REPRESENTATIONS OF ARITHMETIC PROGRESSIONS BY POSITIVE DEFINITE QUADRATIC FORMS

BYEONG-KWEON OH

Abstract. For a positive integer d and a non negative integer a, let $S_{d,a}$ be the set of all integers of the form $dn + a$ for any non negative integer n. A (positive definite integral) quadratic form f is said to be $S_{d,a}$-*universal* if it represents all integers in the set $S_{d,a}$, and is said to be $S_{d,a}$-*regular* if it represents all integers in the non empty set $S_{d,a} \cap Q(\mathrm{gen}(f))$, where $Q(\mathrm{gen}(f))$ is the set of all integers that are represented by the genus of f. In this article we prove that there is a polynomial $U(x, y) \in \mathbb{Q}[x, y]$ ($R(x, y) \in \mathbb{Q}[x, y]$) such that the discriminant df for any $S_{d,a}$-universal ($S_{d,a}$-regular) ternary quadratic forms is bounded by $U(d, a)$ ($R(d, a)$, respectively).

1. Introduction

A positive definite integral quadratic form f is called *regular* if it represents all integers that are represented by the genus of f. Regular quadratic forms were first studied systematically by Dickson in [5] where the term "regular" was coined. Jones and Pall in [8] classified all primitive positive definite diagonal regular ternary quadratic forms. In the last chapter of his doctoral thesis [18], Watson showed by arithmetic arguments that there are only finitely many equivalence classes of primitive positive definite regular ternary forms (see also [20]). More generally, a positive definite integral quadratic form f is called n-*regular* if f represents all quadratic forms of rank n that are represented by the genus of f. It was proved in [3] that there are only finitely many positive definite primitive n-regular forms of rank $n + 3$ for $n \geq 2$. See also [14] on the structure theorem of n-regular forms for higher rank cases.

The problem of enumerating the equivalence classes of the primitive positive definite regular ternary quadratic forms was recently resurrected by Kaplansky and his collaborators [9]. They provided a list of 913 candidates of primitive positive definite regular ternary forms and stated that there are no others. All but 22 of 913 are already verified to be regular. Recently the author verified in [15] that eight forms among 22 candidates are, in fact, regular.

For a positive integer d and a non-negative integer a, we define a set

$$S_{d,a} = \{dn + a \mid n \in \mathbb{Z}^+ \cup \{0\}\}.$$

A positive definite integral quadratic form f is said to be $S_{d,a}$-*universal* if it represents all integers in the set $S_{d,a}$, and f is said to be $S_{d,a}$-*regular* if it represents every integer in the set $S_{d,a}$ that is represented by the genus of f. Since there are infinitely many quadratic forms whose genera do not represent any integer in

2000 *Mathematics Subject Classification.* Primary 11E12, 11E20.

This work was supported by the Korea Research Foundation Grant (KRF-2008-314-C00004) funded by the Korean Government.

the set $S_{d,a}$, we additionally assume that for any $S_{d,a}$-regular form f, at least one integer in the set $S_{d,a}$ is represented by the genus of f.

Clearly, from the definition, every $S_{d,a}$-universal form is $S_{d,a}$-regular. Every regular form is $S_{d,a}$-regular if the genus of it represents at least one integer in the set $S_{d,a}$. The famous Fermat's four squares Theorem (for the proof see, for example, [13] p. 21) says that the unary form bx^2 for every positive integer b does not represent at least one integer in $\{a, d+a, 2d+a, 3d+a\}$ for any non zero d and a. Hence there is no $S_{d,a}$-universal unary form for any d and a. Recently Williams and his collaborators proved in [1] that there is no binary $S_{d,a}$-universal positive definite quadratic form for any d and a. As proved in that article, there are indefinite binary quadratic forms representing all integers in the set $S_{d,a}$, for any d and a.

Though there does not exist a universal ternary quadratic form, that is, a ternary form representing every positive integer, there are some examples of $S_{d,a}$-universal ternary quadratic forms. For example, Kaplansky proved in [10] that there are exactly 5 equivalence classes of $S_{2,1}$-universal ternary quadratic forms. They are, in fact,

$$x^2+y^2+2z^2,\ \ x^2+2y^2+3z^2,\ \ x^2+y^2+4z^2,\ \ x^2+3y^2+2yz+3z^2,\ \ x^2+3y^2+2yz+5z^2.$$

In this article we prove that there is a polynomial $U(x,y) \in \mathbb{Q}[x,y]$ such that the discriminant df for any $S_{d,a}$-universal ternary quadratic form f is bounded by $U(d,a)$. Hence there are only finitely many ternary $S_{d,a}$-universal quadratic forms up to equivalence.

For the regular case, we also prove that there is a polynomial $R(x,y) \in \mathbb{Q}[x,y]$ such that the discriminant df for any $S_{d,a}$-regular ternary quadratic form is bounded by $R(d,a)$.

