NUMBERS OF THE FORM $ax^2 + by^2$

R. MORIKAWA

1. Introduction

Let $a, b \in \mathbb{N}$ which are square free and $(a, b) = 1$. We put $V(a, b) = \{ax^2 + by^2 |\ x, y \in \mathbb{N}\}$. Our aim is to study the structure of $V(a, b)$. A talk on this theme was given at AC 2009, whose Proceedings will appear in ($http://tnt.math.metro-u.ac.jp$) [1].

(Important Remarks) (a) It is regrettable that many propositions given in this report have no proofs. But they are supported by numerical research of about 150 (a, b)'s. Thus we use Assertion for Proposition in this report. And about Numerical Examples given in the report, "all properties" are not proved.

(b) We introduce many new methods and concepts to solve the problem. Many of them are used in treating other problems. And some of them allow a proof (cf. [1]).

2. Preliminary discussion

First note that $t \in V(a, b)$ if and only if $at \in V(1, ab)$. Thus we may confine to the case $V(1, B)$ with square free B.

1. We put $4B = D$. We denote $DP = \{$ prime divisors of $D\ \}$. And we put $|DP| = \rho$. For $U \subset [1, D-1]$, We put $Q(D\ ;\ U) = \{p \mid \text{prime},\ p \equiv u \pmod{D}$ for some $u \in U\}$.
For X a set of primes, $cl(X)$ denotes $\{$ the free products of primes in $X\ \} \cup \{1\}$.

2. An element of $V(1, B)$ is called a V-element. We separate V-elements into three types :
(a) $R(1, B) = \{p \in V \mid p \text{ prime},\ p \nmid D\}$,
(b) $S(1, B) = \{n \in V \mid n \text{ composite}, (n, D) = 1\}$,
(c) $T(1, B) = \{n \in V \mid (n, D) > 1\}$.
These sets are simply noted R, S, T.

3. (Head system) For $V(1, B)$, we attach $\boldsymbol{H}(B) = \{B + r^2 \mid 0 \le r \le s\}$. ($s$ is taken a suitable number for each situation.) We call $\boldsymbol{H}(B)$ Head system of $V(1, B)$. We put
$BP = \{p \mid$ a proper prime divisor of $B + r^2$ for some r with $1 \le r \le s,\ (p, D) = 1\}$.
In the following, we need some Choosing-rules (i.e. $(CR\mathrm{I})$-$(CR\mathrm{III})$) to take suitable prime divisors of $B + r^2$ $(1 \le r \le s)$.

4. For a subset M of V, we define $CoreM$ as follows.
(i) Note that $v \in V$ implies $t^2 v \in V$ for any $t \in \mathbb{N}$. Thus if $w \in M$ allows $t \ge 2$ for which w/t^2 is in V, we omit w from M.
(ii) Note that for $V(1, B)$, $v, w \in V$ implies $vw \in V$. Thus we let $CoreM$ so that its member has no decomposition of this type.
In this situation, we say that the members of $CoreM$ are irreducible.

5. ($Core\hat{T}$) T contains V-elements of special type. We define following three sets: $T(0) = \{t \in T \mid t \in cl(DP)\}$, $T(1) = \{By \in T \mid y > 1, (y, D) = 1\}$ and $T(2) = \{2By \mid y > 1, (y, D) = 1\}$. Note the facts $Bt \in V(1, B) \Leftrightarrow t \in V(1, B)$ and $2Bt \in V(1, B) \Leftrightarrow 2t \in V(1, B)$. Hence we make $\hat{T} = T \setminus (T(0) \cup T(1) \cup T(2))$, and study $Core\hat{T}$ instead of $CoreT$. We treat $T(0)$ separately.

Date: May 21, 2010.

3. Sets F, G, M, $Q(j)$ $(2 \leq j \leq J)$

We define the following sets step by step. (See Example 4.1.)

Step 1. Let $D = 4B$. And $F = \{n \mid n \in [1, D-1], (n, D) = 1\}$. Then $|F| = \varphi(D)$. Here F is a multiplicative group. We put $G = \{u^2 \pmod D \mid (u, D) = 1\}$, and consider
G as a subgroup of F. Then $[F : G] = 2^\rho$.

Step 2. We take M where M is minimal for which $R \subset Q(D; M)$.

Assertion 2.1. $M = G$ for $B \equiv 1 \pmod 4$. And $M = G \cup xG$ for $B \equiv 2, 3 \pmod 4$, where x is chosen by the following rule.

