Presented at the DLSU Research Congress 2017
De La Salle University, Manila, Philippines
June 20 to 22, 2017

On Wordlength in the Discrete and Finite Heisenberg Groups

Melvin A. Vidar[1*], Rodman F. Manalang[2]
[1] *De La Salle University*
[2] *University of the East*
**Corresponding Author: melvin.vidar@dlsu.edu.ph*

Abstract: The discrete Heisenberg group, $H(\mathbb{Z})$, is the set of all 3×3 upper triangular matrices whose diagonal entries are all 1 and whose entries above the diagonal are integers, under matrix multiplication while the finite Heisenberg group, H_p (p is prime), is the set of all 3×3 upper triangular matrices with $1's$ in the diagonal and with entries above the diagonal coming from $\mathbb{Z}_p$, under matrix multiplication $mod\ p$. It is known that $H(\mathbb{Z})$ and H_p have the standard generating set

$$S = \left\{ X = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, Y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right\}.$$

Thus for any element $g \in H(\mathbb{Z})$ (respectively H_p),

$$g = m_1^{\pm 1} m_2^{\pm 1} \dots m_k^{\pm 1}, m_i \in S.$$

In this paper, we define the wordlength of an element with respect to the standard generators. Then we use the properties and algebraic structures of the Heisenberg group to determine the wordlength of an element. The wordlength function, in turn, leads to some conjectures about further algebraic structures on the finite Heisenberg group. The findings are as follows: (1) The wordlength of an element g and its inverse g^{-1} are equal; (2) The wordlength of an element of the center of $H(\mathbb{Z})$ (respectively H_p) is even; (3) In H_p, if $g = (a, b; c) \in H_p$, where $0 \le a, b \le \left\lfloor \frac{p}{2} \right\rfloor$ *and* $0 \le c \le ab$, then $l(g) = a + b$; (4) It is conjectured that H_p can be partitioned into cosets with respect to a normal subgroup $G_0 = (a, a; c)$, and that G_0 , can be expressed as a direct product of cyclic subgroups; (5) It is conjectured that H_p can be partitioned into cosets with respect a normal subgroup $G_0' = (a', -a'; c)$ and $l((a', -a'; c))$ is even.

Key Words: Discrete Heisenberg group; finite Heisenberg group; wordlength

1. INTRODUCTION

The discrete Heisenberg group $H(\mathbb{Z})$ is the set of matrices

$$\left\{\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle| a, b, c \in \mathbb{Z}\right\} \quad (1)$$

under matrix multiplication.

Let p be prime. The finite Heisenberg group H_p is the set

$$\left\{\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle| a, b, c \in \mathbb{Z}_p\right\} \quad (2)$$

under matrix multiplication ($mod\ p$).

If $A = \begin{pmatrix} 1 & a_1 & c_1 \\ 0 & 1 & b_1 \\ 0 & 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & a_2 & c_2 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix}$,

where $a_1, a_2, b_1, b_2, c_1, c_2 \in Z$ (respectively Z_p), then

$$AB = \begin{pmatrix} 1 & a_1 + a_2 & c_1 + c_2 + a_1 b_2 \\ 0 & 1 & b_1 + b_2 \\ 0 & 0 & 1 \end{pmatrix}. \quad (3)$$

From this, one finds

$$e = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } A^{-1} = \begin{pmatrix} 1 & -a_1 & -c_1 + a_1 b_1 \\ 0 & 1 & -b_1 \\ 0 & 0 & 1 \end{pmatrix}$$

respectively.

Observe that multiplication of two matrices in (3) only modifies the entries above the diagonal. Hence, we have these alternative definitions.

Definition 1. The Heisenberg group $H(\mathbb{Z})$ is the set of triples $\{(a,b;c) | a,b,c \in Z\}$ under the group law

$$(a_1, b_1; c_1)(a_2, b_2; c_2) = (a_1 + a_2, b_1 + b_2; c_1 + c_2 + a_1 b_2)$$

Definition 2. Let Let p be prime. The Heisenberg group H_p is the set of triples

$\{(a,b;c) | a,b,c \in Z_p\}$ under the group law

$$(a_1, b_1; c_1)(a_2, b_2; c_2) = (a_1 + a_2, b_1 + b_2; c_1 + c_2 + a_1 b_2)$$

where addition and multiplication are done $mod\ p$.

It is known that $H(Z)$ and H_p have the following generators [1], [2], [4], [5]:

$$X = (1,0;0), Y = (0,1;0) \text{ and } Z = (0,0;1) \quad (4)$$

such that

$$XZ = ZX,\ YZ = ZY \text{ and } XY = YXZ \quad (5)$$

Moreover, if $g = (a, b; c)$ then

$$g = Y^b X^a Z^c \quad (6)$$

2. THE CENTER OF $H(Z)$ AND H_p

It is known that the center of $H(Z)$ and H_p is the subgroup $< Z >$, where Z = (0,0;1) [3], [6]. The following identities hold about the elements of $< Z >$.