The subsequent discussion will be conducted in the better adapted geometric language of quadratic spaces and lattices, and any unexplained notations and terminologies can be found in [11] or [16].

The term "lattice" will always refer to an integral $\mathbb{Z}$-lattice on an n-dimensional positive definite quadratic space over $\mathbb{Q}$. The scale and the norm ideal of a lattice L are denoted by $\mathfrak{s}(L)$ and $\mathfrak{n}(L)$ respectively. Let $L = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \cdots + \mathbb{Z}x_n$ be a $\mathbb{Z}$-lattice of rank n. We write

$$L \simeq (B(x_i, x_j)).$$

The right hand side matrix is called a *matrix presentation* of L, which we often identify with L itself. If L admits an orthogonal basis $\{x_1, \ldots, x_n\}$, we call L *diagonal* and simply write

$$L \cong \langle Q(x_1), \ldots, Q(x_n)\rangle.$$

The determinant of the matrix $(B(x_i, x_j))$ is called the discriminant of L, denoted $d(L)$.

Throughout this paper, we always assume that every $\mathbb{Z}$-lattice L is *positive definite* and is *primitive* in the sense that $\mathfrak{s}(L) = \mathbb{Z}$. In particular, a $\mathbb{Z}$-lattice L is called odd if $\mathfrak{n}(L) = \mathbb{Z}$, even otherwise. For any odd prime p, Δ_p is denoted by a non square unit in $\mathbb{Z}_p^\times$.

The successive minima of a $\mathbb{Z}$-lattice L of rank n are denoted by $\mu_1(L) \le \cdots \le \mu_n(L)$. It is well known that $dL \le \prod_{i=1}^n \mu_i(L)$ (see, for example, [6]). If an integer t is represented by a $\mathbb{Z}$-lattice L, then we write $t \to L$. If t is represented by the genus

of L, that is, if t is represented by $L \otimes \mathbb{Z}_p$ for any prime p, we write $t \to \mathrm{gen}(L)$. For any $\mathbb{Z}$-lattice L, we define sets

$$Q(L) = \{t \in \mathbb{Z} : t \to L\}$$

and

$$Q(\mathrm{gen}(L)) = \{t \in \mathbb{Z} : t \to L_p = L \otimes \mathbb{Z}_p \text{ for any prime } p\}.$$

2. $S_{d,a}$-Universal lattices

Recall that a $\mathbb{Z}$-lattice L is called $S_{d,a}$-*universal* if it represents every integer in the set $S_{d,a}$. Hence we have

$$L \text{ is } S_{d,a}\text{-universal if and only if } S_{d,a} \subset Q(L).$$

The following lemma shows that for any binary lattice L, the set $Q(L)$ always contains an arithmetic progression with an arbitrary finite length.

Lemma 2.1. *Let L be a binary $\mathbb{Z}$-lattice. For any positive integer k, there is an arithmetic progression of length k such that every integer in the arithmetic progression is represented by L.*

Proof. Note that there is an integer s such that $sL_i \to L$ for every $L_i \in \mathrm{gen}(L)$. Let $\{p_1, p_2, \ldots, p_t\}$ be the set of odd primes dividing dL. We also let $p_0 = 2$. For each $i = 1, 2, \ldots, t$, there is an integer a_{p_i} such that $\gcd(a_{p_i}, p_i) = 1$ and

$$L_{p_i} \simeq \langle a_{p_i}, p_i b_{p_i} \rangle,$$

and an integer a_0 such that $4 \nmid a_0$ and $a_0 \to L_2$. If L is odd, then we may assume that a_0 is odd.

Let a be a positive integer such that $a \equiv a_i \pmod{\gcd(2, p_i)^3 p_i}$ for every $i = 0, 1, \ldots, t$ and $d = 8\prod_{i=0}^{t} p_i$. If L is odd, then every prime $p \in S_{d,a}$ is represented by the genus of L by the reciprocity law for Hasse symbols. If L is even, every integer $2p \in S_{d,a}$ for a prime p is represented by the genus of L. For every integer k, there are integers b and c such that $S_{d,a}$ contains an arithmetic progression $T = \{c, b + c, 2b + c, \ldots, (k-1)b + c\}$ consisting of primes or even integers of the form $2p$, p a prime, by the celebrated result [7] of Green and Tao. Hence every integer in T is represented by the genus of L. Consequently every integer in the set $s^2 T = \{s^2 t : t \in T\}$ is represented by L. This completes the proof. □

Lemma 2.2. *Let d be a positive integer and a be a non-negative integer. There is a ternary $\mathbb{Z}$-lattice L such that $S_{d,a} \subset Q(gen(L))$ if and only if $d \nmid a$. In particular there does not exist an $S_{d,0}$-universal ternary $\mathbb{Z}$-lattice for any $d > 0$.*

Proof. First assume that a is divisible by d. Suppose that there exists a ternary $\mathbb{Z}$-lattice L such that $S_{d,a} \subset Q(\mathrm{gen}(L))$. Since the map $S_{d,a} - \{0\} \to \mathbb{Q}_p^\times \to \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ is surjective for every prime p, $V_p \simeq \langle -1, 1, -dV_p \rangle$, where $V_p = \mathbb{Q}_p \otimes L$. Hence the Hasse symbol $S_p V_p = (-1, -1)_p$ for every prime p. This contradicts the reciprocity law for Hasse symbols because V is positive definite.

