Discrete Mathematics and Theoretical Computer Science **4**, 2001, 91–100

A note on representations of the finite Heisenberg group and sums of greatest common divisors

Johannes Grassberger[1] and Günther Hörmann[2†]

[1]*The Abdus Salam International Centre for Theoretical Physics, Trieste, Italy,* `johannes@ictp.ts.it`
[2]*Institut für Mathematik, Universität Wien, Austria,* `guenther.hoermann@univie.ac.at`

received Nov 3, 2000, *revised March 15, 2001*, *accepted March 20, 2001*.

We review an elementary approach to the construction of all irreducible representations of the finite Heisenberg group. Determining the number of inequivalent classes of irreducible representations by different methods leads to an identity of sums involving greatest common divisors. We show how this identity can be generalized and derive an explicit formula for the sums.

Keywords: Heisenberg group, representation of finite groups, sums of gcds

---

1 Introduction

In the framework of algebraic quantum mechanics Heisenberg's uncertainty relation is usually stated in the form of a commutation relation for self-adjoint unbounded operators which represent the observables position Q and momentum P (I denoting the identity element):

$$[Q,P] := QP - PQ = iI. \tag{1}$$

Equation (1) can be obtained formally by application of $\frac{d^2}{dtds}|_{(s,t)=(0,0)}$ to the following equation involving unitary one-parameter groups

$$\exp(itP)\exp(isQ) = \exp(ist)\exp(isQ)\exp(itP)\,. \tag{2}$$

Introducing the notation $X_t := \exp(itP), Y_s := \exp(isQ), Z_r := \exp(ir)I$ we can bring this into the form

$$X_t Y_s = Z_{st} Y_s X_t\,.$$

Furthermore, we have the one-parameter group property $X_{t_1+t_2} = X_{t_1} X_{t_2}$ (and similarly for Y and Z) and that Z commutes with X and Y. We observe that these relations still make sense when the parameters are elements of an arbitrary commutative ring.

[†]currently visiting the Dept. of Mathematical and Computer Sciences, Colorado School of Mines, USA

Definition 1 *Let $\mathcal{R}$ be a commutative ring. The* Heisenberg group $H(\mathcal{R})$ *is generated by objects X_r, Y_s, Z_t with parameters $r,s,t \in \mathcal{R}$ subject to the relations*

$$
\begin{aligned}
&T_{t_1} T_{t_2} = T_{t_1+t_2} \;, \quad Z_t T_s = T_s Z_t && \text{for } T = X,Y,Z \\
&X_t Y_s = Y_s X_t Z_{st} && \forall \text{ parameters in } \mathcal{R} \;.
\end{aligned}
$$

It is convenient to use an isomorphic realization via $X_r Y_s Z_t \mapsto (r,s,t)$ and the following basic consequences of the defining relations (the identity element is $(0,0,0)$)

$$
\begin{aligned}
(r,s,t)^{-1} &= (-r,-s,-t-rs) \\
(r,s,t)\cdot(r',s',t') &= (r+r', s+s', t+t'-sr') \;. \qquad (3)
\end{aligned}
$$

In this paper we study the case where $\mathcal{R} = \mathbb{Z}_n$ the finite ring of remainder classes modulo n. So $H(\mathbb{Z}_n)$ is a finite group of order n^3 which is generated by the two elements $X := X_1$ and $Y := Y_1$:

$$
X_k = X^k, Z_k = X^k Y X^{-k} Y^{-1} \quad \text{and so on} \ldots
$$

Simple computations show that the center $\mathcal{Z}(H(\mathbb{Z}_n))$ is the cyclic subgroup of order n generated by $Z := Z_1$ and that the subgroup N generated by X and Z is a commutative normal divisor in $H(\mathbb{Z}_n)$.

In section 2 we study *linear representations* of $H(\mathbb{Z}_n)$, i.e., the ways its elements can act as (invertible) operators on complex vector spaces. We determine the classes of *irreducible representations* (i.e., those having no non-trivial invariant subspace) by elementary methods. In particular, the number of equivalence classes of irregular representations is derived in two independent ways thereby deriving an identity for sums of multiple common divisors. In section 3 we give simple and direct proofs of the general identity and derive an explicit formula. Finally, we show how an application of a classical result by Cesaro on summatory functions (cf. [Ces]) provides us with still a different interpretation for certain special cases of the identity.

