Proceedings of International Mathematical Sciences
ISSN:2717-6355, URL:https://dergipark.org.tr/tr/pub/pims
Volume III Issue 2 (2021), Pages 98-108
Doi:

THE HASSE-MINKOWSKI THEOREM AND LEGENDRE'S THEOREM FOR QUADRATIC FORMS IN TWO AND THREE VARIABLES

PHUC NGO*, MEHMET DIK**
*BELOIT COLLEGE, BELOIT, WI 53511, U.S.A ORCID NUMBER: 0000-0002-9658-4877
**BELOIT COLLEGE, BELOIT, WI 53511, U.S.A. ORCID NUMBER: 0000-0003-0643-2771

Abstract. Determining the solvability of equations has been an extended and fundamental study in Mathematics. The local-global principle states two objects are equivalent globally if and only if they are equivalent locally at all places. By applying this principle, the Hasse - Minkowski theorem is able to identify the existence of rational solutions of an equation. This paper explores the applications of the Hasse-Minkowski theorem to homogeneous quadratic forms in two and three variables. After providing some of the necessary proofs and definitions, we have been able to introduce some complete computer programs implementing the Hasse-Minkowski theorems and Legendre theorem with some supporting functions like the Eratosthenes sieve.

Reasons for Retraction. Our paper was hugely inspired by Dr. Hohner's master thesis, "The Hasse-Minkowski Theorem in Two and Three Variables." More than half the length of our paper is our original programming implementation of various theorems, like the Hasse-Minkowski theorem and Legendre's theorem, and many supporting concepts, along with the algorithm analysis. We also shorten many proofs from Dr. Hohner's paper by either providing an alternative shorter version or summarizing them. We credit him in section 1 on the binary and ternary quadratic form and the bibliography. However, the location of the credit section 1 was supposed to be before section 1, and this is a formatting mistake. Even though we made an effort to credit Dr. Hohner's work, it could still be insufficient. We think it would be best to retract the paper for those listed reasons.

1. binary and ternary quadratic form

What follows has been inspired by *The Hasse-Minkowski Theorem in Two and Three Variables* by Hoehner, S [1].
A quadratic form is a polynomial with all the terms of degree two. The 2-variable quadratic form, which is also called binary form, has the following general form:

$$q(x, y) = ax^2 + bxy + cy^2. \tag{1.1}$$

2020 *Mathematics Subject Classification.* Primary: 11C04; Secondaries: 11C00.
Key words and phrases. Hasse-Minkowksi; quadratic form; algorithm.

Submitted on Published on Communicated by .

Similarly, the 3-variable quadratic form is called the ternary form and has the general form of:

$$q(x, y, z) = ax^2 + bxy + cy^2 + dyz + ez^2 + fxz. \tag{1.2}$$

Theorem 1.1. *Every quadratic form q in n variables over a field of characteristic not equal to 2 is equivalent to a diagonal form:*

$$q(x) = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2. \tag{1.3}$$

Since the general form is equivalent to diagonal form, we only need to consider the diagonal form to determine the integral solvability. Hence, we just need to look at the equations of form $q(x, y) = ax^2 + by^2$ for the binary case and $q(x, y) = ax^2 + by^2 + cz^2$, where a, b and c are integers.

Consider the binary diagonal form. If we have any rational coefficient, by the homogeneity of the equation $g(x, y) = 0$, we could clear the denominators to obtain an equation with integral coefficients. We also claim that the greatest common divisor of a and b is 1. Given that $gcd(a, b) = g$ and $g > 1$, we could divide $ax^2 + by^2 = 0$ by g to get $q(x, y) = \frac{a}{g}x^2 + \frac{b}{g}y^2$ and obtain $gcd(\frac{a}{g}, \frac{b}{g}) = 1$.

Also, we assume that a and b are square-free. If a is not square-free, $a = a's^2$, where a' is an integer. Then, we have $a = ax^2 + by^2 = a'(sx)^2 + by^2 = 0$. We could repeat the same process to clear all the squares from a and b which eventually leads to square-free coefficients.