(CRI) We decompose $B+1, B+4, \ldots$. And we take the first prime p for which
(a) $B + r^2 = p^t u^2$ with odd t and $u \in \mathbb{N}$, (b) $p \nmid D$.
Here p can be taken as x. M is a subgroup of F. We put $m = [M : G]$.

We say $V(1, B)$ is Full-case if $R = Q(D; M)$. And NF-case in otherwise. In NF-case, we put $M(\tau) = Q(D; M) \setminus R$. And MP denotes the set of pimes in $M(\tau)$.

Step 3. We arrange Cosets of F/M as follows.
($\sharp$) $M,\ t_2 M, \ldots, t_{2J} M$.
The cardinality satisfies $2mJ = 2^\rho$. From ($\sharp$), we choose $t_j M$ $(2 \leq j \leq J)$ by the following rule :

(CRII) Let $\boldsymbol{H}(B)$ be Head system of $V(1, B)$. We consider $p \in BP$, and choose p's which belong to different Cosets.

We explain the process taking $B = 105$:

($B = 105$) In the case $M = \{1, 109, 121, 169, 289, 361\}$. We have
$B+1 = 106 = 2 \cdot 53$, $B+4 = 109 =$ prime, $B+9 = 114 = 2 \cdot 3 \cdot 19$, $B+16 = 121 = 11^2$, $B+25 = 130 = 2 \cdot 5 \cdot 13$, $B+36 = 141 = 3 \cdot 47$, $B+49 = 154 = 2 \cdot 7 \cdot 11$, $B+64 = 169 = 13^2$, $B+81 = 186 = 2 \cdot 3 \cdot 31$, $B+100 = 205 = 5 \cdot 41$, $B+121 = 226 = 2 \cdot 113$, $B+144 = 249 = 3 \cdot 83$, $B+169 = 274 = 2 \cdot 137$, $B+196 = 301 = 7 \cdot 43$, etc.

We choose 7 numbers 53, 19, 11, 13, 47, 41, 43. And we get 7 Cosets which contain these numbers.

Assertion 2.2. Applying (CRII), we obtain $J-1$ Cosets from ($\sharp$). We make $Q(j) = Q(D; t_j M)$ for such j. Let x_j be the least member of $Q(j)$. Here we rearrange $Q(j)$ so that $x_2 < x_3 < \cdots < x_J$.

We call each $Q(j)$ a Cell. And HP denotes the set of primes contained in $Q(j)$ $(2 \leq j \leq J)$.

4. R, $CoreS$, $Core\hat{T}$ for Full-case

For Full-case, we write $Q(j) = (x_j; \sim)$. We define multiple law of $Q(j)$'s as follows:
($\star$) Let $L(M) = L(1) = \{n \in \mathbb{N} \mid n \equiv m \pmod D$ for some $m \in M\}$, and $L(j) = \{n \in \mathbb{N} \mid n \equiv x_j m \pmod D$ for some $m \in M\}$, $(2 \leq j \leq J)$. We define $\{i, j\} = k$ if $x_i x_j \in L(k)$.

Assertion 3.1 ($CoreS$) Let $V(1, B)$ be Full-case. Then $s \in CoreS$ if and only if s satifies the following three conditions:
(1) $s \in cl(HP)$, (2) $s \in L(M)$. (3) s is irreducible.

(Taking-combination) Take $t \in cl(HP)$. Let $t = p_1^{e_1} \cdots p_f^{e_f}$. We put $s(j)$ the sum of e_i for which $p_i \in Q(j)$. We call $(s(2), \ldots, s(J))$ Taking combination of t.

Then Taking-combination of $CoreS$ is finite. In Example 4.1. $CoreS$ of $V(1, 105)$ have Taking-combinations of (1), (2), (3).

To clarify $Core\hat{T}$, we use the following concepts. Let $U = \{u \in \mathbb{N} \mid 1 < u < 2B,\ u|2B,\ u \neq B\}$. For $u \in U$, we put $((u)) = \{uy \in T \mid y > 1, (y, D) = 1\}$. We define $(u) \Rightarrow Q(j)$ if $ux_j \in V$.

Assertion 3.2. (Transfer rule) Assume $(u) \Rightarrow Q(j)$ for $u \in U$. Then $Core((u)) = uC$ where C is given by Transfer rule.

(Transfer rule) : List up Taking-combination $(s(2), \ldots, s(j), \ldots, s(J))$ of $CoreS$ which satisfy the condition $s(j) \geq 1$. Then $C = \{c \in cl(HP) \mid$ Taking-combination of $c = (s(2), \ldots, s(j) - 1, \ldots, s(J))$.

