_2 t^2 + \cdots + a_n t^n + \cdots$, where $a_i \in F$ is a square in $F[[t]]$, any $f \in F((t))$ can be written as

$$f = \lambda g^2, \lambda \in F, g \in F((t)) \text{ or } f = \lambda t g^2, \lambda \in F, g \in F((t)).$$

A quadratic form q over $F((t))$ can be diagonalised as $q_1 \perp tq_2$, where $q_1 = \langle \lambda_1, \lambda_2, \ldots, \lambda_r \rangle$ and $q_2 = \langle \mu_1, \mu_2, \ldots, \mu_s \rangle$ with $\lambda_i, \mu_j \in F$. The form q is isotropic if and only if q_1 or q_2 is isotropic over F. Thus,

$$u\big(F((t))\big) = 2u(F).$$

Example 8.3. Let $\mathbb{F}_q$ be a finite field with q odd. There is a unique nonsquare class, i.e., there is a nonsquare $\epsilon \in \mathbb{F}_q^\star$ such that every $a \in \mathbb{F}_q$ is either a square or ϵ times a square. It follows that $u(\mathbb{F}_q) = 2$.

Example 8.4. Let k be a local field which is not isomorphic to $\mathbb{R}$ or $\mathbb{C}$. Using ideas similar to those in Example 8.2, it can be shown that $u(k) = 4$.

Example 8.5. Let k be a global field without an ordering. Then by the Hasse–Minkowski theorem (Theorem 6.2), $u(k) = 4$.

We would like to study the finiteness of the u-invariant of function fields of curves over p-adic fields or number fields via the Hasse principle with respect to divisorial discrete valuations which are defined as follows:

Let k be a p-adic field or a number field, and let X be a smooth projective geometrically integral curve over k. Let K be the function field of X. Let $\mathcal{O}$ denote the integers in k. A *divisorial discrete valuation of* K is a discrete valuation of K centered on a codimension 1 point of some regular proper model $\mathcal{X}/\mathcal{O}$ of X.

8.1. **Function fields of curves over p-adic fields.** Let $K = \mathbb{Q}_p(t)$. Let Ω_K^0 be the set of all divisorial discrete valuations of K. For $\nu \in \Omega_K^0$, let K_ν denote the completion of K at ν.

- If ν is trivial on $\mathbb{Q}_p$, then K_ν is isomorphic to $k((t))$ where k is a finite extension of $\mathbb{Q}_p$. The residue field $\kappa(\nu)$ at ν is isomorphic to k.
- If ν restricts to the p-adic valuation on $\mathbb{Q}_p$, then K_ν is a complete discrete valued field with residue field $\kappa(\nu)$ a finite extension of $\mathbb{F}_p(t)$.

In either case, by the Hasse–Minkowski theorem, $u\big(\kappa(\nu)\big) = 4$ so that $u\left(K_\nu\right) = 8$. If the Hasse principle holds for quadrics over K with respect to Ω_K^0, it would follow that $u\big(\mathbb{Q}_p(t)\big) = 8$, i.e., every quadratic form in at least nine variables over $\mathbb{Q}_p(t)$ would have a nontrivial zero. Whether $u\left(\mathbb{Q}_p(t)\right) = 8$ was a longstanding open question (cf. [27, pp. 248–249]). Even the finiteness of $u\big(\mathbb{Q}_p(t)\big)$ remained open until the late 1990s. The first finiteness results were due to Merkurjev and independently to Hoffman and VanGeel ([18]). We refer to [4] for a brief summary of results concerning the u-invariant of function fields of p-adic curves. We have

- $u\big(\mathbb{Q}_p(t)\big) = 8$ for $p \neq 2$ ([24]).
- $u\big(\mathbb{Q}_p(t)\big) = 8$ for all p ([14], [19]).

The theorems quoted above do not invoke a Hasse principle for quadrics. A proof that $u\big(\mathbb{Q}_p(t)\big) = 8$ for $p \neq 2$ via the Hasse principle is due to Colliot-Thélène, Parimala, and Suresh ([5]):

Theorem 8.6. *Let K be a function field in one variable over a p-adic field with $p \neq 2$. Then the Hasse principle holds for isotropy of quadrics in at least three variables over K with respect to the set of divisorial discrete valuations of K.*

The proof of the above theorem uses *patching* techniques and theorems developed by Harbater, Hartman, and Krashen ([7], [8]).

8.2. **Function fields of curves over number fields.** Let k be a totally imaginary number field. There are open questions concerning the u-invariant of function fields in one variable over k.

Question I. Is $u\big(\mathbb{Q}(\sqrt{-1})(t)\big) < \infty$?

