ACTA ARITHMETICA
181.2 (2017)

Positive binary forms representing the same integers in an arithmetic progression

by

Myung-Hwan Kim and Byeong-Kweon Oh (Seoul)

1. Introduction. For a positive definite binary form $f(x,y) = ax^2 + bxy + cy^2$, we say that f *represents an integer* n if the diophantine equation $f(x,y) = n$ has an integer solution. The general theory of quadratic forms, including composition of binary quadratic forms, was advanced by Gauss in his great book 'Disquisitiones Arithmeticae'. The problem of determining $Q(f)$, the set of all integers that are represented by a binary form f, has a long and rich history since Fermat's theorem on the representation by a sum of two squares. There is an effective algorithm to determine the set $Q(x^2 + ny^2) \cap P$, where n is a positive integer and P is the set of primes (for details, see [1]). However, determining the set $Q(f)$ itself for a general positive definite binary form f is still an open problem except for some particular cases, including the case when the class number $h(f)$ of f is one.

In 1938, Delone [2] proved that for two (positive definite primitive integral) binary forms f and g, $Q(f) = Q(g)$ if and only if f is equivalent to g or, as an exceptional case, the pair (f,g) is equivalent to (x^2+xy+y^2, x^2+3y^2). This result implies that the set of integers that are represented by a positive definite binary quadratic form decides the form itself except for a single case. This result was generalized to the indefinite case by Li [7]. Related to this result, Jagy and Kaplansky [4] considered the set of primes, instead of the set of integers, that are represented by a binary form. They exhibited a table of 68 pairs (f,g) of non-equivalent binary forms satisfying $Q(f) \cap P = Q(g) \cap P$, and conjectured that their list is complete except for some family of trivial pairs. This conjecture was proved by Voight [11]. In fact, he classified all pairs (f,g) of primitive binary forms having different

2010 *Mathematics Subject Classification*: Primary 11E16; Secondary 11E12.
Key words and phrases: binary forms, arithmetic progressions.
Received 12 February 2016; revised 19 June 2017.
Published online 27 October 2017.

DOI: 10.4064/aa8443-6-2017

fundamental discriminant such that

$$|Q(f) \cap P - Q(g) \cap P| < \infty.$$

In this article, we consider the arithmetic progression

$$A_{p,k} := \{pn + k : n \geq 0\},$$

where p is a prime and k is any integer. We give effective criteria for finding all non-equivalent binary forms f and g satisfying

$$Q(f) \cap A_{p,k} = Q(g) \cap A_{p,k} \neq \emptyset,$$

or

$$r(m, f) = r(m, g) \quad \text{for any } m \in A_{p,k},$$

where $r(m, f)$ is the number of representations of an integer m by f.

In fact, the proof for $\gcd(k, p) = 1$ is a little different from one for the case when k is divisible by p. So, in Section 2, we consider the case when $\gcd(k, p) = 1$. The case of $p \mid k$ will be considered in Section 3. In this case, the composition law of binary forms plays an important role.

For a binary form $f(x, y) = ax^2 + bxy + cy^2$, we simply write $f = [a, b, c]$. For two binary forms f and g, we say f is *equivalent* (resp. *proper equivalent*) to g if there are integers r, s, t and u such that

$$ru - st = \pm 1 \quad (\text{resp. } ru - st = 1) \quad \text{and} \quad f(rx + sy, tx + uy) = g(x, y),$$

and we then write $f \sim g$ (resp. $f \simeq g$).

Let $L = \mathbb{Z}e_1 + \mathbb{Z}e_2$ be a binary $\mathbb{Z}$-lattice. Throughout this paper, the discriminant D_L of L is defined by $D_L = 4(B(e_1, e_2)^2 - Q(e_1)Q(e_2)) = -4dL$, where dL is the discriminant defined in [5] and [9]. The binary quadratic form corresponding to L for the ordered basis $\mathfrak{B} = \{e_1, e_2\}$ is defined by

$$f_{\mathfrak{B}}(x, y) = [Q(e_1), 2B(e_1, e_2), Q(e_2)] = Q(e_1)x^2 + 2B(e_1, e_2)xy + Q(e_2)y^2.$$

Note that the binary form corresponding to L is independent of the choice of basis for L up to equivalence. However, up to proper equivalence, it does depend on the choice of basis. When we consider some properties depending only on the equivalence class, we will use the notation f_L rather than $f_{\mathfrak{B}}$. For binary lattices L and M, we say L is *isometric* to M ($L \simeq M$) if $f_L \sim f_M$. We will use the notation $[a, b, c]$ for the presentation of the lattice L defined over $\mathbb{Z}$ or the p-adic integer ring $\mathbb{Z}_p$ such that $f_L \sim [a, b, c]$.

For pairs (L, M), (L', M') of binary lattices, we say (L, M) is isometric to (L', M') if $L \simeq L'$ and $M \simeq M'$, or $L \simeq M'$ and $M \simeq L'$. In this case, we write $(L, M) \simeq (L', M')$. For pairs (f, g), (f', g') of binary forms, $(f, g) \sim (f', g')$ and $(f, g) \simeq (f', g')$ are defined similarly.

Throughout this article, we always assume that any binary form $f(x, y) = ax^2 + bxy + cy^2$ is *primitive* and *positive definite*, that is, respectively, a, b and c are relatively prime integers and $ax^2 + bxy + cy^2 > 0$ for any

$(x,y) \in \mathbb{Z}^2 - \{(0,0)\}$. For a binary lattice L, we always assume that the corresponding binary form f_L satisfies the above assumptions. Hence $\mathfrak{n}(L) = \mathbb{Z}$. The isotropic (anisotropic) binary $\frac{1}{2}\mathbb{Z}_p$ modular lattice is denoted by $\mathbb{H}_p$ ($\mathbb{A}_p$, respectively).

For any positive integer n, we define

$$R(n,L) := \{(x,y) \in \mathbb{Z}^2 : Q(x,y) = n\} \quad \text{and} \quad r(n,L) := |R(n,L)|.$$

Note that $r(n,L)$ is always finite. Finally, we define $Q(L) = \{n : r(n,L) \neq 0\}$. For a binary form f, we will also use the notations $r(n,f)$ and $Q(f)$ defined quite similarly to the above. The isometry group of a lattice L (resp. a form f) is denoted by $O(L)$ (resp. $O(f)$). Note that the order $o(L) := |O(L)|$ is $2, 4, 8$ or 12. For the proper isometry group, we will use the notation $O^+(\cdot)$. Note that every isometry in $O(L)$ of order 2 is a symmetry or $-I$.

Any unexplained notation and terminology on quadratic forms and lattices can be found in [5] or [9], and especially for binary forms, see [1] or [6].