By this rule, $Core\hat{T}$ is obtainable from $CoreS$. (See the following Example.)

(Example) : We give an Example to clarify these Assertions.

Example 4.1. $V(1, 105)$: Here $D = 420$ and $G = \{1, 109, 121, 169, 289, 361\}$. We have $G = M$ and $R = Q(420; G)$. As stated in Step 3, we have the following:

$Q(2) = (11; \sim)$, $Q(3) = (13; \sim)$, $Q(4) = (19; \sim)$, $Q(5) = (41; \sim)$, $Q(6) = (43; \sim)$, $Q(7) = (47; \sim)$, $Q(8) = (53; \sim)$.

On the other hand we obtain the following $(\star)$-rule:
{2,3} = 7, {2,4} = 5, {2,5} = 4, {2,6} = 8, {2,7} = 3, {2,8} = 6, {3,4} = 6,
{3,5} = 8, {3,6} = 4, {3,7} = 2, {3.8} = 5, {4,5} = 2, {4,6} = 3, {4,7} = 8,
{4,8} = 7, {5,6} = 7, {5,7} = 6, {5,8} = 3, {6,7} = 5, {6,8} = 2, {7,8} = 4.

($CoreS$) Thus $CoreS$ consists of
(1) $\{s^2 \mid s \in Q(j)\}(2 \leq j \leq 8)$.
(2) $\{stu \mid s \in Q(i), t \in Q(j), u \in Q(k)\}$ where (i, j, k) = (2,3,7), (2,4,5), (2,6,8), (3,4,6), (3,5,8), (4,7,8), (5,6,7)
(3) $\{stuv \mid s \in Q(i), t \in Q(j), u \in Q(k), v \in Q(l)\}$ with (i, j, k, l) = (2,3,4,8), (2,3,5,6), (2,4,6,7), (2,5,7,8), (3,4,5,7), (3,6,7,8), (4,5,6,8).

For $Core\hat{T}$, note that (2) $\Rightarrow Q(8)$, (3) $\Rightarrow Q(7)$, (5) $\Rightarrow Q(5)$, (7) $\Rightarrow Q(6)$, (6) $\Rightarrow Q(4)$, (10) $\Rightarrow Q(3)$, (14) $\Rightarrow Q(2)$, (15) $\Rightarrow Q(6)$, (21) $\Rightarrow Q(5)$, (35) $\Rightarrow Q(7)$, (30) $\Rightarrow Q(2)$, (42) $\Rightarrow Q(3)$, (70) $\Rightarrow Q(4)$.

Thus we get $Core\hat{T}$ by Assertion 3.4. For example, $Core((2))$ is $2Q(8)$, $2Q(2)Q(6)$, $2Q(3)Q(5)$, $2Q(4)Q(7)$, $2Q(2)Q(3)Q(4)$, $2Q(2)Q(5)Q(7)$, $2Q(3)Q(6)Q(7)$, $2Q(4)Q(5)Q(6)$.

5. τ-separation, h-separtion

The situation is much more complicated for NF-case. First we introduce two $\sim$ classifications.

(τ-separation) Let $M(\tau) = Q(D; M) \setminus R$. We take y_1 the smallest member of $M(\tau)$. We put $(y_1; \sim) = \{y_1\} \cup \{y \in M(\tau) \mid y_1 y \in V\}$. We denote $M(\tau_1) = (y_1; \sim)$. If $M(\tau_1) = M(\tau)$, the process stops. And if $M(\tau) \setminus M(\tau_1) \neq \emptyset$, we take the smallest member y_2 of $M(\tau) \setminus M(\tau_1)$. And make $(y_2; \sim) = \{y \in M(\tau) \setminus M(\tau_1) \mid y_2 y \in V\} \cup \{y_2\}$. We put $M(\tau_2) = (y_2; \sim)$. If $M(\tau) \setminus (M(\tau_1) \cup M(\tau_2)) \neq \emptyset$, we continue the process taking y_3. Thus finally we obtain $\sim$ classification of $M(\tau)$.

Assertion 5.1. By $\sim$ classification of $M(\tau)$, we obtain a finite classification $M(\tau) = \cup_{k=1}^{K} M(\tau_k)$ where $M(\tau_k) = (y_k; \sim)$ with $1 \leq k \leq K$. We call each $M(\tau_k)$ an M-Cell.