Question I′. Is $u\big(\mathbb{Q}(\sqrt{-1})(t)\big) = 8$?

Even Question I is wide open. Let us look at these questions from the viewpoint of the Hasse principle.

Let $K = \mathbb{Q}\left(\sqrt{-1}\right)(t)$, and let Ω_K^0 be the set of divisorial discrete valuations of K. Let $\nu \in \Omega_K^0$.

- If ν is trivial on $\mathbb{Q}\left(\sqrt{-1}\right)$, then $K_\nu \simeq k((t))$ where k is the residue field at ν which is a finite extension of $\mathbb{Q}\left(\sqrt{-1}\right)$.

- If ν restricts to a discrete valuation on $\mathbb{Q}\left(\sqrt{-1}\right)$ extending the p-adic valuation of $\mathbb{Q}$, then K_ν is a complete discrete valued field with residue field $\kappa(\nu)$ a finite extension of $\mathbb{F}_p(t)$.

In either case, by the Hasse–Minkowski theorem, $u\big(\kappa(\nu)\big) = 4$ and hence $u\left(K_\nu\right) = 8$. If the Hasse principle were true for quadratic forms over K with respect to Ω_K^0, one would get $u\left(\mathbb{Q}\left(\sqrt{-1}\right)(t)\right) = 8$. This seems to be a difficult question. However, there are some conditional results in this direction. In order to explain these results, we begin with the definition of the Brauer–Manin obstruction for the existence of zero-cycles on a smooth projective variety.

8.3. **The Brauer–Manin obstruction.** The Brauer group of a field was introduced by Richard Brauer to study finite dimensional division algebras over the field.

A central simple algebra over a field E is a finite dimensional E-algebra which becomes isomorphic to a matrix algebra over the algebraic closure of E. Given a central simple algebra A over k, there is a finite dimensional central division algebra D_A over k, uniquely determined by A up to isomorphism, such that $A \cong M_r\left(D_A\right)$. The Brauer equivalence on central simple algebras is defined as follows: $A \sim B$ if and only if $M_n(A) \cong M_m(B)$ for some integers $m, n \geq 1$, which happens if and only if $D_A \cong D_B$. A Brauer equivalence class is represented by a central division algebra over E. Brauer equivalence classes of central simple algebras over E form an abelian group under the tensor product operation, called the Brauer group of E, denoted $\mathrm{Br}(E)$.

The following reciprocity (exact) sequence for a global field k is due (independently) to Hasse, Brauer, and Noether and to Albert:

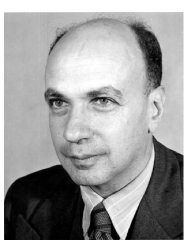
$$1 \to \mathrm{Br}(k) \to \bigoplus_{\nu \in V_k} \mathrm{Br}\left(k_\nu\right) \xrightarrow{\sum \mathrm{inv}_\nu} \mathbb{Q}/\mathbb{Z} \to 0$$

Let D be a finite dimensional central division algebra over k of dimension n^2. Let X_D be the Brauer–Severi variety associated to D introduced by Châtelet, namely, the scheme of left ideals of D of dimension n over k. The variety X_D has a rational point over an extension E of k if and only if $D \otimes_k E$ is a matrix algebra. In view of the above reciprocity sequence, one gets a Hasse principle for X_D:

$$X_D\left(k_\nu\right) \neq \emptyset \;\forall\; \nu \in V_k \implies X_D(k) \neq \emptyset.$$

Let X be a smooth projective geometrically integral variety defined over a field E. Let $Z_0(X)$ be the group of zero cycles on X, i.e., the free abelian group on the

Helmut Hasse (1898–1979)



Richard Brauer (1901–1977)

Emmy Noether (1882–1935)

A. Adrian Albert (1905–1972)

set of closed points of X. The degree map $\deg : Z_0(X) \to \mathbb{Z}$ is defined as

$$\deg\left(\sum_i n_i x_i\right) = \sum_i n_i[\kappa\,(x_i) : E],$$

where $\kappa\,(x_i)$ denotes the residue field at x_i. Let $Z_0^1\,(X)$ denote the set of zero cycles of degree 1 on X. Let $\mathrm{Br}(X)$ denote the Brauer group of the scheme X ([6]). Every element α in $\mathrm{Br}(X)$ is represented by a sheaf of Azumaya algebras on X. For a closed point x in X, let $\alpha_x \in \mathrm{Br}\,(\kappa(x))$ denote the specialization of α at x. Given a zero cycle $z = \sum_i n_i x_i$ on X, we define $\alpha_z \in \mathrm{Br}(k)$ to be $\sum_i n_i\, \mathrm{cores}_{\kappa(x_i)/k}\,(\alpha_{x_i})$.