2. Representations of integers in an arithmetic progression. In this section, we study the representation of integers in an arithmetic progression with a fixed prime difference and non-zero initial term. For the time being, let p be an odd prime and k be a positive integer less than p. Let $L = \mathbb{Z}x + \mathbb{Z}y$ be a positive definite binary lattice such that $\mathfrak{n}(L) = \mathbb{Z}$. The set of binary sublattices of L with index p is denoted by $\Gamma_p(L)$. Note that $|\Gamma_p(L)| = p+1$, and in fact every lattice in $\Gamma_p(L)$ is of the form

$$L(-1) := \mathbb{Z}(px) + \mathbb{Z}y \quad \text{or} \quad L(u) := \mathbb{Z}(x+uy) + \mathbb{Z}(py),$$

where $0 \le u \le p-1$. First assume that L_p is isotropic unimodular. Then each lattice in $\Gamma_p(L)$ is isometric to

$$\langle 1, -p^2\rangle, \quad \langle \Delta_p, -\Delta_p p^2\rangle \quad \text{or} \quad \langle p, -p\rangle$$

over $\mathbb{Z}_p$, where Δ_p is a non-square unit in $\mathbb{Z}_p^\times$. Furthermore one can easily show that the number of such lattices is $(p-1)/2, (p-1)/2$ and 2, respectively. If L_p is anisotropic unimodular, then the norm of each lattice in $\Gamma_p(L)$ is $\mathbb{Z}$, and the number of lattices isometric to $\langle 1, -\Delta_p p^2\rangle$ over $\mathbb{Z}_p$ is $(p+1)/2$. All the other lattices are isometric to $\langle \Delta_p, -p^2\rangle$ over $\mathbb{Z}_p$. Finally, if p divides the discriminant of L, then there is a unique lattice in $\Gamma_p(L)$ whose norm is contained in $p\mathbb{Z}$. We define two subsets $\Gamma_{p,\pm1}(L)$ of $\Gamma_p(L)$ by

$$\Gamma_{p,\pm1}(L) := \left\{ K \in \Gamma_p(L) : K \text{ represents an integer } a \text{ such that } \left(\frac{a}{p}\right) = \pm 1 \right\}.$$

The number of equivalence classes in each set is denoted by $\gamma_{p,\pm1}(L)$.

LEMMA 2.1. *Let $\epsilon = 1$ or -1. For the action $\Phi : O(L) \times \Gamma_{p,\epsilon}(L) \to \Gamma_{p,\epsilon}(L)$ defined by $\Phi(\sigma, M) = \sigma(M)$, each orbit $orb(M)$ of a lattice $M \in \Gamma_{p,\epsilon}(L)$ consists of all lattices isometric to M. Furthermore $|orb(M)| = o(L)/o(M)$.*

Proof. It suffices to show that if there is an isometry $\sigma : L(i) \to L(j)$ for $L(i), L(j) \in \Gamma_{p,\epsilon}(L)$ where $-1 \le i, j \le p-1$, then $\sigma \in O(L)$. Assume that $i, j \neq -1$ and $\sigma(py) = \alpha(x+jy) + \beta(py)$ for $\alpha, \beta \in \mathbb{Z}$. Since

$$\alpha^2 Q(x+jy) + 2p\alpha\beta B(x+jy, y) + p^2\beta^2 Q(y) = \alpha^2 Q(x+jy) \equiv 0 \pmod{p}$$

and $Q(x+jy) \not\equiv 0 \pmod{p}$, α is divisible by p. Therefore $\sigma(L) = L$. The proofs of all the other cases are quite similar. ∎

Note that $o(L) = 12$ (resp. $o(L) = 8$) if and only if $L \simeq [1,1,1]$ (resp. $L \simeq [1,0,1]$). For all the other binary lattices, $o(L) = 2$ or 4. If $o(L) = 2$, then the isometry group of each lattice in $\Gamma_{p,\pm 1}(L)$ is of order 2 and $\gamma_{p,\pm 1}(L) = |\Gamma_{p,\pm 1}(L)|$.

Assume that an odd prime p divides the discriminant D_K of a binary lattice K. If K_p represents a unit square in $\mathbb{Z}_p^\times$, then we define $u_p(K) := 1$, otherwise $u_p(K) := -1$.

LEMMA 2.2. *Assume that $o(L) = 4$ and $\tau_x \in O(L)$ for a primitive vector $x \in L$. If $\left(\frac{-D_L}{p}\right) = 1$, then*

$$\gamma_{p,\left(\frac{Q(x)}{p}\right)}(L) = \mathbf{2} + \frac{p - 4 - \left(\frac{-1}{p}\right)}{4} \quad \text{and} \quad \gamma_{p,-\left(\frac{Q(x)}{p}\right)}(L) = \mathbf{0} + \frac{p - \left(\frac{-1}{p}\right)}{4},$$

and if $\left(\frac{-D_L}{p}\right) = -1$, then

$$\gamma_{p,1}(L) = \gamma_{p,-1}(L) = \mathbf{1} + \frac{p - 2 + \left(\frac{-1}{p}\right)}{4}.$$

Finally, if p divides the discriminant of L, then

$$\gamma_{p,u_p(L)}(L) = \mathbf{1} + \frac{p-1}{2} \quad \text{and} \quad \gamma_{p,-u_p(L)}(L) = \mathbf{0}.$$

In the formula, the boldface number is the number of equivalence classes whose isometry group is of order 4.

Proof. Since $o(L) = 4$, there are integers a, b such that

$$(B(x_i, x_j)) = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \quad \text{or} \quad (B(x_i, x_j)) = \begin{pmatrix} a & b/2 \\ b/2 & a \end{pmatrix},$$

where $\{x_1, x_2\}$ is a basis of L. By Lemma 2.1, it is enough to compute the number of lattices in $\Gamma_p(L)$ fixed by the symmetry $\tau_x \in O(L)$. Here we may take $x = x_1$ for the former case and $x = x_1 - x_2$ for the latter. Let $L(-1) = \mathbb{Z}(px_1) + \mathbb{Z}x_2$ and $L(i) = \mathbb{Z}(x_1 + ix_2) + \mathbb{Z}(px_2)$ for $0 \le i \le p-1$. Suppose that $\tau_x(L(j)) = L(j)$. Then clearly $j = -1, 0$ for the former case. For the latter case, note that $\tau_x(L(-1)) = L(0)$ and $\tau_x(L(j)) = \mathbb{Z}(x_2 + jx_1) + \mathbb{Z}(px_1)$ for $j \ge 1$. Take integers s, t such that $sj - pt = 1$. Then

$$\tau_x(L(j)) = \mathbb{Z}(s(x_2 + jx_1) - t(px_1)) + \mathbb{Z}(-p(x_2 + jx_1) + j(px_1)) = L(s).$$

Therefore only $L(1)$ and $L(p-1)$ are fixed by τ_x. The lemma follows directly from this. ∎

COROLLARY 2.3. *If* $L=[1,0,1]$, *then*

$$\gamma_{p,1}(L)=\frac{\mathbf{3}+\left(\frac{\mathbf{2}}{\boldsymbol{p}}\right)}{\mathbf{2}}+\frac{p-2\left(\frac{2}{p}\right)-\left(\frac{-1}{p}\right)-6}{8},$$
$$\gamma_{p,-1}(L)=\frac{\mathbf{1}-\left(\frac{\mathbf{2}}{\boldsymbol{p}}\right)}{\mathbf{2}}+\frac{p+2\left(\frac{2}{p}\right)-\left(\frac{-1}{p}\right)-2}{8}.$$

If $L=[1,1,1]$ *and* $p\neq 3$ *then*

$$\gamma_{p,1}(L)=\frac{\mathbf{3}+\left(\frac{\mathbf{3}}{\boldsymbol{p}}\right)}{\mathbf{2}}+\frac{p-3\left(\frac{3}{p}\right)-\left(\frac{p}{3}\right)-9}{12}$$

and

$$\gamma_{p,-1}(L)=\frac{\mathbf{1}-\left(\frac{\mathbf{3}}{\boldsymbol{p}}\right)}{\mathbf{2}}+\frac{p+3\left(\frac{3}{p}\right)-\left(\frac{p}{3}\right)-3}{12}.$$

Finally, if $L=[1,1,1]$ *and* $p=3$, *then* $\gamma_{p,1}(L)=1$ *and* $\gamma_{p,-1}(L)=0$.