Assume that $\gcd(d, a) = g$ does not equal to d. If there is a $\mathbb{Z}$-lattice L such that $S_{\frac{d}{g}, \frac{a}{g}} \subset Q(\mathrm{gen}(L))$, then $S_{d,a} \subset Q(\mathrm{gen}(L^g))$. Hence we may assume that $g = 1$. Furthermore since $S_{d,a} \subset S_{q,a}$ for any prime q dividing d, we may assume that $d = q$ is a prime without loss of generality. Since the ternary $\mathbb{Z}$-lattice $\langle 1, 1, 2 \rangle$ represents every integer in $S_{2,1}$, we may further assume that q is odd.

Let r be an odd prime such that $r \equiv a \pmod{p}$, and let s be a prime such that

$$s \equiv -q \pmod 4, \quad \left(\frac{s}{q}\right) = -\left(\frac{-r}{q}\right) \quad \text{and} \quad \left(\frac{s}{r}\right) = \left(\frac{-q}{r}\right).$$

Then one may easily show that for a diagonal $\mathbb{Z}$-lattice $L = \langle q, r, s\rangle$,

$$S_2(L) = S_q(L) = -S_r(L) = -1.$$

Hence $S_s(L) = 1$ by the reciprocity law for Hasse symbols. Therefore L_p represents all integers in $\mathbb{Z}_p$ except $p = q$ and $S_{q,a} \subset Q(L_q)$. This completes the proof. □

There are many examples of $S_{d,a}$-universal ternary $\mathbb{Z}$-lattices for some small integers d and a. In particular one may easily show, by using escalation method, that there does not exist an $S_{23,1}$-universal ternary $\mathbb{Z}$-lattices. For those examples see [2].

The following theorem shows that there are only finitely many equivalence classes of $S_{d,a}$-universal ternary $\mathbb{Z}$-lattices for any d and a.

Theorem 2.3. *Let L be a ternary $S_{d,a}$-universal $\mathbb{Z}$-lattice. Then we have*

$$dL \le U(d,a) = a(3d+a)(16d^2a(3d+a)+a).$$

Proof. Let $L = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \mathbb{Z}x_3$ and $\ell = \mathbb{Z}x_1 + \mathbb{Z}x_2$, where $Q(x_i) = \mu_i(L)$ for $i = 1, 2, 3$. Note that such a basis always exists (cf. [17]) and $d\ell \le a(3d+a)$ by Fermat's four squares Theorem. Assume that $d\ell = 2^g \prod_{i=1}^r p_i^{2e_i} \prod_{j=1}^s q_j^{2f_j-1}$ where p_i's and q_j's are odd primes and e_i's and f_j's are integers, and r or s is possibly a zero. Suppose that $s \ge 1$. Let t be an integer with $\left(\frac{t}{q_s}\right) = -1$ and $\tilde{d} = \dfrac{d}{q_s^{\mathrm{ord}_{q_s} d}}$. Then, by Chinese Remainder Theorem, there is an integer M such that

$$M \equiv 1 \quad \left(\bmod\ 8\tilde{d}\prod_{i=1}^{r} p_i \prod_{j=1}^{s-1} q_j\right), \quad M \equiv t \pmod{q_s} \ \text{ and } \ M < 8\tilde{d}d\ell.$$

From this we have

$$\left(\frac{-d\ell}{M}\right) = -1 \quad \text{and} \quad \gcd(M, 2dd\ell) = 1.$$

If $s = 0$, choose an integer M such that $M \equiv 7 \pmod 8$ and $\gcd(M, 2dd\ell) = 1$. Then, in any cases, there is a prime p dividing M such that

$$p < 8dd\ell, \quad \left(\frac{-d\ell}{p}\right) = -1 \quad \text{and} \quad \gcd(p, 2dd\ell) = 1. \tag{2.1}$$