Lemma 3. With reference to the elements X, Y, Z in (4) the following expressions are all equal to Z:

i. $XYX^{-1}Y^{-1}$

ii. $X^{-1}Y^{-1}XY$
iii. $YX^{-1}Y^{-1}X$
iv. $Y^{-1}XYX^{-1}$

Proof: (i) and (ii) Use (5).
(iii) Eliminate Z on the right side of the identity $XZ = ZX$ using (i) above, then pre-multiply the resulting equation by X^{-1}.
(iv) From (5) we have

$$XY = YXZ.$$

Pre-multiplying the above equation by Y^{-1} and post-multiplying by X^{-1}, we obtain the desired result. □

Lemma 4. Let k be a positive integer. The following expressions are all equal to Z^k.

i. $XY^kX^{-1}Y^{-k}$
ii. $X^{-1}Y^{-k}XY^k$
iii. $X^kYX^{-k}Y^{-1}$
iv. $X^{-k}Y^{-1}X^kY$
v. $YX^{-k}Y^{-1}X^k$
vi. $Y^{-1}X^kYX^{-k}$
vii. $Y^kX^{-1}Y^{-k}X$
viii. $Y^{-k}XY^kX^{-1}$

Proof: Use *Lemma 3* and (5) to do an induction on k. □

Lemma 5. Let s, t be positive integers. The following expressions are all equal to Z^{st}.

i. $Y^tX^{-s}Y^{-t}X^s$
ii. $Y^{-t}X^sY^tX^{-s}$
iii. $Y^sX^{-t}Y^{-s}X^t$
iv. $Y^{-s}X^tY^sX^{-t}$
v. $X^{-s}Y^{-t}X^sY^t$
vi. $X^sY^tX^{-s}Y^{-t}$
vii. $X^{-t}Y^{-s}X^tY^s$
viii. $X^tY^sX^{-t}Y^{-s}$

Proof: Eliminate X and Y in the expressions above using $X^sY^t = Y^tX^sZ^{st}$ or $X^{-s}Y^{-t} = Y^{-t}X^{-s}Z^{st}$ and (5). □

3. WORDLENGTH IN $H(Z)$ AND H_p

Definition 6. Let G be a group and let M be a non-empty subset of G. Then M is a generating set for G if $\forall g \in G$,

$$g = m_1^{\pm 1} m_2^{\pm 1} \dots m_k^{\pm 1},$$

where $m_i \in M, 1 \le i \le k$.

If there exists a generating set M for G such that $|M| < \infty$, then G is said to be *finitely generated.*

Let M be a generating set for G. By the *word,* w in M, we mean a finite sequence of symbols of the form

$m_1^{\pm 1} m_2^{\pm 1} \dots m_k^{\pm 1}$, where $m_i \in M$ $(1 \le i \le k)$ and $k \ge 0$. If $k = 0$, w is called the *empty word,* and $w = e$, where e is the identity element in G. Let w be a word in M. Then the *wordlength* of w, denoted by $l(w)$ in M is the non-negative integer $l := l(w)$ defined by

$$l = \min\{k \mid w = m_1^{\pm 1} m_2^{\pm 1} \dots m_k^{\pm 1}\},$$

where $m_i \in M$ $(1 \le i \le k)$. A word w in M is called *reduced* if it contains no pair of consecutive symbols of the form mm^{-1} or

$m^{-1}m, \{m \in M\}$. By convention, the empty word is reduced.

Example 7. By (1) – (3), $M_1 = \{X, Y, Z\}$ is a generating set for $\boldsymbol{H}(\mathbb{Z})$ and H_p. Moreover, by *Lemma 3*, $M_2 = \{X, Y\}$ is also a generating set for $H(Z)$ and H_p. Observe also that all the expressions for Z in Lemma 3 are reduced words. Apparently, the wordlength of Z in M_2 is 4.

From now on, we fix $M = \{X, Y\}$, where X, Y are the triples in (1). By the wordlength of $g \in H_p$ or $\boldsymbol{H}(\mathbb{Z})$, we mean the wordlength of g in M and we will denote it by $l(g)$. We call M the *standard generating set* and X and Y, the *standard generators* for $H(Z)$ and H_p,

Theorem 8. Let $g \in \boldsymbol{H}(\mathbb{Z})$ or H_p. If $l(g) = k$, then $l(g^{-1}) = k$.