Finally, we claim that $ab < 0$. If $ab = 0$, either one or both of the coefficients is 0 and we could not obtain a non-trivial solution. And, if $ab > 0$, the equation $f(x, y) = ax^2 + by^2$ will not have any solution since it would be either negative or positive.

Similarly, following the same reasoning, we get pairwise relatively prime, square-free coefficients for ternary form.

2. MODULAR ARITHMETIC

Definition 2.1. *An integer is called a quadratic residue modulo n if there exists an integer x such that*

$$x^2 \equiv q \ (mod\ n). \tag{2.1}$$

Due to the Legendre symbol, we could speed up the process of determining if a number is a quadratic residue modulo an odd prime. The Legendre symbol is defined as below.

Definition 2.2. *The Legendre symbol is a function of a and p, where p is an odd prime, defined as:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p}, \\ -1 & \text{if } a \text{ is a non-quadratic residue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases} \tag{2.2}$$

In addition, the Legendre symbol has the following properties:

(1) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(2) If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
(3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
(4) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
(5) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)\cdot(q-1)}$.

For the proof of above Legendre symbol properties, see pages 99, 100 and 102 in [3].

Furthermore, if an odd integer n has the prime factorization of $p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}$ and any integer a, we have a generalization of the Legendre symbol called the Jacobi symbol, stating that:

$$\left(\frac{a}{1}\right) = 1 \tag{2.3}$$

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}\cdots\left(\frac{a}{p_k}\right)^{\alpha_k}. \tag{2.4}$$

Similar to the Legendre symbol, the Jacobi symbol also has some properties that we use to prove the Hasse-Minkowski theorem:

(1) $\left(\frac{a_1a_2}{n}\right) = \left(\frac{a_1}{n}\right)\left(\frac{a_2}{n}\right)$
(2) If $a_1 \equiv a_2 \pmod{n}$, then $\left(\frac{a_1}{n}\right) = \left(\frac{a_2}{n}\right)$
(3) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$
(4) $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$
(5) If $gcd(a,n) = 1$, then $\left(\frac{a}{n}\right)\left(\frac{n}{a}\right) = (-1)^{\frac{1}{4}(a-1)\cdot(n-1)}$

3. The Hasse-Minkowski theorem for binary forms

In order to prove the Hasse-Minkowski theorem for binary forms, we need the following theorems.

Theorem 3.1. *The Chinese Remainder Theorem. Suppose n_i are pairwise coprime and a_1, a_2,...,a_k is any sequence of integers, then there exists an integer x such that:*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned} \tag{3.1}$$

and the solution x is unique modulo n, where $n = \prod_{i=1}^{k} n_i$.

Theorem 3.2. *Suppose a is an integer, b is a natural number, and let $b = \prod_{i=1}^{n} p_i^{\varepsilon_i}$ be the prime factorization of b. Then a is a quadratic residue modulo b if and only if a is a quadratic residue modulo $p_i^{\varepsilon_i}$ for $i = 1, \dots, n$.*

Proof for Theorem 3.2. Suppose a is a quadratic residue modulo b. We then have $a \equiv x^2 \pmod{b}$ for some integer x. Since $p_i^{\varepsilon_i} \mid b$, we also have $a \equiv x^2 \pmod{p_i^{\varepsilon_i}}$.

To prove the order direction, if a is a quadratic residue modulo $p_i^{\varepsilon_i}$, we have $a \equiv x^2$

(mod $p_i^{\varepsilon_i}$), if $j \neq k$, $gcd(p_j^{\varepsilon_j}, p_k^{\varepsilon_k})$. Thus, we could apply the Chinese Remainder Theorem to the congruences $x \equiv x_i \pmod{p_i^{\varepsilon_i}}$ where $i = 1, \ldots, n$. Obtaining $x^2 \equiv x_i^2 \equiv a \pmod{p_i^{\varepsilon_i}}$ from the Chinese Remainder theorem, we thus have $x^2 \equiv a \pmod{\prod_{i=1}^{n} p_i^{\varepsilon_i}}$ or a is a quadratic residue modulo b.