It is understood that in itself the derivation of the irreducible representations of the Heisenberg group is of course not a new result. For example, good sources for this in the context of harmonic analysis are [Sche, Ter, Schu]. In fact, for this part we merely give an explicit solution to the exercise stated in [Ter], p. 297. However we considered it worth while to expose here an elementary derivation in comparing it with a discrete version of Kirillov's orbit theory — originally developed for nilpotent Lie Groups — and, in particular, to explore its link with Cesaro sums.

2 Representations of $H(\mathbb{Z}_n)$

Let $\rho : H(\mathbb{Z}_n) \to \mathrm{GL}(V)$ be a group homomorphism, i.e. a representation of $H(\mathbb{Z}_n)$ over the complex vector space V. Since $H(\mathbb{Z}_n)$ is finite we may assume that V is finite dimensional. Then $\rho|_N \colon N \to \mathrm{GL}(V)$ defines a representation of the commutative group N. Therefore $\rho(N) \subseteq \mathrm{GL}(V)$ is a set of pairwise commuting operators. Therefore we can find a basis $\mathcal{E} = \{v_1, \ldots, v_{\dim V}\}$ of V consisting of joint eigenvectors.

The complete information about $\rho|_N$ is given by the actions of X and Z:

$$
X \cdot v_j = \lambda_j v_j \qquad Z \cdot v_j = \mu_j v_j \qquad j = 1, \ldots, \dim V \;.
$$

We can always assume the group elements to act as unitary operators (take the invariant mean of an arbitrary Hermitian form; see [Ser], remark in 1.3). Therefore we may assume $|\lambda_j| = |\mu_j| = 1$. Furthermore, since both X^n and Z^n are equal to the neutral element in $H(\mathbb{Z}_n)$ we have $\lambda_j^n = \mu_j^n = 1$.

We pick an arbitrary vector v in $\mathcal{E}$ — we drop the eigenvector index j for the moment since it will be fixed during the following construction. Then with $\omega = e^{2\pi i/n} \in \mathbb{C}$ we have

$$Xv = \omega^x v \quad \text{and} \quad Zv = \omega^z v \quad \text{for some } x,z \in \{0,\dots,n-1\}. \tag{4}$$

The subspace $W \subseteq V$ defined as the linear hull of $\{v, Yv, \dots, Y^{n-1}v\}$ is $H(\mathbb{Z}_n)$–invariant and therefore defines a subrepresentation ρ_W of ρ.

The vectors $Y^k v$ are eigenvectors for X with eigenvalues ω^{x+kz}:

$$X(Y^k v) = (XY^k)v = (Y^k X Z^k)v = Y^k(\omega^{x+kz}v) = \omega^{x+kz}Y^k v. \tag{5}$$

Theorem 2 ρ_W *defines an irreducible representation of dimension* $n/\gcd(z,n)$.

Proof: let $d = \gcd(z,n)$; we observe that X and $Y^{n/d}$ commute as operators on W since

$$XY^{\frac{n}{d}}(Y^k v) = Y^{\frac{n}{d}}XZ^{\frac{n}{d}}Y^k v = \underbrace{\omega^{\frac{zn}{d}}}_{=1} Y^{\frac{n}{d}}X(Y^k v) = Y^{\frac{n}{d}}X(Y^k v)$$

for arbitrary k. Therefore eigenvectors in W are joint eigenvectors of X and $Y^{n/d}$ and in particular

$$Y^{\frac{n}{d}}v = \omega^y v \qquad \text{with} \qquad \omega^{yd} = \omega^{ny} = 1\ .$$

Hence $\frac{n}{d} \mid y$ and among $\{v, Yv, \dots, Y^{n-1}v\}$ there are at most n/d linearly independent eigenvectors. Since the vectors $v, Yv, \dots, Y^{\frac{n}{d}-1}v$ are eigenvectors of X corresponding to distinct eigenvalues they are linearly independent and hence $\dim W = n/d$.