Proof. One can easily show that if $L=[1,0,1]$ (resp. $L=[1,1,1]$ and $p\neq 3$), then up to equivalence, $[1,0,p^2]$ and $[2,2,(1+p^2)/2]$ (resp. $[1,1,(3p^2+1)/4]$ and $[3,3,(p^2+3)/4]$) are the only binary lattices in $\Gamma_{p,1}(L)\cup\Gamma_{p,-1}(L)$ whose isometry group is of order 4. The formula follows directly from this. ∎

LEMMA 2.4. *Let* p *be an odd prime and let* k *be any integer relatively prime to* p. *For any binary* $\mathbb{Z}$*-lattice* L,

$$r(pn+k,L)=\sum_{K\in\Gamma_{p,(\frac{k}{p})}(L)/\sim}\frac{o(L)}{o(K)}r(pn+k,K).$$

Proof. Note that for any distinct $K_1,K_2\in\Gamma_p(L)$, we have $K_1\cap K_2=pL$. Hence, for any vector $x\in L$ such that $Q(x)=pn+k$, x is contained in exactly one lattice in $\Gamma_{p,(\frac{k}{p})}(L)$. The lemma follows from this and the fact that the number of lattices isometric to K for any $K\in\Gamma_{p,(k/p)}(L)$ is $o(L)/o(K)$. ∎

When $p=2$, one can have similar results. In this case, the following lemma will be enough for our purpose.

LEMMA 2.5. *Let* ℓ *be a binary* $\mathbb{Z}$*-lattice such that* $\ell_2\simeq[1,1,1]$. *Define* $t(\ell)=1$ *if* $|O(\ell)|=12$, $t(\ell)=2$ *if* $|O(\ell)|=4$, *and* $t(\ell)=3$ *if* $|O(\ell)|=2$. *Then there are exactly* $t(\ell)$ *non-isometric sublattices of* ℓ *with index* 2. *Furthermore, if* $t(\ell)=2$, *then the isometry groups of two non-isometric sublattices of* ℓ *with index* 2 *are of order* 2 *and* 4, *respectively, and if* $t(\ell)=3$, *then every sublattice with index* 2 *has a trivial isometry group.*

Proof. Let $\mathfrak{B} = \{e_1, e_2\}$ be an ordered basis of ℓ. Then all binary sublattices of ℓ with index 2 are

$$S_1(\mathfrak{B}) := \mathbb{Z}(2e_1) + \mathbb{Z}e_2, \quad S_2(\mathfrak{B}) := \mathbb{Z}e_1 + \mathbb{Z}(2e_2),$$
$$S_3(\mathfrak{B}) := \mathbb{Z}(e_1 + e_2) + \mathbb{Z}(2e_2).$$

If $|O(\ell)| = 12$, then $f_\ell \simeq [1,1,1]$. One can easily show that all three sublattices are isometric to each other. Assume that $|O(\ell)| = 4$. Then there is a basis $\mathfrak{B}' = \{e_1', e_2'\}$ of ℓ such that $f_{\mathfrak{B}'} \sim [a,b,a]$, where ab ($a \neq b$) is an odd integer. Hence $S_1(\mathfrak{B}') \simeq S_2(\mathfrak{B}')$.

Suppose that there is an isometry $\sigma : S_3(\mathfrak{B}') \to S_1(\mathfrak{B}')$ such that $\sigma(2e_2') = \alpha(2e_1') + \beta e_2'$, where $\alpha, \beta \in \mathbb{Z}$. Then

$$Q(\sigma(2e_2')) = 4a\alpha^2 + 2\alpha\beta b + a\beta^2 \equiv 0 \pmod 4.$$

Hence β is even and $\sigma(\ell) = \ell$. Therefore

$$(\sigma(e_1'), \sigma(e_2')) = \pm(e_1', e_2') \quad \text{or} \quad (\sigma(e_1'), \sigma(e_2')) = \pm(e_2', e_1'),$$

which is a contradiction.

Note that $(f_{S_1(\mathfrak{B}')}, f_{S_3(\mathfrak{B}')}) \sim ([4a, 2b, a], [2a - b, 0, 2a + b])$. Clearly, $|O([4a,2b,a])| = 2$ and $|O([2a+b,0,2a-b])| = 4$. When $|O(\ell)| = 2$, one can easily show that any isometry between $S_i(\mathfrak{B})$'s for $i = 1,2,3$, if exists, induces an isometry of ℓ. Everything follows from this observation. ∎

In 1840, Dirichlet conjectured that for any (primitive) binary lattice L such that $Q(L) \cap A_{m,k} \neq \emptyset$, L represents infinitely many primes in $A_{m,k}$, where m, k ($m > 0$) are relatively prime integers and $A_{m,k}$ is an arithmetic progression with common difference m and initial term k. Weber [12] proved a special case of this conjecture and Meyer [8] finally proved the conjecture. Meyer's theorem will be frequently used in the proofs of our results.

THEOREM 2.6. *Let p be an odd prime and let k be any integer relatively prime to p. Let L and M be primitive binary $\mathbb{Z}$-lattices such that $D_M \leq D_L$, $L \not\simeq M$ and $(L, M) \not\simeq ([1,1,1],[1,0,3])$. The lattices L and M satisfy*

$$Q(L) \cap A_{p,k} = Q(M) \cap A_{p,k} \neq \emptyset \tag{2.1}$$

if and only if either

$$L_2 \simeq M_2 \text{ and every lattice in } \Gamma_{p,(\frac{k}{p})}(L) \text{ is isometric to } M, \tag{2.2}$$

or $L = [1,0,3]$ and the pair $([1,1,1], M)$ satisfies (2.2) *in place of (L, M). Furthermore,* (2.2) *is equivalent to the conditions given in Tables* I *and* II.

Proof. Assume that binary lattices L and M satisfy (2.1). Then one can easily show that $L_q \simeq M_q$ for any prime $q \neq 2, p$, and $L_2 \simeq M_2$ or $(L_2, M_2) \simeq ([1,1,1],[1,0,3])$ (for details see, for example, [7]).