Theorem 3.3. *Dirichlet's Theorem on Arithmetic Progressions. For any two positive coprime integers a and d, there are infinitely many primes of the form $a+nd$, where n is also a positive integer*

Theorem 3.4. *The congruence $x^2 \equiv a \pmod{p}$ is solvable for every prime p if and only if $a = b^2$ for some $b \in \mathrm{Z}$.*

Proof for Theorem 3.4. Suppose $a = b^2$ for some b, we have $x^2 \equiv a \equiv b^2 \pmod{p}$. Therefore, for all prime p, we have a solution $x \equiv b \pmod{p}$.
To prove the other direction, we try to prove an equivalent statement "if $a \neq b^2$ for some b, a is not a quadratic residue modulo for every prime p."
Suppose a is a positive non-square. Then, if $a = 2$, we could just choose $p = 5$ and apply property 4 from the Legendre symbol to get $\left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$. Otherwise, a could be factored into $p_1 p_2 \ldots p_k$ for $p_1, \ldots, p_k$ prime. Also, a has an odd prime divisor p_k. Now we choose a prime such that $p \equiv 1 \pmod{8}$, $p \equiv 1 \pmod{p_i}$ for $i = 1, 2, \ldots, k-1$ and $p \equiv a \pmod{p_k}$. Such a prime number p exists according to Theorem 3.3. Then, since p_k is not a quadratic residue modulo p, a is not a quadratic non residue modulo p. Thus, we have proved Theorem 3.4 for the case where a is positive.
If a number is negative, it is not a square. We present all negative numbers in the form of $-a$ where a is a positive integer. Let p be a prime number and apply property 1 from the Legendre symbol to get $\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)$. We then apply property 3 to obtain $\left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{a}{p}\right)$. If a is a square, we can choose $p = 3$ to get $(-1)^{\frac{3-1}{2}}\left(\frac{a}{p}\right) = (-1) \cdot 1 = -1$. If a is a non square, we choose $p = 5$ to obtain $(-1)^{\frac{5-1}{2}}\left(\frac{a}{p}\right) = 1 \cdot (-1) = -1$.

Theorem 3.5. *The Hasse-Minkowski Theorem 1. Let a and b be nonzero, square-free, relatively prime integers of opposite signs. If for each prime p the congruence $ax^2 + by^2 \equiv 0$ (mod p) has a solution in integers (x, y) both not divisible by p, then $ax^2 + by^2 = 0$ has a nontrivial integral solution.*

Consider the first case where $p \nmid ab$, we claim that $gcd(x, p) = 1$. We can prove this statement by using contradiction. Suppose $gcd(x, p) > 1$, then we have $p \mid x$. Hence, $ax^2 + by^2 \equiv by^2 \equiv 0 \pmod{p}$. Also, we could see that either $p \mid b$ or $p \mid y$. Since we assume that $p \nmid ab$, we have $p \mid y$. Now that we have $p \mid x$ and $p \mid y$, this contradicts our assumption that the solution (x, y) to nontrivial modulo p, establishing our claim that $gcd(x, p) = 1$. Now, from $ax^2 + by^2 \equiv 0 \pmod{p}$, we have $ax^2 \equiv -by^2 \pmod{p}$ and by multiplying the congruence on both sides by $-b$, we obtain $-bax^2 \equiv (by)^2 \pmod{p}$. Since $gcd(x, p) = 1$, we could divide

$-bax^2 \equiv (by)^2$ by x^2 to obtain $-ba \equiv (\frac{by}{x})^2$. Thus, $-ba$ is a quadratic residue modulo p for all $p \nmid ab$. Now, assume $p \mid ab$. We have $-ab \equiv 0^2 \pmod{p}$, therefore $-ab$ is a quadratic residue modulo p for all $p \mid ab$.
Thus, $-ba$ is a quadratic residue modulo for all primes p. According to Theorem 3.4, we have $-ba = d^2$ for some integer d. Plugging the pair of integer (b, d) into $f(x, y)$, we obtain $f(b, d) = ab^2 + bd^2 = ab^2 + b(-ab) = 0$. Hence, we have found a nontrivial integral solution to equation $f(x, y) = 0$.