Now take any positive integer k such that

$$\mathrm{ord}_p(kd+a) = 1 \quad \text{and} \quad k \le 2p.$$

Since the integer $kd+a$ is not represented by ℓ, $\mu_3(L) \le kd+a$. Therefore we have

$$dL \le \prod_{i=1}^{3} \mu_i(L) \le a(3d+a)(kd+a).$$

The theorem follows from this. □

3. $S_{d,a}$-REGULAR TERNARY LATTICES

Recall that a $\mathbb{Z}$-lattice L is called $S_{d,a}$*-regular* if it represents every integer in the set $S_{d,a} \cap Q(\mathrm{gen}(L))$, and at least one integer (therefore infinitely many) in the set $S_{d,a}$ is represented by the genus of L. Hence

$$L \text{ is } S_{d,a}\text{-regular if and only if } \varnothing \neq Q(\mathrm{gen}(L)) \cap S_{d,a} \subset Q(L).$$

There are many examples of $S_{d,a}$-regular ternary lattices for some d and a. For example the Ramanujan form $\langle 1, 1, 10\rangle$ is $S_{3,1}$- and $S_{10,5}$-regular though it is not regular. In this section we prove that there are only finitely many $S_{d,a}$-regular ternary $\mathbb{Z}$-lattices.

Lemma 3.1. *Let L be a ternary $\mathbb{Z}_2$-lattice such that $\mathfrak{s}(L) = \mathbb{Z}_2$ and $S_{d,a} \cap Q(L) \neq \varnothing$. Then there is a positive integer n_0 such that $S_{16d,dn_0+a} \subset Q(L)$.*

Proof. Assume that $\mathrm{ord}_2(\gcd(d, a)) = g$. Assume that $\frac{d}{2^g}$ is even. Let $dt + a \in S_{d,a} \cap Q(L)$ and let t_0 be the remainder of t divided by 8. Note that $\frac{dt+a}{2^g}$ is odd and

$$d(8n + t_0) + a = 2^g \left(8\frac{dn}{2^g} + \frac{dt_0 + a}{2^g}\right) = 2^g \left(8\left(\frac{dn}{2^g} + \frac{d(t_0 - t)}{2^{g+3}}\right) + \frac{dt + a}{2^g}\right)$$

Hence for any integer n, there is an $\epsilon_n \in \mathbb{Z}_2^\times$ such that

$$d(8n + t_0) + a = (dt + a)\epsilon_n^2 \in Q(L).$$

Therefore $S_{8d,dt_0+a} \subset Q(L)$ in this case.

Assume that $\frac{d}{2^g}$ is odd. First we consider the case when L is odd. Let $\tau \in \{0, 1\}$ be an integer having same parity to g. Note that there is an integer $s_0 \in \{1, 3, 5, 7\}$ such that $S_{8,s_0} \subset Q(L)$. Let $n_0 \leq 2^{\tau+3}$ be a non negative integer such that

$$\frac{dn_0 + a}{2^g} \equiv 2^\tau s_0 \pmod{2^{\tau+3}}.$$

Since

$$d(2^{\tau+3}n + n_0) + a = 2^{g+\tau}\left(s_0 + 8\left(\frac{dn}{2^g} + \frac{dn_0 + a - 2^{g+\tau}s_0}{2^{g+\tau+3}}\right)\right),$$

we have $S_{2^{\tau+3}d,dn_0+a} \subset Q(L)$.

Finally assume that L is even. Since $\mathfrak{s}(L) = \mathbb{Z}_2$ from the assumption, L has an even unimodular sublattice of rank 2. Therefore $S_{16,2s_0} \subset Q(L)$ for any $s_0 \in \{1, 3, 5, 7\}$. So the proof is quite similar to the above one. □

Lemma 3.2. *For an odd prime p, Let L be a ternary $\mathbb{Z}_p$-lattice such that $S_{d,a} \cap Q(L) \neq \varnothing$. Then there is a positive integer n_0 such that $S_{p^2d,dn_0+a} \subset Q(L)$.*

Proof. Since the proof is quite similar to the above, the proof is left to the readers. □

Corollary 3.3. *Let L be an $S_{d,a}$-regular ternary $\mathbb{Z}$ -lattice. Then there is a positive integer t ($t \leq 16d^2$) such that $S_{16d^3,dt+a} \subset Q(L_p)$ for every prime p dividing $2d$.*

Proof. This corollary is a direct consequence of Lemmas 3.1 and 3.2. □

From now on we always assume that d is divisible by 16 and for every $S_{d,a}$-regular ternary $\mathbb{Z}$-lattice L,

$$S_{d,a} \subset Q(L_p) \quad \text{for every prime } p \text{ dividing } d. \tag{3.1}$$

Let L be a $\mathbb{Z}$-lattice. For any positive odd integer m, the Watson transformation Λ_m is defined by

$$\Lambda_m(L) = \{x \in L : Q(x+z) \equiv Q(z) \pmod{m} \text{ for all } z \in L\}.$$

The $\mathbb{Z}$-lattice $\lambda_m(L)$ is denoted by the primitive lattice obtained from $\Lambda_m(L)$ by scaling $L \otimes \mathbb{Q}$ by a suitable rational number.