First, assume that $L_2 \simeq M_2$. If $L_p \simeq M_p$, then $D_L = D_M$. By Meyer's theorem on Dirichlet's conjecture, there is a prime $q \in A_{p,k}$ that is repre-

Table I ($x \in L$ is a primitive vector such that $\tau_x \in O(L)$)

p	$k \pmod p$	$o(L)$	D_L	$(\frac{Q(x)}{p})$	M
3	1	2	1 (mod 3)	$\times$	$[L:M]=3,\ u_p(M)=1$
3	2	2	1 (mod 3)	$\times$	$[L:M]=3,\ u_p(M)=-1$
3	1	4	1 (mod 3)	$\times$	$[L:M]=3,\ u_p(M)=1$
3	2	4	1 (mod 3)	$\times$	$[L:M]=3,\ u_p(M)=-1$
3	1	4	2 (mod 3)	-1	$[L:M]=3,\ u_p(M)=1$
3	2	4	2 (mod 3)	1	$[L:M]=3,\ u_p(M)=-1$
5	1, 4	4	$\pm 1 \pmod 5$	-1	$[L:M]=5,\ u_p(M)=1$
5	2, 3	4	$\pm 1 \pmod 5$	1	$[L:M]=5,\ u_p(M)=-1$

Table II

p	$k \pmod p$	L	M	p	$k \pmod p$	L	M
3	1	$[1,1,1]$	$[1,1,7]$	5	1, 4	$[1,1,1]$	$[1,1,19]$
5	2, 3	$[1,1,1]$	$[3,3,7]$	7	1, 2, 4	$[1,1,1]$	$[1,1,37]$
7	3, 5, 6	$[1,1,1]$	$[3,3,13]$	11	2, 6, 7, 8, 10	$[1,1,1]$	$[7,1,13]$
13	2, 5, 6, 7, 8, 11	$[1,1,1]$	$[7,5,19]$	3	1	$[1,0,1]$	$[1,0,9]$
3	2	$[1,0,1]$	$[2,2,5]$	5	1, 4	$[1,0,1]$	$[1,0,25]$
5	2, 3	$[1,0,1]$	$[2,2,13]$	7	3, 5, 6	$[1,0,1]$	$[5,2,10]$

sented by L. By assumption, q is also represented by M. Since there is only one equivalence class with discriminant D_L that represents the prime q, L is isometric to M. Therefore we may assume that

$$L_p \simeq [\epsilon_1, 0, \epsilon_2 p^\alpha] \quad \text{and} \quad M_p \simeq [\epsilon_1, 0, \epsilon_2 p^\beta],$$

where $\epsilon_i \in \mathbb{Z}_p^\times$, $\beta - \alpha$ is a positive even integer and $\epsilon_1 k \in (\mathbb{Z}_p^\times)^2$. Suppose that $\gamma_{p,u_p(M)}(L) \geq 2$ and L_1, L_2 are non-isometric binary lattices in $\Gamma_{p,u_p(M)}(L)$. If M is represented by both L_1 and L_2, then there is a prime that is represented by both L_1 and L_2. This is impossible for $D_{L_1} = D_{L_2}$. Therefore we may assume that M is not represented by L_1. Note that by Meyer's theorem, there is a prime $q \in A_{p,k}$ that is represented by L_1 and hence by L. Hence there is a sublattice ℓ of L_1 with $[L_1 : \ell] = p^{(\beta-\alpha)/2-1}$ that represents q. Since ℓ is not isometric to M and $D_\ell = D_M$, the prime q is not represented by M, which is a contradiction. Therefore $\Gamma_{p,(\frac{k}{p})}(L)$ consists of only one orbit, say $orb(K)$, and M is represented by K. If K is not isometric to M, then M is also represented by a primitive sublattice of K with index p. Since the number of such non-isometric lattices is greater than 1, this contradicts the assumption for the same reason as above. Therefore every lattice in $\Gamma_{p,(\frac{k}{p})}(L)$ is isometric to M. The converse is almost trivial.

To complete the proof, we have to find all possible cases such that $\gamma_{p,(\frac{k}{p})}(L) = 1$. This can be easily done by using Lemma 2.2 and Corollary 2.3.

Now assume without loss of generality that $L_2 \simeq [1,0,3],\ M_2 \simeq [1,1,1]$. Let

$$L_p \simeq [\epsilon_1, 0, \epsilon_2 p^\alpha] \quad \text{and} \quad M_p \simeq [\epsilon_1, 0, \epsilon_2 p^\beta],$$

where $\epsilon_i \in \mathbb{Z}_p^\times$ and $\epsilon_1 k \in (\mathbb{Z}_p^\times)^2$. First assume that $\alpha \geq \beta$. Since at most one sublattice of M with index 2 represents L, we have $M \simeq [1,1,1]$ by Lemma 2.5, and the pair $(L, [1,0,3])$ satisfies the condition (2.2). Note that $D_{[1,0,3]} = -12$ does not satisfy any of the discriminant conditions given in Table I. Hence such pairs do not exist.

Now assume that $\alpha < \beta$. Note that $\beta - \alpha$ is even. Let m be any sublattice of M with index 2 and let $\{L_1, \ldots, L_t\}$ be the set of all sublattices of L with index $[L_p : M_p]$. Note that $D_m = D_{L_i}$ for any $i = 1, \ldots, t$.

If m is not isometric to any of the sublattices L_i, then there is a prime $q \in A_{p,k}$ such that q is represented by m (and also by M) but is not represented by any of the L_i's by Meyer's theorem. Since every integer that is represented by L is also represented by at least one of the L_i's, q is not represented by L. This is a contradiction.

Therefore m is isometric to at least one of the L_i's. Since $M \not\simeq [1,1,1]$, the number of non-isometric sublattices of M with index 2 is two or three and hence $t \geq 2$. Furthermore, there is a sublattice whose isometry group is of order 4 in the former case. Since $2M$ is represented by any sublattice of M with index 2, there is a prime $q \in Q(M) - \{2, p\}$ such that

$$\sum_{\substack{m \subset M \\ [M:m]=2}} r(4q, m) \geq 6.$$

Since $L_i \cap L_j \subset pL$ for any $i \neq j$, the number of representations of $4q$ by L is greater than or equal to 6, that is, $r(4q, L) \geq 6$. Since we are assuming that $L_2 \simeq [1,0,3]$, there is a basis $\{x, y\}$ of L such that $Q(x) \equiv 1 \pmod 8$, $Q(y) \equiv 3 \pmod 8$ and $B(x,y) = 0 \pmod 4$. If $Q(ax + by) = 4q$, then $a \equiv b \pmod 2$. This implies that

$$r\left(q, \mathbb{Z}\left(\frac{x+y}{2}\right) + \mathbb{Z}y\right) \geq 6.$$

Since q is a prime and $\mathbb{Z}(\frac{x+y}{2}) + \mathbb{Z}y$ is a primitive lattice that is not isometric to $[1,0,1]$, we have $\mathbb{Z}(\frac{x+y}{2}) + \mathbb{Z}y \simeq [1,1,1]$. Therefore, $L \simeq [1,0,3]$. Since $Q([1,1,1]) = Q([1,0,3])$ and $[1,1,1]_2 \simeq M_2$, the pair $([1,1,1], M)$ satisfies (2.2). ∎

Corollary 2.7. *Let p be a prime greater than* 13 *and let k be any integer relatively prime to p. For any primitive binary lattices L and M, $Q(L) \cap A_{p,k} = Q(M) \cap A_{p,k}$ if and only if $L \simeq M$ or $(L, M) \simeq ([1,1,1], [1,0,3])$.*

Proof. This is a direct consequence of the previous theorem. ∎

Now we consider the case when $p = 2$.