4. THE HASSE-MINKOWSKI THEOREM FOR TERNARY FORMS

Theorem 4.1. *Legendre's Theorem. Suppose a, b, c are non-zero square-free, pairwise relatively prime integers not all of the same sign. Then the equation $ax^2 + by^2 + cz^2 = 0$ has a non-trivial solution if and only if the following conditions are satisfied: (i) $-bc$ is a quadratic residue modulo $|a|$, (ii) $-ab$ is a quadratic residue modulo $|c|$, and (iii) $-ac$ is a quadratic residue modulo $|b|$.*

Definition 4.1. *Let (x_0, y_0, z_0) be a nontrivial integral solution to the congruence $ax^2 + by^2 + cz^2 \equiv 0$ (mod p), and at most one of x_0, y_0, z_0 is divisible by p, then we call (x_0, y_0, z_0) a p-focused solution.*

Theorem 4.2. *Hasse-Minkowski 2. Let a, b, c be nonzero, square-free, pairwise relatively prime integers not all the same sign. If for each odd prime $p \mid abc$ the congruence $ax^2 + by^2 + cz^2 \equiv 0$ (mod m) has a p-focused solution in integers (x, y, z), then $ax^2 + by^2 + cz^2 = 0$ has a nontrivial integral solution.*

Proof for theorem 4.2. Let p be an odd prime, $p \mid a$ and $f(x, y, z) \equiv 0 \pmod{p}$ has a p-focused solution. According to Theorem 3.2, to prove $-bc$ is a quadratic residue modulo $|a|$, it suffices to show $-bc$ is a quadratic residue modulo p for all $p \mid a$.
Suppose (x_0, y_0, z_0) is a p-focused solution to the congruence. Since $p \mid a$, we have $by_0^2 + cz_0^2 \equiv 0 \pmod{p}$. If $p = 2$ or $p \mid bc$, we have $-bc \equiv 0 \pmod{p}$ and it is a quadratic residue modulo p. If $p \nmid bc$, we obtain $\gcd(b, p) = \gcd(c, p) = 1$. We also know that at most one of x_0, y_0, z_0 is divisible by p. First, suppose p doesn't divide x_0, y_0 or z_0. We have

$$-by_0^2 \equiv cz_0^2 \pmod{p}. \tag{4.1}$$

Divide both sides by z_0^2 to get

$$-b(y_0 z_0^{-1})^2 \equiv c \pmod{p}. \tag{4.2}$$

Multiply both sides by $-b$ to obtain

$$-bc \equiv (by_0 z_0^{-1})^2 \pmod{p}. \tag{4.3}$$

Now suppose p divides exactly one of x_0, y_0, z_0. In the case where $p \mid x_0$, we are done. Suppose $p \mid y_0$ and $p \nmid z_0$, we have

$$cz_0^2 \equiv 0 \pmod{p}. \tag{4.4}$$

Divide both sides by z_0 to get

$$c \equiv 0 \pmod{p}. \tag{4.5}$$

Multiply both sides by $-b$ to obtain

$$-bc \equiv 0 \pmod{p}. \tag{4.6}$$

So, we have $-bc$ a quadratic modulo p. Hence, $-bc$ is a quadratic residue modulo p. The case where $p \mid z_0$ and $p \nmid y_0$ could be proved using a similar procedure. Since the congruence $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}$ has a p-focused solution for all $p \mid a$, we have $-bc$ a quadratic residue modulo $|a|$. Similarly, we can determine that $-ac$ is a quadratic residue modulo $|b|$ and $-ab$ is a quadratic modulo c.
We do not need to consider the case where p is even or $p = 2$ since $-bc$, $-ac$, $-ad$ are either odd and even. Thus, they are congruent to 0 or 1 modulo 2 and both 0 and 1 are squares.
Finally, we need to show that if $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}$ has a p-focused solution for all odd $p \mid abc$, then $f(x, y, z) = 0$ has a nontrivial integral solution. Since $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}$ has a p-focused solution for all odd $p \mid abc$, it has a p-focused solution for all odd $p \mid a$, $p \mid b$ and $p \mid c$. We can also determine that $-bc$ is a quadratic residue modulo $|a|$, $-ac$ is a quadratic residue modulo $|b|$, $-ab$ is a quadratic residue modulo $|c|$. Hence, according to the Legendre's Theorem, the equation $ax^2 + by^2 + cz^2 = 0$ has a nontrivial integral solution.