Let k be a number field, and let X be a smooth projective geometrically integral variety over k. By the reciprocity sequence, given $\alpha \in \mathrm{Br}(X)$ and a zero cycle z on X, $\sum_\nu \mathrm{inv}_\nu\,(\alpha_z) = 0$. We look for a local-global principle for the existence of zero cycles of degree 1 on X. An obstruction is given by the Brauer–Manin set:

$$\left(\prod_{\nu\in V_k} Z_0^1\,(X_{k_\nu})\right)^{\mathrm{Br}(X)} = \left\{\{z_\nu\}_{\nu\in V_k}, z_v \in Z_0^1\,(X_{k_\nu})\,, \sum_\nu \mathrm{inv}_\nu\,(\alpha_{z_\nu}) = 0\ \forall\ \alpha \in \mathrm{Br}(X)\right\}.$$

We have

$$Z_0^1(X) \subseteq \left(\prod_{\nu\in V_k} Z_0^1\,(X_{k_\nu})\right)^{\mathrm{Br}(X)} \subseteq \prod_{\nu\in V_k} Z_0^1\,(X_{k_\nu})\,.$$

We say that the Brauer–Manin obstruction is the only obstruction for the existence of zero cycles on X if

$$\left(\prod_{\nu\in V_k} Z_0^1\,(X_{k_\nu})\right)^{\mathrm{Br}(X)} \neq \emptyset \implies Z_0^1(X) \neq \emptyset.$$

It is known that the analogous Brauer–Manin obstruction for the existence of rational points is not the only obstruction to the existence of rational points on X (Skorobogatov [28]).

Colliot-Thélène Conjecture ([3])**.** *Let X be a smooth projective geometrically integral variety over a number field k. Then the Brauer–Manin obstruction is the only obstruction to the existence of zero-cycles of degree 1 on X.*

We have the following conditional result for the finiteness of the u-invariant of function fields of curves over number fields.

Theorem 8.7 (Lieblich, Parimala, and Suresh ([20]))**.** *Suppose that Colliot-Thélène conjecture is true. Let K be a function field in one variable over a number field. Then the u-invariant of K is finite.*

Ackowledgments

The author thanks A. Auel, J.-L. Colliot-Thélène, D. Leep, and M. Ojanguren for their profound help in the preparation of the text. The author also thanks N. Bhaskhar and Sumati Varadarajan for their timely help in producing this document.

About the author

R. Parimala is Arts and Sciences Distinguished Professor at Emory University, Atlanta. She was on the faculty of the Tata Institute of Fundamental Research, Mumbai, India, before she moved to Emory University.

References

[1] R. Brauer, H. Hasse and E. Noether, *Beweis eines Hauptsatzes in der Theorie der Algebren*, J. Reine Angew. Math. **167** (1931), 399-404.

[2] Jean-Louis Colliot-Thélène, *L'arithmétique des variétés rationnelles* (French, with English and French summaries), Ann. Fac. Sci. Toulouse Math. (6) **1** (1992), no. 3, 295–336. MR1225663 (94i:11040)

[3] J.-L. Colliot-Thélène, *Conjectures de type local-global sur l'image des groupes de Chow dans la cohomologie étale* (French), Algebraic K-theory (Seattle, WA, 1997), Proc. Sympos. Pure Math., vol. 67, Amer. Math. Soc., Providence, RI, 1999, pp. 1–12. MR1743234 (2001d:11067)

[4] J.-L. Colliot-Thélène, *Quadrics over function fields in one (or more) variables over a p-adic field*, Exposé à l'Institut Hausdorff, Bonn, (2009) : `http://www.math.u-psud.fr/~colliot/liste-cours-exposes.html`, 18.

[5] Jean-Louis Colliot-Thélène, Raman Parimala, and Venapally Suresh, *Patching and local-global principles for homogeneous spaces over function fields of p-adic curves*, Comment. Math. Helv. **87** (2012), no. 4, 1011–1033, DOI 10.4171/CMH/276. MR2984579

[6] Alexander Grothendieck, *Le groupe de Brauer. I. Algèbres d'Azumaya et interprétations diverses* (French), Dix Exposés sur la Cohomologie des Schémas, North-Holland, Amsterdam, 1968, pp. 46–66. MR0244269 (39 #5586a)

[7] David Harbater and Julia Hartmann, *Patching over fields*, Israel J. Math. **176** (2010), 61–107, DOI 10.1007/s11856-010-0021-1. MR2653187 (2012a:12009)