For $t, u \in \mathbb{N}$, we denote $t \sim u$, if $tu \in V$. About τ-separation, there are two types. Namely if $y_k \sim y_k$, we say $M(\tau_k)$ to be square type, and denote $M(\tau_k)$ (sqr). And $M(\tau_k)$ is said to be different type if $y_k \not\sim y_k$. For the case, we write $M(\tau_k)$(dif).

Assertion 5.2. If $M(\tau_k)$ is of square type, $y \sim y$ for all $y \in M(\tau_k)$. The same property holds for $M(\tau_k)$ of different type.

(h-separation) We operate $\sim$ clasification for each $Q(j)$. We call this operation as h-separation. Let $H(j)$ be the cardinality of h-separation of $Q(j)$.

Assertion 5.3. Each $Q(j)$ separates $H(j)$ $(< \infty)$ sets. We put $Q(j) = \cup_t Q(j; t)$ with $1 \leq t \leq H(j)$ for each j. Let $Q(j; t) = (x_j(t); \sim)$, and call it H-Cell.

(Structure Constant, Base-set) We arrange $(K;\ H(2), \ldots, H(J))$ and call it Structure Constant (SC) of $V(1; B)$. And make $< y_k\ (1 \leq k \leq K) \mid X(2), \ldots, X(J) >$ where $X(j) = \{x_j(t) \mid 1 \leq t \leq H(j)\}$, and call it Base-set of $V(1; B)$.

6. DMH-decomposition, Lifting Principle

We use Y as a general name of a Cell. And we use ω as a general name of $Y = (\omega; \sim)$.

Assertion 6.1. (DMH decomposition) Let $v \in Core(V \setminus R)$. Then $v = dmh$ with $d \in cl(DP)$, $m \in cl(MP)$, $h \in cl(HP)$.

(Taking combination) As for mh, m is a product of primes taken from $M(\tau_k)(1 \leq k \leq K)$. Taking ways are $(\emptyset)$, (one), ($\forall$ two), (different two), ($\forall$ three), (t^4), (t^6) etc.
A similar property hold for h with H-Cells. Collecting those taking-ways, we get Taking-combination of mh.

Assertion 6.2. (Lifting Principle) All mh with the same Taking-combination are $\in V$ or $\notin V$ simultaneously.

To study $Core\hat{T}$ we define as follows:
Let $Y = (\omega; \sim)$. For some $r \in \mathbb{N}$, we define $(r) \Rightarrow Y$ if $r\omega \in V$. In some cases, Transfer rule works to obtain $Core\hat{T}$.
We give five numerical Examples which suggest the complexity of the nature of $CoreS$ and $Core\hat{T}$.

7. Numerical Examples

Example 7.1. $V(1, 11)$: We see $D = 44$, $m = 2$, $G = \{1, 5, 9, 25, 37\}$ and $M = G \cup 3G$, and $R = \{47, 53, 103, 163, 199, 257, 269 \ldots\}$. We put $M(\tau) = Q(44; M)\backslash R$. We have $M(\tau) = \{3, 5, 23, 31, 37, 59, 67, 71 \ldots\}$. $M(\tau)$ does not separates. Some caluculation show that $CoreS$ consists of (1) $\{st \mid s, t \in M(\tau), s \neq t\}$, (2) $\{stu \mid s, t, u \in M(\tau)\}$.
With respect to T, $T(0) = \emptyset$. And we see $Core\hat{T} = 4M(\tau) \cup \{4t^2 \mid t \in M(\tau)\}$.

Example 7.2. $V(1, 47)$: Then $D = 188$. We see $J = 1$, and $|M| = 46$. In this case, $M(\tau)$ separates to two Cells. $M(\tau_1) = (3; \sim)$ and $M(\tau_2) = (7; \sim)$. We denote each as $M(1)$ and $M(2)$.
Some calculations show that $CoreS$ consists of
(1) $\{st \mid s, t \in M(k), s \neq t\}$ for $k = 1, 2$, (2) $\{t^5 \mid t \in M(k)$ for $k = 1, 2$, (3) $\{stu \mid s, t \in M(1), u \in M(2)\}$, (4) $\{stu \mid s \in M(1), t, u \in M(2)\}$, (5) $\{stuv \mid s, t, u \in M(1), v \in M(2)\}$, (6) $\{stuv \mid s \in M(1), t, u, v \in M(2)\}$.
We see $CoreT(0)$=128. $Core\hat{T}$ consists of (1) $8M(2)$, (2) $\{8tu \mid t, u \in M(1)\}$,
(3) $\{8tu \mid t \in M(1), u \in M(2)\}$, (4) $\{8tuv \mid t.u, v \in M(1)\}$,
(5) $16M(1)$, (6) $\{16st \mid s, t \in M(1), s \neq t\}$, (7) $\{16st \mid s \in M(1), t \in M(2)\}$, (8) $\{16st \mid s, t \in M(2)\}$, (9) $\{16stu \mid s, t, u \in M(1), s, t, u$ all differs$\}$, (10) $\{16t^4 \mid t \in M(1)\}$, (11) $32M(1)$, (12) $\{32st \mid s, t \in M(2)\}$, (13) $\{64s \mid s \in M(2)\}$, (14) $\{64t^2 \mid t \in M(1)\}$.
(The complexity of T seems to become from the fact that $B = 43 \equiv 7 \pmod 8$.