For any odd prime p, a ternary $\mathbb{Z}$-lattice L is called *p-stable* if

$$\langle 1, -1\rangle \to L_p \quad \text{or} \quad L_p \simeq \langle 1, -\Delta_p, p\epsilon_p\rangle,$$

where ϵ_p is a unit in $\mathbb{Z}_p$. It is well known that if L is regular and L_p is not p-stable then $\lambda_p(L)$ is also regular. For some properties of this transformation, see [4] or [19].

Lemma 3.4. *Let L be an $S_{d,a}$-regular ternary $\mathbb{Z}$-lattice and let p be a prime not dividing d such that L_p is not p-stable. Then $\lambda_p(L)$ is a S_{d,a_0}-regular lattice satisfying (3.1) for a suitable non-negative integer $a_0 \le \max(d,a)$.*

Proof. Let $L_p \simeq \langle \epsilon_1, \epsilon_2 p^{\alpha_2}, \epsilon_3 p^{\alpha_3}\rangle$ be a Jordan decomposition, where $\epsilon_i \in \mathbb{Z}_p^\times$ for $i = 1,2,3$, and $0 \le \alpha_2 \le \alpha_3$. We define $\tau = 1$ when $\alpha_2 = 1$, $\tau = 2$ otherwise. Then clearly $\mathfrak{s}(\Lambda_p(L)) = p^\tau \mathbb{Z}_p$. Let s be an integer such that

$$ds + a \equiv 0 \pmod{p^\tau} \quad \text{and} \quad 0 \le s \le p^\tau - 1.$$

Note that $a_0 = \frac{ds+a}{p^\tau} \le \max(d,a)$ and

$$S_{p^\tau d, p^\tau a_0} \subset S_{d,a} \subset Q(L_q) = Q(\Lambda_p(L)_q) \quad \text{for every prime } q \text{ dividing } d. \tag{3.2}$$

From this one may easily show that

$$S_{p^\tau d, p^\tau a_0} \cap Q(\mathrm{gen}(\Lambda_p(L))) \neq \varnothing.$$

Assume that $d_n = p^\tau dn + p^\tau a_0$ is represented by the genus of $\Lambda_p(L) \subset L$. Then $d_n = d(p^\tau n + s) + a$ is represented by L. Since L_p is not p-stable, d_n is also represented by $\Lambda_p(L)$. Therefore $\Lambda_p(L)$ is $S_{p^\tau d, p^\tau a_0}$-regular and hence $\lambda_p(L)$ is S_{d,a_0}-regular. The equation (3.2) shows that $\lambda_p(L)$ satisfies the condition (3.1). □

Lemma 3.5. *Let L be an $S_{d,a}$-regular ternary $\mathbb{Z}$-lattice and let $\{p_1, p_2, \dots, p_t\} \subset \{p : \ p \text{ is a prime such that } p \mid dL \text{ and } p \nmid d\}$. If L represents every element in $S_{d,a}$ that is not divisible by $P = \prod_{i=1}^t p_i$, then there is a polynomial $F(x,y) \in \mathbb{Q}[x,y]$ such that $dL \le F(d,a)$.*

Proof. We define $g = \gcd(d,a)$ and $d = gd_1,\ a = ga_1$. Let $p < d$ be a prime not dividing d and let $u < p$ be any positive integer such that $\left(\frac{u}{p}\right) = -1$. Note that such a prime p always exists, for d is divisible by 16 from the assumption. For these p and u, let $a_2 = ga_2'$ be a positive integer satisfying

$$a_1 \le a_2' \le a_1 + (p-1)d_1, \quad a_2' \equiv a_1 \pmod{d_1}, \quad \text{and} \quad a_2' \equiv u \pmod{p}.$$

Then for any $e \in S_{pd,a_2} \subset S_{d,a}$, e/g is not a square of an integer. Furthermore every integer in S_{pd,a_2} relatively prime to P is represented by L. We define $\widetilde{P}$ as follows: if p divides P, then we define $\widetilde{P} = \frac{P}{p}$, otherwise $\widetilde{P} = P$.

Now by Lemma 3 of [12], if we define $n_1 = (t+1)2^t$, which is greater than $\frac{p_1+t-1}{p_1-1}2^t$, then there is a non negative integer $k < n_1$ such that $pdk+a_2$ is relatively prime to P. Hence it is represented by L. Therefore we have

$$\mu_1(L) \le a_2 + (n_1-1)pd \le a + (d-1)d + ((t+1)2^t - 1)d^2.$$

Let $x \in L$ be a vector such that $Q(x) = pdk + a_2$.