THEOREM 2.8. *For any primitive binary $\mathbb{Z}$-lattices L and M such that $L \not\simeq M$ and $(L, M) \not\sim ([1,1,1],[1,0,3])$, $Q(L) \cap A_{2,1} = Q(M) \cap A_{2,1}$ if and only if either*

(i) *$(L, M) \sim ([a,b,a],[a,2b,4a])$, where $a \equiv 1 \pmod 2$ and $b \equiv 0 \pmod 2$, or*

(ii) *$L_2 \simeq \mathbb{H}_2$ and M is the unique primitive sublattice of L with index 2.*

Proof. Assume that $Q(L) \cap A_{2,1} = Q(M) \cap A_{2,1}$. Then $L_p \simeq M_p$ for any odd prime p. By a similar argument used in Theorem 2.6, we may assume that M is isometric to a sublattice of L with index 2^t for some non-negative integer t and there is only one primitive sublattice of L with index 2 up to equivalence.

Assume that $o(L) > 4$. Note that up to equivalence, $[1,0,3]$ is the unique sublattice of $[1,1,1]$ with index 2, and $[1,0,12],[3,0,4]$ are sublattices of $[1,0,3]$ with index 2. The primitive sublattice of $[1,0,1]$ with index 2 is $[1,0,4]$; the latter has two sublattices $[4,4,5],[1,0,16]$ with index 2, up to equivalence. Therefore $([1,0,1],[1,0,4])$ is the only pair satisfying the assumption.

From now on we assume that $o(L) = 2$ or 4. Suppose that $L_2 \not\simeq \mathbb{H}_2$. Then there is a basis $\{x, y\}$ of L such that both $Q(x)$ and $Q(y)$ are odd.

Assume that $o(L) = 2$. If there is an isometry $\sigma : \mathbb{Z}(2x) + \mathbb{Z}y \to \mathbb{Z}x + \mathbb{Z}(2y)$, then $\sigma(2x) \in 2L$. Hence σ induces an isometry of L, which is a contradiction.

Therefore $o(L) = 4$. Assume that $L \simeq [a,0,b]$ for some integers $a \neq b$. Then $[4a,0,b],[a,0,4b]$ and $[a+b,4b,4b]$ are all sublattices of L with index 2. One can easily show that there are exactly two primitive lattices among them up to equivalence.

If $L \simeq [a,b,a]$, then $[a,2b,4a],[2a-b,0,2a+b]$ are both sublattices of L with index 2. If $ab \equiv 1 \pmod 2$, both of them are primitive, and they are not isometric to each other by Lemma 2.5. Therefore $a \equiv 1 \pmod 2$ and $b \equiv 0 \pmod 2$. In this case, $[2a-b,0,2a+b]$ is not primitive. Since the isometry group of the lattice $[a,2b,4a]$ is trivial, the pair of L and any proper sublattice of $[a,2b,4a]$ does not satisfy the condition.

Finally, suppose that $L_2 \simeq \mathbb{H}_2$. Then there is a basis $\{x, y\}$ of L such that $Q(x) \equiv 2B(x,y) \equiv 1 \pmod 2$ and $Q(y) \equiv 0 \pmod 2$. Hence $\ell := \mathbb{Z}x + \mathbb{Z}(2y)$ is the only primitive sublattice of L with index 2. Therefore every odd integer that is represented by L is also represented by ℓ and vice versa. Note that $\ell_2 \not\simeq \mathbb{H}_2$ and every isometry of ℓ is contained in $O(L)$. Hence if $o(L) = 2$, then ℓ contains at least two non-isometric primitive sublattices with index 2

by the above observation. If $o(L) = 4$, then $L \simeq [a, b, a]$ for an even integer a and an odd integer b. Hence $\ell = [2a - b, 0, 2a + b]$ is the only primitive sublattice of L with index 2 and contains at least two non-isometric primitive sublattices with index 2. Therefore the pair of L and any proper sublattice of ℓ does not satisfy the condition. The proof of the converse is almost trivial. ∎

COROLLARY 2.9. *Let p be a prime and let k be a positive integer less than p. For any non-isometric primitive binary lattices L and M representing at least one integer in $A_{p,k}$, $r(pn + k, L) = r(pn + k, M)$ for any non-negative integer n if and only if $(p, k) = (2, 1), (3, 1)$ or $(3, 2)$, $L_p \simeq \mathbb{H}_p$, and M is the unique primitive sublattice of L with index p such that $u_p(M) = \left(\frac{k}{p}\right)$ only when $p = 3$.*

Proof. Assume that $r(pn + k, L) = r(pn + k, M)$ for any non-negative integer n. Then L and M satisfy the conditions in Theorem 2.6 or Theorem 2.8. Hence we may assume that either M is isometric to a sublattice of L with index p, or $L = [1, 0, 3]$. Furthermore we may assume that M is isometric to a sublattice of $[1, 1, 1]$ with index p in the latter case. Assume that $L \not\simeq [1, 0, 3]$. To satisfy the condition, $\Gamma_{p,u_p(M)}(L)$ contains only one lattice, which is stronger than the condition in (2.2). Using this, one can easily show that $p = 2, k = 1$ or $p = 3$, $k = 1$ or $p = 3$, $k = 2$, $L_p \simeq \mathbb{H}_p$, and M is the unique primitive sublattice of L with index p such that $u_p(M) = \left(\frac{k}{p}\right)$ only when $p = 3$.