[8] David Harbater, Julia Hartmann, and Daniel Krashen, *Applications of patching to quadratic forms and central simple algebras*, Invent. Math. **178** (2009), no. 2, 231–263, DOI 10.1007/s00222-009-0195-5. MR2545681 (2010j:11058)

[9] Günter Harder, *Bericht über neuere Resultate der Galoiskohomologie halbeinfacher Gruppen* (German), Jber. Deutsch. Math.-Verein. **70** (1967/1968), no. Heft 4, Abt. 1, 182–216. MR0242838 (39 #4165)

[10] H. Hasse, *Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen*, J. Reine Angew. Math. **152** (1923), 129–148.

[11] H. Hasse, *Über die Äquivalenz quadratischer Formen im Körper der rationalen Zahlen*, J. Reine Angew. Math. **152** (1923), 205–224.

[12] H. Hasse, *Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper*, J. Reine Angew. Math. **153** (1924), 113–130.

[13] H. Hasse, *Äquivalenz quadratischer Formen in einem beliebigen algebraischen Zahlkörper*, J. Reine Angew. Math. **153** (1924), 158–162.

[14] D. R. Heath-Brown, *Zeros of systems of $\mathfrak{p}$-adic quadratic forms*, Compos. Math. **146** (2010), no. 2, 271–287, DOI 10.1112/S0010437X09004497. MR2601629 (2011e:11066)

[15] K. Hensel, *Über eine neue Begründung der Theorie der algebraischen Zahlen*, Jahresbericht der Deutschen Mathematiker-Vereinigung **6** (1897), 83–88.

[16] K. Hensel, *Zahlentheorie*, Göschen, Berlin, (1913).

[17] D. Hilbert, *Über die Theorie des relativquadratischen Zahlkörpers*, Mathematische Annalen **51(1)** (1898), 1-127.

[18] Detlev W. Hoffmann and Jan Van Geel, *Zeros and norm groups of quadratic forms over function fields in one variable over a local non-dyadic field*, J. Ramanujan Math. Soc. **13** (1998), no. 2, 85–110. MR1666433 (2000c:11058)

[19] David B. Leep, *The u-invariant of p-adic function fields*, J. Reine Angew. Math. **679** (2013), 65–73. MR3065154

[20] M. Lieblich, R. Parimala and V. Suresh, Colliot-Thélène's conjecture and finiteness of u-invariants (2012), *arXiv preprint arXiv:1209.6418.*

[21] Carl-Erik Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins* (German), Thesis, University of Uppsala, **1940** (1940), 97. MR0022563 (9,225c)

[22] H. Minkowski, *Mémoire sur la théorie des formes quadratiques à coëfficients entiers*. Paris. Impr. nationale. Extrait des Mém. présentés par divers savants à l'ac. des sc. de l'Inst. de France 29, (1884).

[23] H. Minkowski, *Über die Bedingungen, unter welchen zwei quadratische Formen mit rationalen Coefficienten ineinander rational transformiert werden können*, J. Reine Angew. Math. **106** (1890), 5–26.

[24] Raman Parimala and V. Suresh, *The u-invariant of the function fields of p-adic curves*, Ann. of Math. (2) **172** (2010), no. 2, 1391–1405, DOI 10.4007/annals.2010.172.1397. MR2680494 (2011g:11074)

[25] Emmanuel Peyre, *Obstructions au principe de Hasse et à l'approximation faible* (French, with French summary), Astérisque **299** (2005), Exp. No. 931, viii, 165–193. Séminaire Bourbaki. Vol. 2003/2004. MR2167206 (2007b:14041)

[26] Hans Reichardt, *Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen* (German), J. Reine Angew. Math. **184** (1942), 12–18. MR0009381 (5,141c)

[27] Jean-Pierre Serre, *Cohomologie galoisienne: progrès et problèmes* (French, with French summary), Astérisque **227** (1995), Exp. No. 783, 4, 229–257. Séminaire Bourbaki, Vol. 1993/94. MR1321649 (97d:11063)

[28] Alexei N. Skorobogatov, *Beyond the Manin obstruction*, Invent. Math. **135** (1999), no. 2, 399–424, DOI 10.1007/s002220050291. MR1666779 (2000c:14022)

[29] André Weil, *Number theory: An approach through history; From Hammurapi to Legendre*, Birkhäuser Boston Inc., Boston, MA, 1984. MR734177 (85c:01004)

Department of Mathematics & Computer Science, Emory University, 400 Dowman Drive NE, Atlanta, Georgia 30322

E-mail address: parimala@mathcs.emory.edu