Let q be any prime such that $\mathrm{ord}_q(pd_1k+a_2') \equiv 1 \pmod 2$. Since pd_1k+a_2' is not a square, such a prime q always exists. Furthermore if q divides pd_1, then q divides both d_1 and a_1. This is a contradiction. Now if $n_2 = (t+2)2^{t+1} \ge \frac{p_1+t}{p_1-1}2^{t+1}$, then there is an integer s $(k+1 \le s \le k+n_2)$ such that $pd_1s + a_2'$ is relatively prime to $\widetilde{P}q$. From the assumption on the prime q, we may easily check that the quadratic space spanned by x does not represent $pds + a_2$. Therefore we have

$$\mu_2(L) \le a_2 + (n_1+n_2-1)pd \le a + (d-1)d + ((3t+5)2^t - 1)d^2.$$

Let $\ell = \mathbb{Z}x_1 + \mathbb{Z}x_2$ be a primitive sublattice of L such that $Q(x_i) = \mu_i(L)$ for $i = 1, 2$. For this binary lattice ℓ, we may find a prime r such that

$$r < 8pdd\ell, \quad \gcd(r, pdd\ell) = 1, \quad \text{and} \quad \left(\frac{-d\ell}{r}\right) = -1$$

by applying a similar argument in the proof of Theorem 2.3.

We define integers m_r, ϵ_r and $\widetilde{P}_r$ as follows: If $r \nmid \widetilde{P}$, then $m_r = 1, \epsilon_r = 1$ and $\widetilde{P}_r = \widetilde{P}$. If $r \mid \widetilde{P}$, then we let m_r be the largest odd integer less than or equal to $\mathrm{ord}_r(dL) + 1$. In this case ϵ_r is any integer such that

$$r^{m_r}\epsilon_r \to L_r \quad \text{and} \quad \gcd(\epsilon_r, r) = 1,$$

and $\widetilde{P}_r = \frac{\widetilde{P}}{r}$. Now let a_3 be the positive integer such that

$$a_3 \equiv a_2 \pmod{pd} \quad a_3 \equiv r^{m_r}\epsilon_r \pmod{r^{m_r+1}}, \quad \text{and} \quad a_2 \le a_3 \le a_2 + pd(r^{m_r+1}-1).$$

Then $S_{pdr^{m_r+1},a_3} \subset S_{pd,a_2}$ and every integer in $S_{pdr^{m_r+1},a_3}$ relatively prime to $\widetilde{P_r}$ is represented by L. Furthermore $S_{pdr^{m_r+1},a_3} \cap Q(\mathrm{gen}(\ell)) = \varnothing$. Hence we have

$$\mu_3(L) \le pdr^{m_r+1}((t+1)2^t - 1) + a_3.$$

Therefore there is a polynomial $f(x_1, x_2, x_3, x_4) \in \mathbb{Q}[x_1, \ldots, x_4]$ such that

$$P = \prod_{i=1}^{t} p_i \le \frac{dL}{r^{m_r-2}} \le \frac{\prod_{i=1}^{3}\mu_i(L)}{r^{m_r-2}} \le f(2^t, t, d, a).$$

As a consequence of this inequality, t is bounded and hence P as well as dL are also bounded. □

Theorem 3.6. *There is a polynomial $G(x, y) \in \mathbb{Q}[x, y]$ such that*

$$\prod_{p \in \{p : L_p \text{ is anisotropic}\}} p \le G(d, a),$$

for any $S_{d,a}$-regular ternary $\mathbb{Z}$-lattice L.

Proof. Let $\{p_1 < p_2 < \cdots < p_t\}$ be the set of all anisotropic primes of L not dividing d and $P = \prod_{i=1}^{t} p_i$. Then it suffices to show that there is a polynomial in $\mathbb{Q}[d, a]$ that is independent of L and is greater than P.

For any prime $p \nmid d$ such that L_p is not stable, we apply the Lemma 3.4 repeatedly so that we obtain a new lattice, denoted by $\lambda(L)$, satisfying the following properties:

(i) $\lambda(L)$ is S_{d,a_0}-regular for some $a_0 \le \max(d,a)$;
(ii) $\lambda(L)$ satisfies the condition (3.1);
(iii) $\lambda(L)_p$ is p-stable for every prime $p \nmid d$.

Let p be a prime not dividing d. If $\lambda(L)_p$ is isotropic, then L_p represents every element in $\mathbb{Z}_p$ and if $\lambda(L)_p$ is anisotropic then L_p represents every element in $\mathbb{Z}_p^\times$. Hence $\lambda(L)$, S_{d,a_0} and P satisfies all conditions in Lemma 3.5. Therefore the theorem follows from the fact that L_p is anisotropic if and only if $\lambda(L)_p$ is anisotropic for any prime p. □

Corollary 3.7. *Let L be any $S_{d,a}$-regular ternary $\mathbb{Z}$-lattice. Then there is a polynomial $T(x,y) \in \mathbb{Q}[x,y]$ satisfying the following properties: there are integers $d_0, a_0 \le T(d,a)$ such that*