We can describe an explicit matrix representation with respect to the basis $\mathcal{B} = \{v, Yv, \dots, Y^{\frac{n}{d}-1}v\}$: the matrix $[Z]_{\mathcal{B}}$ corresponding to the operator Z is simply $\omega^z \,\mathrm{Id}_W$; the matrices corresponding to X and Y are immediately seen to be given by

$$[X]_{\mathcal{B}} = \omega^x \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \omega^z & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \omega^{(\frac{n}{d}-1)z} \end{pmatrix} \qquad [Y]_{\mathcal{B}} = \begin{pmatrix} 0 & 0 & \dots & 0 & \omega^y \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix} \tag{6}$$

With this explicit form of the representation at hand we can easily determine the corresponding *character* $\chi\colon H(\mathbb{Z}_n) \mapsto \mathbb{C}$ of the representation. By definition (cf. [Ser],2.1) χ is given by

$$\chi(r,s,t) = \mathrm{Tr}(X^r Y^s Z^t)\ .$$

To calculate the value of the trace we only have to consider the diagonal of the matrix product $X^r Y^s Z^t$. Since X and Z are diagonal we mainly have to focus on Y^s: apart from the factor ω^y in the last column Y is a cyclic right shift of the base vectors; successive products of this matrix produce a downward cyclic shift of the rows where each row reentering from the top introduces an additional factor ω^y; in particular, after n/d steps we obtain $\omega^y \,\mathrm{Id}_W$; for $s > 0$ arbitrary the nonzero entries of the matrix $[Y^s]_{\mathcal{B}}$ are organized as follows

$$\omega^{\hat{s}y}\begin{pmatrix} & \bar{s}\text{ rows}\left\{\begin{matrix}\omega^y & & \\ & \ddots & \\ & & \omega^y\end{matrix}\right. \\ \left.\begin{matrix}1 & & \\ & \ddots & \\ & & 1\end{matrix}\right\}\tfrac{n}{d}-\bar{s}\text{ rows} & \end{pmatrix} \quad \text{where} \quad s = \hat{s}\frac{n}{d} + \bar{s} \quad \text{with} \quad 0 < \bar{s} < \frac{n}{d}\ .$$

For the determination of $X^r Y^s$ we only have to use the simple fact that multiplication with a diagonal matrix from the left scales the columns by the corresponding diagonal entries. Hence we have

$$\omega^{rx}\omega^{\hat{s}y}\begin{pmatrix} & \bar{s}\text{ rows}\left\{\begin{matrix}\omega^{(\frac{n}{d}-\bar{s})rz+y} & & \\ & \ddots & \\ & & \omega^{(\frac{n}{d}-1)rz+y}\end{matrix}\right. \\ \left.\begin{matrix}1 & & \\ & \ddots & \\ & & \omega^{(\frac{n}{d}-\bar{s}-1)rz}\end{matrix}\right\}\tfrac{n}{d}-\bar{s}\text{ rows} & \end{pmatrix}$$

Therefore we see that the trace can be nonzero only if $\bar{s} = 0$, i.e., $\frac{n}{d} \mid s$. In this case we set $\omega^{\hat{s}y} = \omega^{s\hat{y}}$ where $\hat{y} = y/(n/d)$ and simply have to evaluate the following geometric progression:

$$\chi(r,s,t) = \omega^{tz+rx+s\hat{y}} \sum_{l=0}^{n/d-1} \omega^{lrz}\ .$$

If we observe that $n \mid rz$ is equivalent to $\frac{n}{d} \mid r$ or $z = 0$ and that the factor ω^{rx} depends only on $\bar{x} = x \pmod p$ when $\frac{n}{d} \mid r$ the trace is found to be

$$\chi(r,s,t) = \begin{cases} 0 & \frac{n}{d} \nmid s \vee (\frac{n}{d} \nmid r \wedge z \neq 0) \\ \frac{n}{d}\omega^{tz+r\bar{x}+s\hat{y}} & \text{otherwise} \end{cases}\ .$$