Now assume that $L \simeq [1, 0, 3]$. Clearly, $p \neq 2$ by Theorem 2.8. Note that for any integer t,

$$r(2t + 1, [1, 1, 1]) = 3r(2t + 1, [1, 0, 3]) \quad \text{and} \quad r(2t, [1, 1, 1]) = r(2t, [1, 0, 3]).$$

Since the pair $([1, 1, 1], M)$ satisfies (2.2), there is a constant c such that

$$r(pn + k, [1, 1, 1]) = c \cdot r(pn + k, M)$$

for any integer n. Therefore there is an integer n such that $r(pn + k, L) \neq r(pn + k, M)$. The converse is almost trivial. ∎

3. Representations of multiples of a prime. For any integer D with $D \equiv 0, 1 \pmod 4$, the set $\mathfrak{S}_D$ of all proper equivalences (of primitive forms) having discriminant D forms a finite abelian group with the composition law. For any form f with $D_f = D$, the binary form f^{-1} is defined by any form in the proper equivalence class $\{f\}^{-1}$ in $\mathfrak{S}_D$. So it is well defined up to proper equivalence. Note that

$$f \simeq f^{-1} \quad \text{if and only if} \quad [o(f) : o^+(f)] = 2 \quad \text{if and only if} \quad o(f) \geq 4.$$

For binary forms f, f', g and g', even if $f \sim f'$ and $g \sim g'$, it can happen that $f \cdot g$ is not equivalent to $f' \cdot g'$. For example,

$$[3, 2, 10] \cdot [3, 2, 10] \simeq [5, 2, 6] \nsim [1, 0, 29] \simeq [3, 2, 10] \cdot [3, -2, 10].$$

Let L and M be primitive binary lattices. Note that the binary form $f_{\mathfrak{B}} \cdot f_{\mathfrak{B}'}$ depends on the choice of bases $\mathfrak{B}$ and $\mathfrak{B}'$ for L and M, respectively. However, the pair $(f_{\mathfrak{B}} \cdot f_{\mathfrak{B}'}, f_{\mathfrak{B}} \cdot f_{\mathfrak{B}'}^{-1})$ is independent of the choices of bases up to equivalence, so we use the notation $(f_L \cdot f_M, f_L \cdot f_M^{-1})$ up to equivalence. For any binary lattice L with $D_L = D$, the set $\{\{f_{\mathfrak{B}}\}, \{f_{\mathfrak{B}}\}^{-1}\} \subset \mathfrak{S}_D$ is also independent of the choice of the basis $\mathfrak{B}$ for L. Hence $(f_{\mathfrak{B}}, f_{\mathfrak{B}}^{-1})$ is independent of the choice of $\mathfrak{B}$ up to proper equivalence. So we also use the notation (f_L, f_L^{-1}) up to proper equivalence.

For any prime p, the *Watson transformation* $\Lambda_p(L)$ of a lattice L is defined by

$$\Lambda_p(L) = \{x \in L : Q(x+z) \equiv Q(z) \pmod{p} \ \forall z \in L\}.$$

Note that $\Lambda_p(L)$ is a sublattice of L which is not primitive. The primitive binary lattice obtained from $\Lambda_p(L)$ by a suitable scaling is denoted by $\lambda_p(L)$. One can easily show that

$$L_p \not\simeq \mathbb{H}_p \quad \text{if and only if} \quad Q(L) \cap p\mathbb{Z} = Q(\Lambda_p(L)).$$

Let L and M be primitive binary lattices such that

$$Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}. \tag{3.1}$$

Then one can easily show that $L_q \simeq M_q$ for any prime $q \neq 2, p$. If $p \neq 2$, then $L_2 \simeq M_2$ or $(L_2, M_2) \simeq ([1,1,1],[1,0,3])$ (see, for example, [7]). At the prime p, one can easily show that $L_p \simeq \mathbb{H}_p$ if and only if $M_p \simeq \mathbb{H}_p$. Hence if $L_p \not\simeq \mathbb{H}_p$, then $Q(\Lambda_p(L)) = Q(\Lambda_p(M))$. Therefore by Delone's result,

$$\lambda_p(L) \simeq \lambda_p(M) \quad \text{or} \quad (\lambda_p(L), \lambda_p(M)) \simeq ([1,1,1],[1,0,3]). \tag{3.2}$$

Note that (3.2) does not imply (3.1) even though neither L_p nor M_p is isometric to $\mathbb{H}_p$. For example, if $L = [1,0,p]$ and $M = [1,0,p^3]$, then $\lambda_p(L) \simeq \lambda_p(M) \simeq [1,0,p]$. However $r(p,L) = 2$, $r(p,M) = 0$. Note that if we add the condition $\mathfrak{n}(\Lambda_p(L)) = \mathfrak{n}(\Lambda_p(M))$, then (3.2) does imply (3.1).

From now on we assume that $L_p \simeq M_p \simeq \mathbb{H}_p$. For the time being we also assume that $L_2 \simeq M_2$ if $p \neq 2$. Then clearly M is contained in the genus of L. Let T be any binary $\mathbb{Z}$-lattice such that $D_T = D_L$ and $r(p,T) > 0$. Note that such a lattice is unique up to isometry.

LEMMA 3.1 ([10]). *Under the assumptions given above, if S is any lattice such that $D_S = D_L$, then*

$$r(pn, f_S) = r(n, f_S \cdot f_T) + r(n, f_S \cdot f_T^{-1}) - r(n/p, f_S).$$

THEOREM 3.2. *Under the assumptions above, if L is not isometric to M, then $Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}$ if and only if $|f_T| = 4$ and $f_L \sim f_M \cdot f_T^2$.*

REMARK 3.3. Note that $|f_T|$ is the order of f_T in the group under the composition law. If $|f_T| = 4$, then the binary form $f_M \cdot f_T^2$ is well defined up to equivalence.

Proof of Theorem 3.2. Assume that $Q(L)\cap p\mathbb{Z} = Q(M)\cap p\mathbb{Z}$. Note that for any integer n,

$$r(pn, f_L) = r(n, f_L\cdot f_T) + r(n, f_L\cdot f_T^{-1}) - r(n/p, f_L),$$
$$r(pn, f_M) = r(n, f_M\cdot f_T) + r(n, f_M\cdot f_T^{-1}) - r(n/p, f_M).$$

Suppose that $f_L\cdot f_T$ is equivalent to neither $f_M\cdot f_T$ nor $f_M\cdot f_T^{-1}$. Then by Meyer's Theorem, there is a prime q such that $r(q, f_L\cdot f_T) > 0$ and $r(q, f_M\cdot f_T) = r(q, f_M\cdot f_T^{-1}) = 0$. Then $r(pq, L) > 0$ and $r(pq, M) = 0$. This contradicts the assumption. Therefore

$$(f_L\cdot f_T, f_L\cdot f_T^{-1}) \sim (f_M\cdot f_T, f_M\cdot f_T^{-1}).$$

This implies that $(f_L\cdot f_T, f_L\cdot f_T^{-1})$ is properly equivalent to

$$(f_M\cdot f_T, f_M\cdot f_T^{-1}),\quad (f_M\cdot f_T, f_M^{-1}\cdot f_T),\quad (f_M^{-1}\cdot f_T^{-1}, f_M\cdot f_T^{-1})\quad \text{or}$$
$$(f_M^{-1}\cdot f_T^{-1}, f_M^{-1}\cdot f_T).$$

Since we are assuming that L is not isometric to M,

$$f_L \simeq f_M\cdot f_T^{-2} \simeq f_M\cdot f_T^2 \quad\text{or}\quad f_L \simeq f_M^{-1}\cdot f_T^{-2} \simeq f_M^{-1}\cdot f_T^2.$$

The proof of the converse is similar. ∎

Example 3.4. Let L and M be non-isometric primitive binary lattices such that $Q(L)\cap 2\mathbb{Z} = Q(M)\cap 2\mathbb{Z}$ and $L_2 \simeq M_2 \simeq \mathbb{H}_2$. To find all such pairs of lattices, we have to find an integer t such that $f_T = [2, 1, t]$ is of order 4. By a direct computation, we have $f_T^2 \simeq [4, 1, k]$ if $t = 2k$ is even, and $f_T^2 \simeq [4, -3, k+1]$ if $t = 2k+1$ is odd. If $|f_T| = 4$, then 1 is not represented by f_T^2, and f_T^2 should have a non-trivial isometry. Therefore $t = 5, 7$ or 8, and all possible such pairs are

$$(f_L, f_M) \simeq ([1,1,10],[3,3,4]),\ ([1,1,14],[4,3,4]) \text{ or } ([1,1,16],[4,1,4]).$$

The following lemma shows that such pairs are always finitely many for any prime p.