(a) *L is S_{d_0,a_0}-regular;*
(b) *Every anisotropic prime of L divides d_0, and in particular $16 \mid d_0$.*
(c) *For every prime $p \mid d_0$, $S_{d_0,a_0} \subset Q(L_p)$*

Proof. Let p be an anisotropic prime of L not dividing d. Then there is an integer $a_p \le d(p-1)+a$ such that $S_{dp,a_p} \subset S_{d,a} \cap Q(L_p)$. Note that $S_{dp,a_p} \cap Q(L_q) \ne \varnothing$ for any prime $q \nmid dp$. Hence the corollary follows directly from Theorem 3.6. □

Theorem 3.8. *There is a polynomial $H(x,y) \in \mathbb{Q}[x,y]$ such that*

$$\prod_{p \in \{p : p \text{ is a prime such that } p \mid dL\}} p \le H(d,a)$$

for any $S_{d,a}$-regular ternary $\mathbb{Z}$-lattice.

Proof. Let d_0, a_0 be integers satisfying all conditions given in Corollary 3.7. Define

$$\Phi = \{p : p \mid dL \text{ is a prime not dividing } d_0\}.$$

We also define

$$\prod_{p \in \{p_1,\dots,p_t\}} \lambda_p(L) = \lambda_{p_1} \circ \cdots \circ \lambda_{p_t}(L).$$

Note that L_p is isotropic for any prime $p \in \Phi$. For each $p \in \Phi$ we define a non negative integer s_p as follows: if L_p is p-stable then $s_p = 0$, otherwise s_p is a positive integer such that $\lambda_p^s(L)_p$ is not p-stable for any $0 \le s \le s_p - 1$ and $\lambda_p^{s_p}(L)_p$ is p-stable. Let Φ_1 be the subset of Φ consisting of all primes p such that L_p is p-stable or $\det(\lambda_p^{s_p}(L))$ is divisible by p. Let $\Phi_2 \subset \Phi - \Phi_1$ be the subset of all primes p such that $\lambda_p^{s_p-1}(L) \simeq \langle 1, -\Delta_p, p^2\epsilon\rangle$ for $\epsilon \in \mathbb{Z}_p^\times$. Finally we define $\Phi_3 = \Phi - (\Phi_1 \cup \Phi_2)$. Note that for any prime $p \in \Phi_3$,

$$\lambda_p^{s_p-1}(L)_p \simeq \langle \epsilon_{p,1}, p^2\epsilon_{p,2}, p^2\epsilon_{p,3}\rangle,$$

where $\epsilon_{p,i} \in \mathbb{Z}_p^\times$ for $i = 1,2,3$.

Now there is an integer $a_1 \le \max(d_0,a_0)$ such that

$$M = \prod_{p \in \Phi_1 \cup \Phi_3} \lambda_p^{s_p} \circ \prod_{p \in \Phi_2} \lambda_p^{s_p-1}(L)$$

is S_{d_0,a_1}-regular. Note that M represents every integer $e \in S_{d_0,a_1}$ that is not divisible by $\prod_{p\in\Phi_2} p$. Therefore by Lemma 3.5,

$$\prod_{p \in \Phi_1} p \times \prod_{p \in \Phi_2} p^2 \le dM \le F(d_0,a_1). \tag{3.3}$$

Finally there is also an integer $a_1' \le \max(d_0, a_0)$ such that

$$N = \prod_{p\in\Phi_1\cup\Phi_2} \lambda_p^{s_p} \circ \prod_{p\in\Phi_3} \lambda_p^{s_p-1}(L)$$

is $S_{d_0,a_1'}$-regular. In this case N represents every integer $e \in S_{d_0,a_1'}$ such that $e\epsilon_{p,1} \in (\mathbb{Z}_p^\times)^2$ for any $p \in \Phi_3$. Define $P = \prod_{p\in\Phi_3} p$. For any $\epsilon > 0$, there is a constant $C = C(\epsilon)$ satisfying the following property: there is a positive integer $m < CP^{\frac{3}{8}+\epsilon}$ such that$(d_0m + a_1')\epsilon_{p,1} \in (\mathbb{Z}_p^\times)^2$ for any $p \in \Phi_3$ (see Corollary 3.3 of [6]). From this and the fact that for any binary sublattice ℓ of N, $d(\ell)$ is divisible by P^2, we have

$$P^2 \le (d_0(CP^{\frac{3}{8}+\epsilon}) + a_1')(d_0(3P + CP^{\frac{3}{8}+\epsilon}) + a_1'). \tag{3.4}$$

The theorem follows from (3.3) and (3.4). □

Theorem 3.9. *There is a polynomial $R(x, y) \in \mathbb{Q}[x, y]$ such that*

$$d(L) \le R(d, a)$$

for any $S_{d,a}$-regular ternary $\mathbb{Z}$-lattice L. Therefore there are only finitely many $S_{d,a}$-regular ternary $\mathbb{Z}$-lattices up to equivalences.