Using the Iverson symbol (cf. [GKP], 2.1) as a "generalized Kronecker delta" ($[P] = 1$ if property P holds and 0 otherwise) and noting that $z = 0$ implies $d = n$ we may rewrite this in the more compact form

$$\chi(r,s,t) = \begin{cases} \omega^{rx+sy} & \text{if } z = 0 \\ \left[\frac{n}{d} \mid r\right] \left[\frac{n}{d} \mid s\right]\ \frac{n}{d}\,\omega^{r\bar{x}+s\hat{y}+tz} & \text{if } z \neq 0 \end{cases}\ . \tag{7}$$

Now we are in a position to apply the standard criterion for irreducibility in terms of the character ([Ser], 2.3). The (weighted) l^2–norm of χ is

$$||\chi||^2 = \frac{1}{n^3}\left\{\begin{matrix} \sum_{r,s,t} 1 & \text{if } z = 0 \\ \sum_{t,\frac{n}{d}|s,\frac{n}{d}|r} \frac{n^2}{d^2} & \text{if } z \neq 0 \end{matrix}\right\} = 1\ .$$

This implies that the corresponding representation is indeed irreducible. □

Equation (7) shows that the irreducible representations are completely described by the choices of $z \in \mathbb{Z}_n$, $\bar{x} \in \mathbb{Z}_d$, and $\hat{y} \in \mathbb{Z}_n / \frac{n}{d}\mathbb{Z} \cong \mathbb{Z}_d$. Hence after changing notation we may denote the corresponding characters by $\chi^{x,y,z}$ with parameters $(x,y,z) \in \mathbb{Z}_d \times \mathbb{Z}_d \times \mathbb{Z}_n$. The orthogonality relations for irreducible characters enable us to determine the number of inequivalent irreducible representations.

Corollary 3 *The characters satisfy the orthogonality relations*

$$\langle \chi^{x,y,z} | \chi^{x',y',z'} \rangle \;=\; \left[x = x'\right]\left[y = y'\right]\left[z = z'\right] \tag{8}$$

where $d = \gcd(z,n)$ *(*$= \gcd(z',n)$ *in the nonzero cases) Consequently, the number* $\nu(n)$ *of distinct (classes of) irreducible (unitary) representations of* $H(\mathbb{Z}_n)$ *is given by*

$$\nu(n) = \sum_{z \in \mathbb{Z}_n} \gcd(z,n)^2 \,. \tag{9}$$

Proof: A straightforward insertion of the character formula shows that the corresponding sum over three indices splits into three factors of sums over one index only; each such sum vanishes unless each summand in it equals 1 (which produces also the correct factors to cancel the weight factor given by the group order). □

2.1 Alternative methods from representation theory

Counting conjugacy classes: One of the main theorems in representation theory of finite groups states that the number of (equivalence classes of) irreducible representations of a group G is equal to the number of disjoint *conjugacy classes*

$$C_g := \{hgh^{-1} \mid h \in G\} \,.$$

Denote by c_g the cardinality of the class C_g.

A short calculation using the basic relations 3 for the "triple realization" of $H(\mathbb{Z}_n)$ yields the formula

$$C_{(a,b,c)} = \{(a,b,c+bx-ay) \mid x,y \in \mathbb{Z}_n\} \,.$$

Thus, two elements (a,b,c) and (a',b',c') belong to the same conjugacy class iff $a = a'$, $b = b'$ and there exist whole numbers x, y and z such that $c = c' - ay + bx + nz$. This equation is solvable iff $c \equiv c' \pmod{\gcd(a,b,n)}$. Therefore every conjugacy class contains exactly one element of the set

$$L := \{(a,b,c) \in \{0,\ldots,n-1\}^3 \mid c < \gcd(a,b,n)\} \tag{10}$$

and we obtain for the number of irreducible representations

$$\sum_{a=0}^{n-1}\sum_{b=0}^{n-1} \gcd(a,b,n) \,. \tag{11}$$

Corollary 4 *For any natural number* n

$$\nu(n) = \sum_{z \in \mathbb{Z}_n} \gcd(z,n)^2 = \sum_{a=0}^{n-1}\sum_{b=0}^{n-1} \gcd(a,b,n) \,. \tag{12}$$

A miniature of Kirillov's orbit theory: The Heisenberg group is one of the first main examples to which Kirillov applied his *method of orbits* in representation theory of Lie groups (cf. [Kir62]). In this subsection we apply the algebraic machinery of the geometric theory to the finite case.