Example 7.3, $V(1, 17)$: Here $M(\tau)$ and $Q(2)$ do not separates.
$CoreS$ cnsists of (1) $\{st \mid s, t \in M(\tau)\}$, (2) $\{st \mid s, t \in Q(2), s \neq t\}$, (3) $\{t^4 \mid t \in Q(2)\}$, (4) $\{stu \mid s \in M(\tau), t, u \in Q(2)\}$.
And we see $Core\hat{T}$ consists of $2M(\tau)$ and $\{2tu \mid t, u \in Q(2)\}$.

Example 7.4. $V(1, 65)$: Here we have five Cells, namely $M(\tau) = (29; \sim)$, $Q(2) = (3; \sim)$, $Q(3) = (11; \sim)$, $Q(4; 1) = (37; \sim)$ and $Q(4; 2) = (97; \sim)$. (For simplicity, we denote $M(\tau)$ as M, $Q(4; 1)$ as $Q(\sigma)$ and $Q(4; 2)$ as $Q(\tau)$.)
$CoreS$ consists of the following sets :(1) $\{st \mid s, t \in Q(j), s \neq t\}$ for $j = 1, 2$. (2) $\{t^4 \mid t \in Q(j)\}$ for $j = 1, 2$. (3) $\{st \mid s, t \in Q(\sigma)\}$, (4) $\{st \mid s, t \in Q(\tau)\}$, (5) $\{stu \mid s \in Q(2), t \in Q(3), u \in Q(4)\}$, (6) $\{t^2u^2 \mid t \in Q(2), u \in Q(3)\}$, (7) $\{stuv \mid s, t \in Q(j), u \in Q(\sigma), v \in Q(\tau)\}$ for $j = 2, 3.$, (8) $\{st \mid s, t \in M\}$, (9) $\{stu \mid s \in M, t, u \in Q(j)\}$ for $j = 2, 3.$, (10) $\{stu \mid s \in M, t \in Q(\sigma), u \in Q(\sigma)\}$ (11) $\{stuv \mid s \in M, t \in Q(2), u \in Q(3), v \in Q(4)\}$.
Core T are given by Transfer rule. Note that (2) $\Rightarrow Q(\sigma)$, (5) $\Rightarrow Q(\tau)$, (13) $\Rightarrow Q(\tau)$, (10) $\Rightarrow M$, and (26) $\Rightarrow M$.

Example 7.5. V(1,41) : We have four Cell's. They are $M(\tau_1)$, $M(\tau_2)$, $Q(2; 1)$, and $Q(2; 2)$. (We write them as $M(1), M(2), Q(\sigma), Q(\tau)$.)
$CoreS$ consists of the following sets : (1) $\{st \mid s, t \in M(1), s \neq t\}$, (2) $\{t^4 \mid t \in M(1)\}$, (3) $\{st \mid s, t \in M(2)\}$, (4) $\{st \mid s, t \in Q(\sigma), s \neq t\}$, (5) $\{st \mid s, t \in Q(\tau), s \neq t\}$, (6) $\{stu \mid s, t \in M(1), u \in M(2)\}$, (7) $\{stuv \mid s, t, u \in Q(\sigma), v \in Q(\tau)\}$, (8) $\{stuv \mid s \in Q(\sigma), t, u, v \in Q(\tau)\}$, (9) $\{t^2u^2 \mid t \in Q(\sigma), u \in Q(\tau)\}$, (10) $\{stu \mid s \in M(1), t, u \in Q(2)\}$, (11) $\{stuv \mid s, t \in M(1), u \in Q(\sigma), v \in Q(\tau)\}$, (12) $\{stu \mid s \in M(2), t \in$

$Q\sigma), u \in Q(\tau)\}$, (13) $\{stuvw \mid s \in M(2), t, u, \in Q(\sigma), v, w \in Q(\tau)\}$, (14) $\{stuvw \mid s \in M(2), t, u, v, w \in Q(\sigma)\}$, (15) $\{stuvw \mid s \in M(2), t, u, v, w \in Q(\tau)\}$, (16) $\{stuv \mid s \in M(1), t \in M(2), u, v \in Q(2)\}$.