5. HASSE-MINKOWSKI AND LEGENDRE THEOREM IMPLEMENTATION

Let $f(x, y, z) = ax^2 + by^2 + cz^2$. Obviously, since checking whether a congruence $f(x, y, z) \equiv 0 \pmod{p}$ has a p-focused solution is a tedious task in real life, especially when abc has a lot of prime factors or when a, b, c are large, we could write a computer program to check it.

Eratosthenes Sieve

Eratosthenes Sieve is an old algorithm used to rapidly identify all the primes to a certain limit. The program first gets the integers a, b and c from the keyboard. Then, it creates the Eratosthenes sieve of primes that are odd and divide abc. The code below is the modified Eratosthenes sieve function written in C++.
The parameter *upperBound* is the maximum number which we would check if it is a prime number. The program always calls the function with $upperBound = abc$. Then, we create a bitset, a data structure that stores bits, named *flag*. Suppose i is a number from 2 to $upperBound$, given that $flag[i] = 1$, then i is prime, and vice versa. Next, we reset our bitset which would set all the value of *flag* to 1. Our first loop iterates from 2 to $upperBound$ and for every number, if *flag[i]* $= 1$. Next, we process the second loop that iterates every multiple of that prime number to $upperBound$. For every multiples of that prime, we set the corresponding $flag$ value to 0 since the multiple of a prime can not be a prime. After the second loop, we would append our prime to a vector named *primes* to store it.

Function. $sieve(upperBound)$

Pseudocode

Input. $upperBound$, the maximum number to check if it is a prime number.
Determine. Every prime less than or equal to $upperBound + 1$.

(1) $primes \leftarrow$ an empty dynamic array, $flag \leftarrow$ an bitset
(2) $upperBound \leftarrow |upperBound|$
(3) for $i \leftarrow 0$ to 1000009
(4) $\quad flag_i \leftarrow 1$

(5) for $i \leftarrow 2$ to $upperBound + 1$
(6) if $flag_i = 1$
(7) $j \leftarrow 2i$
(8) while $j <= sievesize$
(9) $flag_j \leftarrow 0$
(10) if $i \neq 2$ and $flag_i \equiv 0 \pmod{upperBound}$
(11) append i to $primes$

C++ Implementation

```
bitset<10000010> flag;
vector<int> primes;
int a, b, c;

void sieve(long upperBound) {
    upperBound = abs(upperBound);
    flag.set();
    flag[0] = flag[1] = 0;
    for (long long i = 2; i <= upperBound; i++)
        if (flag[i]) {
            for (long long j = i * i; j <= upperBound; j += i) flag[j] = 0;
            if(i != 2 && upperBound % i == 0) primes.push_back((int)i);
        }
}
```

The Hasse-Minkowski Theorem 2

Suppose p is a prime that divides abc. To check for p-focused solution, we write a boolean method, *pFocusedCheck*, with parameter *primes*, the prime to check. *pFocusedCheck* has three loops that create every combination of x, y, z, where x, y, z are integer and less than *primes*. For every combination, if it is a *primes*-focused solution we immediately return true. After it finishes three loops, we would haven't found a *primes*-focused solution, thus return false.

Function. *pFocusedCheck*(*prime*)

Pseudocode

Input. *primes*, the prime number to look for a *primes*-focused solution to the congruence.

Output. Return true if there is a *primes*-focused solution, otherwise returns false.