We give a short sketch of the constructions from differential geometry. If G is a Lie group it acts (differentiable) on itself by conjugation, i.e. we have a map $\phi : G \to \mathrm{Aut}(G)$, $\phi_{(g)}(h) = ghg^{-1}$. So the derivative of $\phi_{(g)}$ at the identity element e is an invertible linear operator on the Lie algebra $\mathfrak{g}$. Moreover, by the chain rule the map $\rho : G \to \mathrm{GL}(\mathfrak{g})$, $g \mapsto d\phi_{(g)}|_e$ is shown to be a (linear) representation, the so-called *adjoint representation*. The corresponding dual representation $\rho : G \to \mathrm{GL}(\mathfrak{g}^*)$, defined by $\langle \rho_{(g)} f, x\rangle := \langle f, \rho_{(g)}^{-1} x\rangle$ for $x \in \mathfrak{g}$ and $f \in \mathfrak{g}^*$, is rich of geometric structure. It is called the *co-adjoint representation* of G.

Kirillov proved in 1962 that for large classes of Lie groups one can obtain all (equivalence classes of) irreducible representations by further constructions on the orbits of the co-adjoint representation in $\mathfrak{g}^*$. In particular, the equivalence classes are in one-to-one correspondence with the disjoint orbits. For details and further references see [Kir62], [Kir76].

We now mimic Kirillov's constructions for our example $H(\mathbb{Z}_n)$. In analogy to the continuous case we model the "Lie algebra" $\mathfrak{h}$ as $\mathbb{Z}_n^3$ with component-wise addition and "scalar multiplication" with elements of $\mathbb{Z}_n$, i.e. as $\mathbb{Z}_n$-module. The duality $(\mathfrak{h},\mathfrak{h}^*) \cong (\mathbb{Z}_n^3,\mathbb{Z}_n^3)$ is defined by $\langle(\alpha,\beta,\gamma),(a,b,c)\rangle := \alpha a + \beta b + \gamma c$.

In this setting a short computation leads to the following formula for the "co-adjoint representation":

$$\rho^*_{(a,b,c)}(\alpha,\beta,\gamma) = (\alpha + b\gamma, \beta - a\gamma, \gamma)\,. \tag{13}$$

How many disjoint orbits does this action produce in $\mathbb{Z}_n^3$? Two points (α,β,γ) and (α',β',γ') belong to the same orbit iff

$$\begin{aligned} \gamma &= \gamma' \\ \alpha &\equiv \alpha' \pmod{\gcd(\gamma,n)} \\ \beta &\equiv \beta' \pmod{\gcd(\gamma,n)} \end{aligned}$$

Thus, to every orbit belongs exactly one point of the set

$$R := \{(\alpha,\beta,\gamma) \in \{0,\dots,n-1\}^3 \mid \alpha,\beta < \gcd(\gamma,n)\}. \tag{14}$$

Hence the number of disjoint orbits is

$$\sum_{\gamma=0}^{n-1} \gcd(\gamma,n)^2 \tag{15}$$

in accordance with the expression in (9).

3 Sums of powers of greatest common divisors

We turn our attention to more general sums of powers of greatest common divisors as they appeared above. For the sake of conciseness we introduce the following notation: $\gcd(v,n) := \gcd(v_1,\dots,v_q,n)$ where $v = (v_1,\dots,v_q)$.

We then define

$$\nu_{q,r}(n) := \sum_{v \in \mathbb{Z}_n^q} \gcd(v,n)^r \tag{16}$$

The sums $\nu(n)$ examined in the previous section are obviously represented by $\nu_{1,2}(n)$ and $\nu_{2,1}(n)$. Hence the results there imply $\nu_{1,2}(n) = \nu_{2,1}(n)$.

3.1 A generalized equation

Before establishing an explicit formula for $\nu_{q,r}(n)$, we prove a generalized symmetry property.