$Core\hat{T}$ is given easily by noting the fact $(2) \Rightarrow M(2)$.

8. Further Research

8-1. Above examples suggest the complexity of $V(1; B)$ for NF-cases. We tried to seek the way to overcome the difficulties by scrutinizing Numerical Results. But a right way is not yet clear. Thus we use "Fact" to indicate this situation.

(Full-case) Fact 1. $V(1; B)$ is Full-case for $B = 1$, 2, 3, 7, 10, 13, 15, 21,22, 30, 31, 37, 42, 57, 58, 70, 78, 105, 165, 210, 330, 462.

Fact 2. We conjecture that the cardinality of square free B's with Full-case is finite. It is desirable to obtain a complete list of them.

For NF-case, we classify $V(1; B)$ with its (SC), especially by its J.

(Case $J = 1$) Fact 1. We have the following list:

$K = 1$ for $B = 11$, 19, 23, 31, 43, 67. $K = 2$ for $B = 47$, 79, 103. $K = 3$ for $B = 71$. $K = 4$ for $B =$59, 83, 107, 211. $K = 5$ for $B = 167$. $K = 6$ for $B = 191$. $K = 7$ for $B = 131$, 179. $K = 10$ for $B = 251$.

Fact 2. It is notable that $B \equiv 3 \pmod 8$ for $K = 4$, 7, 10. And $B \equiv 7 \pmod 8$ for $K = 2$, 3, 5, 6.

(Case $J = 2$) Fact 1. Known (SC)'s with $J = 2$ are of type (1;1), (1;2), (2;2), (2;3), (3;3), (3;4), (4;4).

Fact 2. The following B's are known for each (SC)'s :

(1;1) for $B = 14$, 17, 34, 39, 46, 55, 73. (1;2) for $B = 26$, 29, 35, 38, 52, 53, 61, 87. (2;2) for $B =$ 41, 62, 95, 137. (2;3) for $B = 86$, 181. (3;3) for $B = 89$. (3;4) for $B = 101$, 149, 173. (4;4) = for $B = 257$.

(Case $J = 4$) For $J = 4$, only two (SC)'s appear. Namely (1; 1,1,2) for $B = 65$, 66, 69, 77. And (1; 2,2,2) for $B = 231$.

It seems plausible that the other (SC)'s do not appear.

8-2. To clarify these $V(1; B)$'s, it seems the following $(CR\text{III})$ works.

$(CR\text{III})$ For each ω which appears in Base-set of $V(1; B)$, find the rule of the place of ω in $\boldsymbol{H}(B)$.

The following two Examples may explain the meaning of $(CR\text{III})$.

Example A. Let $B = 167$, whose (SC)is $K = 5$. Base-set of $V(1, 167)$ is $< 3, 7, 11, 19, 31 >$. And $\boldsymbol{H}(167)$ is $167,\ 168 = 8 \cdot 3 \cdot 7,\ 171 = 3^2 \cdot 19,\ 176 = 16 \cdot 11,\ 183 = 6 \cdot 31$, etc.

Example B. Let $B = 101$, whose (SC) is (3;4). Base set of $V(1; 101)$ is
$< 5, 13, 17 \mid 3, 7, 11, 163 >$. And $\boldsymbol{H}(101)$ is $101,\ 102 = 2 \cdot 3 \cdot 17,\ 105 = 3 \cdot 5 \cdot 7,\ 110 = 2 \cdot 5 \cdot 11,$
$117 = 3^2 \cdot 13,\ 126 = 2 \cdot 3^2 \cdot 7,\ 137,\ 150 = 2 \cdot 3 \cdot 5^2,\ 182 = 2 \cdot 7 \cdot 13,\ 201 = 3 \cdot 67,\ 222 = 2 \cdot 3 \cdot 37,$
$245 = 5 \cdot 7^2,\ 270 = 2 \cdot 3^3 \cdot 5,\ 297 = 3^3 \cdot 11,\ 326 = 2 \cdot 163$, etc.

E-mail address: rmorikawa@muj.biglobe.ne.jp