Proof. Let L be an $S_{d,a}$-regular $\mathbb{Z}$-lattice. Fix a polynomial $T(x, y)$ and integers $d_0, a_0 < T(d, a)$ in Corollary 3.7, and $H(x, y)$ in Theorem 3.8. Let $p_1 < p_2 < \cdots < p_t$ be all prime divisors of dL that are relatively prime to d, and let $P = \prod_{i=1}^t p_i$ which is less than or equal to $H(d, a)$. There is an integer $a_1 < d_0P + a_0$ such that L is S_{d_0P,a_1}-universal. Therefore, by Theorem 2.3,

$$dL \le U(d_0P, a_1) \le U(T(d, a)H(d, a), T(d, a)(H(d, a) + 1)).$$

This completes the proof. □

Corollary 3.10. *There is a polynomial $f(x) \in \mathbb{Q}[x]$ satisfying the following property: for any ternary $\mathbb{Z}$-lattice L whose discriminant is bigger than $f(k)$, the set $Q(gen(L)) - Q(L)$ contains an integer not less than k.*

Proof. Define $f(x) = R(1, x)$. Since $S_{1,k} \cap Q(\mathrm{gen}(L)) \ne \varnothing$ for any ternary $\mathbb{Z}$-lattice L, the corollary follows directly from Theorem 3.9. □

Remark 3.11. If we use the method in [15], we may find various examples of $S_{d,a}$-regular ternary lattices. For example, both diagonal ternary $\mathbb{Z}$-lattices $\langle 1, 2, 12\rangle$ and $\langle 2, 3, 4\rangle$, which are in the same genus, are $S_{3,0}$-regular. Note that these two lattices are not regular.

References

[1] A. Alaca, Ş. Alaca and K. S. Williams, *Arithmetic progressions and binary quadratic forms*, Amer. Math. Monthly **115**(2008), 252–254.

[2] Y.-S. Chi, M.-H. Kim and B.-K. Oh, *Ternary quadratic forms representing all integers in some arithmetic progressions*, in preparation.

[3] W. K. Chan and B.-K, Oh, *Finiteness theorems for positive definite n-regular quadratic forms*, Trans. Amer. Math. Soc. **355**(2003), 2385–2396.

[4] W. K. Chan and B.-K. Oh, *Positive ternary quadratic forms with finitely many exceptions*, Proc. Amer. Math. Soc. **132**(2004), 1567–1573.

[5] L. E. Dickson, *History of the theory of numbers*, Vol 1; Divisibility and primality.

[6] A. G. Earnest. *The representation of binary quadratic forms by positive definite quaternary quadratic forms*, Trans. Amer. Math. Soc. **345**(1994), 853-863.

[7] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progression*, preprint.
[8] B. W. Jones and G. Pall, *Regular and semi-regular positive ternary quadratic forms*, Acta Math. **70** (1940), 165–190.
[9] W. C. Jagy, I. Kaplansky and A. Schiemann, *There are 913 regular ternary forms*, Mathematika **44**(1997), 332–341.
[10] I. Kaplansky, *Ternary positive forms that represent all odd positive integers*, Acta Arith. **120**(1995), 209–214.
[11] Y. Kitaoka, *Arithmetic of quadratic forms*, Cambridge University Press, 1993.
[12] B. M. Kim, M.-H. Kim and B.-K. Oh, 2-*universal positive definite integral quinary quadratic forms*. Integral quadratic forms and lattices (Seoul, 1998), 51–62, Contemp. Math., 249, Amer. Math. Soc., Providence, RI, 1999.
[13] L. J. Mordell, *Diophantine equations*, Academic Press 1969.
[14] B.-K. Oh, *Positive definite n-regular quadratic forms*, Invent. Math. **170**(2007), 421–453.
[15] B.-K. Oh, *regular positive ternary quadratic forms*, to appear in Acta Arith..
[16] O. T. O'Meara, *Introduction to quadratic forms*, Springer Verlag, New York, 1963.
[17] B. van der Waerden, *Die Reduktion der Positiven Quadratischen Formen*, Acta Math. **96**(1956), 265–309.
[18] G. L. Watson, *Some problems in the theory of numbers*, Ph.D. Thesis, University of London, 1953.
[19] G. L. Watson, *Transformations of a quadratic form which do not increase the class-number*, Proc. London Math. Soc. (3) **12**(1962), 577-587.
[20] G. L. Watson, *Regular positive ternary quadratic forms*, J. London Math. Soc. **13**(1976), 97-102.

Department of Mathematical Sciences, Seoul National University, Seoul 151-747, Korea

E-mail address: bkoh@snu.ac.kr