(1) $x \leftarrow$ an int, $y \leftarrow$ an int, $z \leftarrow$ an int
(2) for $x \leftarrow 0$ to $prime - 1$
(3) for $y \leftarrow 0$ to $prime - 1$
(4) for $z \leftarrow 0$ to $prime - 1$
(5) if $ax^2 + by^2 + cz^2 \equiv 0 \pmod{primes}$ and at most one of x, y, z is divisible by *primes*.
(6) return true
(7) return false

C++ Implementation

```
bool pFocusedCheck(int prime){
    int x, y, z;
```

```
    for(x = 0; x < prime; ++x){
        for(y = 0; y < prime; ++y){
            for(z = 0; z < prime; ++z){
                if((((a * (x * x))  + (b * (y * y)) + (c * (z * z))) % prime == 0)
                   && (((x % prime) == 0) + ((y % prime) == 0) + ((z % prime) == 0) <= 1)){
                    return true;
                }
            }
        }
    }
    return false;
}
```

Then, we create a function named $HasseMinkowski2Check$ that loops through the *sieve* vector to check whether the congruence $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}$ has a p-focused solution. The function returns true if the congruence has a p-focused solution to every p, otherwise, returns false.

Function. $HasseMinkowski2Check()$

Pseudocode

Output. Returns true if for every p, the congruence $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}$ has a p-focused solution, otherwise, returns false.

(1) for every prime in *primes*
(2) if not *pFocusedCheck*(prime)
(3) return false
(4) return true

C++ Implementation

```
bool HasseMinkowski2Check(){
    for(int i = 0; i < primes.size(); ++i){
        if(!pFocusedCheck(primes[i])){
            return false;
        };
    }
    return true;
}
```

Legendre's Theorem.

Initially, we want to implement the Legendre's symbol. We define *LegendreSymbol* function with two parameters, *toCheck* and *modulo*. The function returns 0 if *toCheck* $\equiv 0 \pmod{modulo}$ and returns 1 if there exists an x such that $x^2 \equiv$ *toCheck* $\pmod{modulo}$, elsewise returns -1.

First, if *toCheck* $\equiv 0 \pmod{modulo}$, the function immediately returns 0. Next, if *toCheck* is negative, applying property 1 and 3 of the Legendre symbol, we can calculate $\left(\frac{-1}{p}\right)$ and save the result to a variable named *offset*. Otherwise, *offset* is set as 1. We, then, apply property 2 of the Legendre symbol to make *toCheck* less than *modulo*. Now, we make a loop that iterates from 1 to $modulo - 1$. If there exists a number i in that range such that $i^2 \equiv$ *toCheck* $\pmod{modulo}$, we return $1 \cdot$*offset*. Otherwise, after finishing the loop, we return $-1 \cdot$*offset*

Function. *LegendreSymbol()*
Pseudocode
Input. *toCheck*, the number to check if it is a quadratic residue
modulo, the modulo
Output. Returns 0 if $toCheck \equiv 0 \pmod{modulo}$ and returns 1 if *toCheck* is a quadratic residue modulo *modulo*, elsewise returns -1.

(1) if $toCheck \equiv 0 \pmod{modulo}$
(2) return 0
(3) if $toCheck < 0$
(4) $offset \leftarrow -1^{\frac{modulo-1}{2}}$
(5) else $offset \leftarrow 1$
(6) $toCheck \leftarrow |toCheck|$
(7) while $toCheck > modulo$
(8) $toCheck \leftarrow toCheck \bmod modulo$
(9) for $i \leftarrow 1$ to *modulo*
(10) if $i^2 \equiv toCheck \pmod{modulo}$
(11) return $1 \cdot offset$
(12) return $-1 \cdot offset$

C++ Implementation

```
int LegendreSymbol(int toCheck, int modulo){
    if(toCheck % modulo == 0) return 0;
    int offset = (toCheck < 0) ?  (int)(pow(-1, (modulo - 1) / 2)) : 1;
    toCheck = aflag(toCheck);
    while (toCheck > modulo){
        toCheck %= modulo;
    }

    for(int i = 1; i < modulo; ++i){
        if((i * i) % modulo == toCheck) return 1 * offset;
    }
    return -1 * offset;
}
```

Next, we only need to to write the Legendre theorem function. We will name it *LegendreCheck*.
Function. *LegendreCheck()*
Pseudocode
Output. return true if $-bc$ is a quadratic residue modulo $|a|$, $-ab$ is a quadratic residue modulo $|c|$ and $-ac$ is a quadratic residue modulo $|b|$. Otherwise, return false.