Lemma 3.5. *Let L and M be non-isometric primitive binary lattices having the same discriminant. If L and M satisfy condition* (3.1) *and $L_p \simeq M_p \simeq \mathbb{H}_p$, then $D_L \geq -4p^4 + 1$.*

Proof. By Theorem 3.2, there is a form $f \in \mathfrak{S}_{D_M}$ such that $r(p, f) > 0$ and $|f| = 4$. Then $|O(f^2)| \geq 4$. Since p^2 is primitively represented by f^2, there are integers u and t such that $f^2 \simeq [p^2, u, t]$ and $0 < |u| < p^2$. Suppose that $D_L = D_{f^2} \leq -4p^4$. Then $t \geq p^2 + 1$. This implies that $[p^2, u, t]$ is Minkowski reduced and the isometry group of f^2 is trivial. This is a contradiction. ∎

REMARK 3.6. Note that the bound given above is extreme. For example, if $(f_L, f_M) \simeq ([1,1,p^4],[p^2,1,p^2])$, then L and M satisfy all conditions in the above lemma.

Now assume that $L_p \simeq M_p \simeq \mathbb{H}_p$ $(p \neq 2)$, $L_2 \simeq [1,1,1]$ and $M_2 \simeq [1,0,3]$.

THEOREM 3.7. *Under the assumption above, $Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}$ if and only if there are odd integers a, b such that $f_L \sim [a,b,a]$, $f_M \sim [4a,2b,a]$, and p^2 is represented by $[4,2,(1-D_L)/4]$.*

Proof. Let T be a binary lattice such that $D_T = D_M$ and $r(p,T) > 0$. First assume that $Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}$. We may also assume that f_L is not equivalent to $[1,1,1]$.

Suppose that no sublattice of L with index 2 is isometric to M. Let $S(L)$ be a sublattice of L with index 2. Clearly, $D_{S(L)} = D_M$. For any integer n such that $r(pn, S(L)) > 0$, we have $r(pn, M) > 0$ by assumption. Hence, by a similar argument to that in Theorem 3.2, both $f_{S(L)} \cdot f_T$ and $f_{S(L)} \cdot f_T^{-1}$ is equivalent (not necessarily proper equivalent) to $f_M \cdot f_T$ or $f_M \cdot f_T^{-1}$. Since we are assuming that $f_{S(L)}$ is not equivalent to f_M,

$$f_{S(L)} \cdot f_T \simeq f_M^{-1} \cdot f_T^{-1} \text{ or } f_M \cdot f_T^{-1}$$

and

$$f_{S(L)} \cdot f_T^{-1} \simeq f_M \cdot f_T \text{ or } f_M^{-1} \cdot f_T.$$

By considering all possible cases, we have

$$\begin{aligned} &f_{S(L)} \simeq f_M \cdot f_T^2, \quad f_M^{-2} \simeq f_T^4, \qquad f_{S(L)} \simeq f_M^{-1} \cdot f_T^2, \quad f_T^4 \simeq I, \\ &f_{S(L)} \simeq f_M \cdot f_T^2, \quad f_T^4 \simeq I \quad \text{or} \quad f_{S(L)} \simeq f_M^{-1} \cdot f_T^2, \quad f_M^2 \simeq f_T^4, \end{aligned}$$

where $I \simeq [1,0,-D_M/4]$ is the form in the identity class. Note that if the first or the fourth case occurs, then $f_{S(L)}^2 \simeq I$. In all cases, $f_{S(L)}$ is equivalent to $f_M \cdot f_T^2$ or $f_M^{-1} \cdot f_T^2$. Therefore L has, up to isometry, only two sublattices, say $S_1(L)$ and $S_2(L)$, with index two. Furthermore since $|O(L)| = 4$ by Lemma 2.5, we may assume that $|O(f_{S_1(L)})| = 4$ and $|O(f_{S_2(L)})| = 2$. Since $f_{S_2(L)}^2 \not\simeq I$, only the second or third case can happen for this $S_2(L)$. Therefore $f_T^4 \simeq I$ and $S_1(L) \simeq S_2(L)$. This is a contradiction. Consequently, M is isometric to one of the sublattices of L with index 2.

Suppose that $|O(L)| = 2$. Then L has two non-isometric sublattices, say $S_2(L)$ and $S_3(L)$, with index 2 that are not isometric to M. Since $|O(S_i(L))| = 2$, we have $f_{S_i(L)}^2 \not\simeq I$ for $i = 2,3$. Therefore only the second or third case is possible, and $f_{S_2(L)} \sim f_{S_3(L)}$. This is a contradiction. Therefore $|O(L)| = 4$ and hence there are odd positive integers a and b such that $f_L \sim [a,b,a]$. Let $S_1(L) \simeq M$ and let $S_2(L)$ be the other sublattice of L with index 2 that is not isometric to $S_1(L)$.

Suppose that $f_M \sim [2a+b, 0, 2a-b]$. Since $f_M^2 = I$, we also have $f_{S_2(L)}^2 = I$ by a similar reasoning to the above. This is a contradiction.

Therefore $f_M \sim [a, 2b, 4a]$ and $f_{S_2(L)} \sim [2a-b, 0, 2a+b]$. Finally, since $f_T^2 \sim f_M \cdot f_{S_2(L)} \sim [4, 2, (1-D_L)/4]$, p^2 is represented by $[4, 2, (1-D_L)/4]$.