Proof. Suppose $l(g) = k$. Then there exists $m_1, m_2, \ldots, m_k \in M$ such that

$$g = m_1^{\pm 1} m_2^{\pm 1} \ldots m_{k-1}^{\pm 1} m_k^{\pm 1} \quad (7)$$

is a reduced word. Now,

$$g^{-1} = \left(m_1^{\pm 1} m_2^{\pm 1} \ldots m_k^{\pm 1}\right)^{-1} = m_k^{\mp 1} \ldots m_2^{\mp 1} m_1^{\mp 1} \quad (8)$$

Observe that g^{-1} is a reduced word. Otherwise, if there exists a pair of consecutive symbols say $m_i m_i^{-1}$ or $m_i^{-1} m_i$ in (8), the pair of consecutive symbols $m_i m_i^{-1}$ or $m_i^{-1} m_i$ also exists in (7), a contradiction. □

Theorem 9. Let $g = (0,0;c) \in H_p$, where $0 < c \leq \lfloor \frac{p}{2} \rfloor$.

i. If c is composite, then $l(g) = 2(a+b)$, where $c = ab$ and $a + b$ is a minimum.
ii. If c is prime,
$$l(g) = \min \begin{cases} 2(c+1) \\ 2(a' + b') \end{cases}$$
where $p - c = c' = a'b'$ and $a' + b'$ is a minimum.

Proof: Immediate from Lemma 4 and Lemma 5. □

Theorem 10. Let $g = (a, b; c) \in H_p$ *and* $0 \leq a, b \leq \lfloor \frac{p}{2} \rfloor$. If $0 \leq c \leq ab$, then $l(g) = a + b$.

Proof: First, observe that

$$l(a, b; ab) = l(Y^b X^a Z^{ab}) = l(X^a Y^b) = a + b.$$

Next, if $0 \leq c \leq ab$, we start with $X^a Y^b$ for $c = ab$, then switch some powers of X with some powers of Y to obtain $l(a, b; c)$ as follows:

$$\begin{aligned} l(a, b; ab) &= l(X^a Y^b) = a + b \\ l(a, b; ab - 1) &= l(X^{a-1} Y X Y^{b-1}) = a + b \\ l(a, b; ab - 2) &= l(X^{a-2} Y X^2 Y^{b-1}) = a + b \\ &\vdots \\ l(a, b; ab - a) &= l(X^{a-a} Y X^a Y^{b-1}) = l(Y X^a Y^{b-1}) = a + b \end{aligned}$$

In general, if $c = ab - (ka + l)$ where $0 \leq k \leq b - 1, 0 \leq l \leq a$ then

$$\begin{aligned} (a, b; c) &= \left(a, b; ab - (ka + l)\right) \\ &= Y^k X^{a-l} Y X^l Y^{b-k-1} \end{aligned}.$$

The result follows. □

Corollary 11. Let $g = (a, b; c) \in H_p$ such that $0 \le a, b \le \lfloor \frac{p}{2} \rfloor$ and $ab \ge p - 1$. Then $l(g) = a + b$ for all $c \in \mathbb{Z}_p$. □

4. NORMAL SUBGROUPS, COSETS AND WORDLENGTH IN H_p

Further investigation into the wordlength of elements of H_p reveals the following algebraic structures of H_p.

Theorem 12. Fix an element $h = (a,b; c) \in Hp \setminus <Z>$. For $0 \le i \le p-1$, define $G_i = \{g \in H_p \mid ghg^{-1} = hZ^i\}$. Then the following hold:

(i) G_0 is a normal subgroup of Hp.

(ii) $\{G_i\}_{i=0}^{p-1} = H_p / G_0$.

Proof. (i) Let $g_1, g_2 \in G_0$. Then

$$g_1 h g_1^{-1} = h \text{ and } g_2 h g_2^{-1} = h. \qquad (9)$$

Using (9), we find

$(g_1 g_2) h (g_1 g_2)^{-1} = g_1 (g_2 h g_2^{-1}) g_1^{-1} = g_1 h g_1^{-1} = h,$ so $g_1 g_2 \in G_0$. Moreover, from (8), we also find $g_1^{-1} h (g_1^{-1})^{-1} = h$, so $g_1^{-1} \in G_0$. Thus, $G_0 \le H_p$. We next show that $G_0 \lhd H_p$. Observe that $<Z> \subseteq G_0$ since $Z^k h Z^{-k} = h$. Now suppose $g_0 = (a_0, b_0; c_0) \in G_0 \setminus <Z>$. Then

$$g_0 h g_0^{-1} = h \Rightarrow ab_0 = a_0 b \pmod p \quad (10)$$

Thus, either

$$g_0 = (a_0, a^{-1} a_0 b; c_0) \text{ if } a \ne 0 \qquad (11)$$

or $g_0 = (b^{-1} a b_0, b_0; c_0)$ if $b \ne 0$. (12)

Now, if $a \ne 0$, we use (11) to evaluate $g^* g_0 (g^*)^{-1} = (a_0, a^{-1} a_0 b; c_0 - a_0 b^* + a^* a^{-1} a_0 b)$ where $g^* = (a^*, b^*; c^*)$. Similarly, if $b \ne 0$, $g^* g_0 (g^*)^{-1} = (b^{-1} a b_0, b_0; c_0 + a^* b_0 - b^* b^{-1} a b_0)$ by (12). In either case, $g^* g_0 (g^*)^{-1} \in G_0$. Combining the above results, we have now shown that $G_0 \lhd H_p$.