(1) bool *ans*
(2) temp $\leftarrow LegendreSymbol(-b * c, abs(a))$
(3) $ans \leftarrow temp = 0$ or $temp = 1$
(4) temp $\leftarrow LegendreSymbol(-a * b, abs(c))$
(5) $ans \leftarrow (temp = 0$ or $temp = 1)$ and *ans*
(6) temp $\leftarrow LegendreSymbol(-a * c, abs(b))$
(7) $ans \leftarrow temp = 0$ or $temp = 1$ and *ans*

(8) reuturn *ans*

C++ Implementation

```
bool LegendreCheck(){
    int temp = LegendreSymbol(-b * c, abs(a));
    bool ans = (temp == 0 || temp == 1);
    temp =  LegendreSymbol(-a * b, abs(c));
    ans &= (temp == 0 || temp == 1);
    temp = LegendreSymbol(-a * c, abs(b));
    return (ans & ((temp == 0 || temp == 1)));
}
```

Sample Program Run

We now add a few print functions to the code and try running two inputs in order to test our program.

Input 1

Input.

```
a = 1
b = 1
c = -3
```

Output.

```
Legendre Theorem Check
-bc is  a quadratic residue modulo |a|
-ab is not a quadratic residue modulo |c|
-ac is  a quadratic residue modulo |b|
There is no nontrivial integral solution to f(x, y, z) = 0

Hasse-Minkowski Theorem Check
There is no 3-focused solution
There is no nontrivial integral solution to f(x, y, z) = 0
```

Input 2

Input.

```
a = -7
b = 15
c = 13
```

Output.

```
Legendre Theorem Check
-bc is a quadratic residue modulo |a|
-ab is a quadratic residue modulo |c|
-ac is a quadratic residue modulo |b|
There are nontrivial integral solutions to f(x, y, z) = 0

Hasse-Minkowski Theorem Check
There is a 3-focused solution: x = 1, y = 0, z = 1
There is a 5-focused solution: x = 1, y = 0, z = 2
There is a 7-focused solution: x = 0, y = 1, z = 1
There is a 13-focused solution: x = 1, y = 6, z = 0
```

```
There are nontrivial integral solutions to f(x, y, z) = 0
```

We can see that in both cases the result is the same as the Legendre theorem and the Hasse-Minkowski theorem. We can also modify the program or add more functions depending on the task we intend to apply them to.

6. conclusion

We have proved two Hasse-Minkowski theorems which facilitate the problem of determining the integral solvability of quadratic forms. After the Hasse-Minkowski theorem, in the binary form, we could find a prime p which $f(x, y) \equiv 0 \pmod{p}$ does not have a solution (x, y) both not divisible by p to show that $f(x, y) = 0$ does not have nontrivial integral solutions. In the ternary form, the Hasse-Minkowski theorem reduces the problem to determining if there is a p-focused solution to the congruence $f(x, y, z) = 0 \pmod{p}$, which p is finite. The crux of this paper is the introduction of a complete program implementing the Hasse-Minkowski theorems and Legendre theorem with some supporting functions like the Eratosthenes sieve and the Legendre symbol.

Acknowledgments. I wish to record my deep sense of gratitude and profound thanks to Dr. Mehmet Dik for guiding me in every stage of this research paper. Without his support, guidance, and encouragement, it would have been difficult for me to complete this paper.

References

[1] S. D. Hoehner, *The Hasse-Minkowski Theorem in Two and Three Variables* (2012).
etd.ohiolink.edu/!etd.send_file?accession=osu1338317481
[2] G. A. Jones and J. M. Jones, *Elementary Number Theory* (Springer, 1998).
[3] W. J. LeVeque, *Fundamentals of Number Theory* (Dover Publications, 1977).

Phuc Ngo,
Beloit College, 700 College St., Beloit, WI 53511, U.S.A, (+1)248-759-0828, Orcid number:0000-0002-9658-4877
Email address: ngoph@beloit.edu

Mehmet Dik,
Beloit College, 700 College St., Beloit, WI 53511, U.S.A, (+1)815-986-9524, Orcid number:0000-0003-0643-2771
Email address: dikm@beloit.edu