Now we prove the 'if' part. If $f_L \simeq [1,1,1]$, then everything is trivial. So we assume that $D_L < -4$. First we show that $[4, 2, (1-D_L)/4] \sim f_T^2$. Since

$$\sum_{g \in \mathfrak{S}_{D_M}} r(p^2, g) = 2 \sum_{t \mid p^2} \left(\frac{D_M}{t} \right) = 6,$$

we have $r(p^2, I) = 2$ and

$$r\left(p^2, \left[4, 2, \frac{1-D_L}{4}\right]\right) = r\left(p^2, \left[4, -2, \frac{1-D_L}{4}\right]\right) = 2.$$

If $f_T^2 \simeq I$, then p^2 is primitively represented by $I \simeq [1, 0, -D_L]$ (see [3]), which is a contradiction. The assertion follows from this. Since M is isometric to a sublattice of L with index 2, $Q(M) \cap p\mathbb{Z} \subset Q(L) \cap p\mathbb{Z}$. Assume that $pn \in Q(L) \cap p\mathbb{Z}$. Since every integer that is represented by L is also represented by a sublattice of L with index 2, we may assume that pn is represented by the sublattice S of L with index 2 such that $f_S \sim [2a-b, 0, 2a+b]$. Hence n is represented by $f_S \cdot f_T$ or $f_S \cdot f_T^{-1}$. Since

$$f_M \cdot f_S \sim [a, 2b, 4a] \cdot [2a-b, 0, 2a+b] \sim \left[4, 2, \frac{1-D_L}{4}\right] \sim f_T^2,$$

we have $f_M \cdot f_S \simeq f_T^2$ or f_T^{-2}. In the former case,

$$f_S \cdot f_T^{-1} \simeq f_M^{-1} \cdot f_T \sim f_M \cdot f_T^{-1},$$

and in the latter,

$$f_S \cdot f_T \simeq f_M^{-1} \cdot f_T^{-1} \sim f_M \cdot f_T.$$

Therefore n is represented by $f_M \cdot f_T$ or $f_M \cdot f_T^{-1}$. This implies that pn is represented by M. The theorem follows from this. ∎

Note that $D_L \geq -4p^2 + 1$ in the above theorem. Therefore the number of pairs (L, M) of binary lattices such that $Q(L) \cap p\mathbb{Z} = Q(M) \cap p\mathbb{Z}$, $L \not\simeq M$ and $\lambda_p(L) \not\simeq \lambda_p(M)$ is finite for any prime p. Table III provides all such pairs when $p = 3$.

THEOREM 3.8. *Let p be a prime and let L, M be non-isometric primitive binary lattices. Then $r(pn, L) = r(pn, M)$ for any integer n if and only if neither L_p nor M_p is isometric to $\mathbb{H}_p$ and $\Lambda_p(L) \simeq \Lambda_p(M)$.*

Proof. Assume that $r(pn, L) = r(pn, M)$ for any integer n. Then L and M satisfy condition (3.1).

Suppose that $L_p \simeq \mathbb{H}_p$ and $L_2 \simeq M_2$ when $p \neq 2$. Then by Theorem 3.2, $(f_L \cdot f_T, f_L \cdot f_T^{-1}) \sim (f_M \cdot f_T, f_M \cdot f_T^{-1})$, where T is a binary lattice such that

Table III (for $p = 3$)

	f_L, f_M	f_L, f_M	f_L, f_M
$L_3 \simeq M_3 \simeq \mathbb{H}_3$, $L_2 \simeq M_2$	$[1,0,17], [2,2,9]$	$[1,0,32], [4,4,9]$	$[1,0,56], [8,8,9]$
$L_3 \simeq M_3 \simeq \mathbb{H}_3$, $L_2 \simeq M_2$	$[7,0,8], [4,4,15]$	$[1,0,65], [9,8,9]$	$[5,0,13], [2,2,33]$
$L_3 \simeq M_3 \simeq \mathbb{H}_3$, $L_2 \simeq M_2$	$[1,0,77], [9,4,9]$	$[7,0,11], [2,2,39]$	$[1,0,80], [9,2,9]$
$L_3 \simeq M_3 \simeq \mathbb{H}_3$, $L_2 \simeq M_2$	$[5,0,16], [4,4,21]$	$[1,1,39], [5,5,9]$	$[1,1,51], [7,7,9]$
$L_3 \simeq M_3 \simeq \mathbb{H}_3$, $L_2 \simeq M_2$	$[1,1,69], [9,7,9]$	$[1,1,81], [9,1,9]$	$[5,1,15], [7,3,11]$
$L_3 \simeq M_3 \simeq \mathbb{H}_3$, $L_2 \simeq M_2$	$[1,1,75], [9,5,9]$		
$L_3 \simeq M_3 \simeq \mathbb{H}_3$, $L_2 \not\simeq M_2$	$[3,1,3], [3,2,12]$	$[1,1,9], [4,2,9]$	$[1,1,3], [4,2,3]$
$L_3 \not\simeq \mathbb{H}_3$	$[1,1,1], [1,0,3]$	$[1,1,7], [1,0,27]$	$[1,1,7], [4,2,7]$

$D_T = D_L$ and $r(p,T) > 0$. Therefore $r(n/p, L) = r(n/p, M)$ for any integer n by Lemma 3.1. This is a contradiction for $r(1,[1,1,1]) \neq r(1,[1,0,3])$ and $L \not\simeq M$.

Suppose that $L_p \simeq \mathbb{H}_p$ and $L_2 \simeq [1,1,1] \not\simeq M_2$. Then by Theorem 3.7, M is a sublattice of L with index 2. One may easily show that there is an integer n such that $r(pn, L) > r(pn, M)$. Suppose that neither L_p nor M_p is isometric to $\mathbb{H}_p$. Then $r(pn, L) = r(pn, \Lambda_p(L))$ and $r(pn, M) = r(pn, \Lambda_p(M))$. Therefore $\mathfrak{n}(\Lambda_p(L)) = \mathfrak{n}(\Lambda_p(M))$ and $r(n, \lambda_p(L)) = r(n, \lambda_p(M))$ for any integer n. The theorem follows from this. The converse is trivial. ∎

Acknowledgements. The first author was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (grant number NRF-2013-R1A1A2011655).

The second author was supported by NRF-2011-0016437 and NRF-2010-0019516 funded by the Korea government (MEST).

References

[1] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, Wiley, 1997.

[2] B. N. Delone, *Geometry of positive quadratic forms. Part II*, Uspekhi Mat. Nauk 4 (1938), 102–164 (in Russian).

[3] A. G. Earnest and R. W. Fitzgerald, *Represented value sets for integral binary quadratic forms and lattices*, Proc. Amer. Math. Soc. 135 (2007), 3765–3770.

[4] W. C. Jagy and I. Kaplansky, *Positive definite binary quadratic forms that represent the same primes*, preprint.

[5] Y. Kitaoka, *Arithmetic of Quadratic Forms*, Cambridge Univ. Press, 1993.

[6] L. K. Hua, *Introduction to Number Theory*, Springer, London, 2011.

[7] D. Li, *Indefinite binary forms representing the same numbers*, Math. Proc. Cambridge Philos. Soc. 92 (1982), 29–33.

[8] A. Meyer, *Ueber einen Satz von Dirichlet*, J. Reine Angew. Math. 103 (1888), 98–117.

[9] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer, New York, 1963.
[10] G. Pall, *The structure of the number of representations function in a positive binary quadratic form*, Math. Z. 36 (1933), 321–343.
[11] J. Voight, *Quadratic forms that represent almost the same primes*, Math. Comp. 259 (2007), 1589–1617.
[12] H. Weber, *Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist*, Math. Ann. 20 (1882), 301–329.

Myung-Hwan Kim
Department of Mathematical Sciences
Seoul National University
Seoul 08826, Korea
E-mail: mhkimath@snu.ac.kr

Byeong-Kweon Oh
Department of Mathematical Sciences and
Research Institute of Mathematics
Seoul National University
Seoul 08826, Korea
E-mail: bkoh@snu.ac.kr