(ii) Let $g^* = (a^*, b^*; c^*) \in H_p, g_0 \in G_0$. Then

$$\begin{aligned}(g^* g_0) h (g^* g_0)^{-1} &= g^* (g_0 h g_0^{-1}) (g^*)^{-1} \\ &= g^* h (g^*)^{-1} \\ &= hZ^i\end{aligned}$$

for some $i \in Z_p$ (since conjugation only twists the third coordinate of h as shown in the proof of (i) above). Thus, $g^* g_0 \in G_i$ for some $i \in Z_p$, and $g^* G_0 \subseteq G_i$. To show the reverse inclusion, fix an integer $i \in Zp$, and set $g^* = g_i g_0^{-1} \in H_p$. Then

$$g_i = (g_i g_0^{-1}) g_0 = g^* g_0.$$

That is s, $g_i \in g^* G_0$ for some $g^* \in H_p$, hence $G_i \subseteq H_p / G_0$. The result follows. □

We finish this section with the following conjectures.

Conjecture 13. With reference to the normal subgroup G_0 in Theorem 12, the following hold:

(i) If $a \ne 0$ then $G_0 = N_1 \times N_2 \times \ldots \times N_{p+1}$ (direct product)

where $N_1 =< (0, 0; 1) >$
$N_2 =< (1, a^{-1}b; 0) >$
$N_3 =< (2, 2a^{-1}b; 0) >$
$\vdots$
$N_p =< (p-1, (p-1)a^{-1}b; 0) >$
$N_{p+1} =< (1, a^{-1}b\,; -\left\lfloor \frac{p}{2} \right\rfloor a^{-1}b) >.$

(ii) If $b \neq 0$ *then* $G_0 = N_1 \times N_2 \times \dots \times N_{p+1}$ *(direct product)*
where $N_1 =< (0, 0; 1) >$
$N_2 =< (b^{-1}a, 1; 0) >$
$N_3 =< (2b^{-1}a, 2; 0) >$
$\vdots$
$N_p =< ((p-1)b^{-1}a, (p-1); 0) >$
$N_{p+1} =< (b^{-1}a, 1\,; -\left\lfloor \frac{p}{2} \right\rfloor b^{-1}a) >.$ □

Conjecture 14. The set $G_0' = \{(a, -a; c) | a, c \in \mathbb{Z}_p\}$ is a normal subgroup of H_p. Moreover, the wordlength of each element of G_0' is even. □

5. CONCLUSION

This paper investigated some algebraic structures of the discrete and finite Heisenberg groups. Explicit expressions were formulated regarding the expansion of some elements of the above groups in terms of the standard generators. A combinatorial algorithm is also presented in expanding an element $g = (a, b; c)$ of H_p when $0 \leq a, b \leq \left\lfloor \frac{p}{2} \right\rfloor$ and $0 \leq c \leq ab$. These initial results indicate that the algebraic structures of the abovementioned groups are related to the wordlength of an element with respect to the standard generators. On the other hand, investigations into the wordlength of elements of H_p resulted to some conjectures on further algebraic structures of H_p.

6. REFERENCES

[1] S. Blachere, "Word Distance on the Discrete Heisenberg Group", vol. 95, *Colloquium Mathematicum*, 2003, pp. 21-36

[2] V.V. Kochmani, P.L. Lilly and K.T. Joju. "Hashing with discrete heisenberg group and graph with large girth." *Journal of Theoretical Physics & Cryptography*. **11**(2016):1-4.

[3] P. J. Kahn." Automorphisms of the discrete Heisenberg groups", preprint, 2005, pp. 1-7, available at https://www.math.cornell.edu/m/sites/default/files/imported/People/Faculty/Heisen.pdf

[4] D.V. Osipov. "Discrete Heisenberg groups and its automorphism group. *Mat. Zametski*, **98**:1(2015), 152-155; *Math Notes*, **98**:1(2015), 185-188.

[5] J. Pate. "Geometric Aspects of the Heisenberg group." Preprint, 2006, pp.1-17, available at http://math.arizona.edu/~ura-reports/061/Pate.John/Final.pdf.

[6] J. Schulte. "Harmonic analysis on finite Heisenberg groups." *European Journal of Combinatorics:* **25**(2004)327-338.