Proposition 5 *For all q, r, n in* $\mathbb{N}$

$$\nu_{q,r}(n) = \nu_{r,q}(n). \tag{17}$$

Remark 6 *This will also follow independently from the explicit formula given in the next subsection, but we don't want to omit the following nice proof which also gives a meaning to the value of the function for general q and r.*

Proof: We count the elements of the set

$$S := \left\{(v,w) \in \mathbb{Z}_n^q \times \mathbb{Z}_n^r \middle| n \mid \gcd(v,n)\gcd(w,n)\right\}$$

For a given v, how many w can we find with $(v,w) \in S$? For w we have the condition

$$\frac{n}{\gcd(v,n)} \,\Bigg|\, \gcd(w,n)$$

Therefore it is necessary and sufficient that all w_i are multiples of the fraction on the left. In $\mathbb{Z}_n$ there are $\gcd(v,n)$ such numbers, so we get $\gcd(v,n)^r$ combinations for w. Hence

$$|S| = \sum_{v \in \mathbb{Z}_n^q} \gcd(v,n)^r = \nu_{q,r}(n)$$

Repeating the same deduction with the roles of v and w interchanged we arrive at

$$|S| = \nu_{r,q}(n)$$

which completes the proof. $\square$

3.2 An explicit formula

Fortunately our function is multiplicative, that is:

Proposition 7

$$\nu_{q,r}(mn) = \nu_{q,r}(m)\nu_{q,r}(n) \quad \textit{when } \gcd(m,n) = 1. \tag{18}$$

Proof: This follows from the Chinese Remainder Theorem and basic properties of the gcd function: Every vector $v \in \mathbb{Z}_{mn}^q$ can be written in a unique way as $v'n + v''m$ with $v' \in \mathbb{Z}_m^q$ and $v'' \in \mathbb{Z}_n^q$. Since m and n have no divisors in common,

$$\begin{aligned}
\gcd(v'n+v''m, mn) &= \gcd(v'n+v''m, m)\gcd(v'n+v''m, n) \\
&= \gcd(v'n, m)\gcd(v''m, n) \\
&= \gcd(v', m)\gcd(v'', n)
\end{aligned}$$

Thus

$$\nu_{q,r}(mn) = \sum_{v' \in \mathbb{Z}_m^q} \sum_{v'' \in \mathbb{Z}_n^q} \gcd(v', m)^r \gcd(v'', n)^r = \nu_{q,r}(m)\nu_{q,r}(n)$$

□

By the multiplicativity of $\nu_{q,r}$ it is sufficient to find an explicit formula for $\nu_{q,r}(n)$ when n is a prime power p^k.

We observe that all gcds in the sum are divisors of p^k. Hence they are of the form p^i for some i with $0 \le i \le k$. If we define $\eta(i)$ as the number of times $\gcd(v, p^k)$ assumes the value p^i then obviously

$$\nu_{q,r}(p^k) = \sum_{i=0}^{k} \eta(i) p^{ir}. \tag{19}$$

We have $\gcd(v, p^k) = p^k$ only with v as null vector, so $\eta(k) = 1$. Now let's assume that $i < k$. There are p^{k-i} multiples of p^i and therefore $p^{(k-i)q}$ vectors v with $\gcd(v, p^k)$ *at least* p^i. From this we have to subtract the number of vectors where the gcd is *at least* p^{i+1}:

$$\eta(i) = p^{(k-i)q} - p^{(k-i-1)q} \quad \text{where } i < k$$

Inserting this into (19) yields a sum over a geometric progression (with factor 1 when $q = r$) which can be evaluated easily. Hence we arrive at the following

Theorem 8

$$\nu_{q,r}(p^k) = \begin{cases} (k+1)p^{kq} - kp^{(k-1)q} & \textit{for } q = r \\ \frac{p^{kr}(p^r-1) - p^{kq}(p^q-1)}{p^r - p^q} & \textit{for } q \neq r \end{cases}. \tag{20}$$

3.3 Applying a result of Cesaro

Cesaro (cf. [Ces]) found the following

Theorem 9

$$\sum_{v_1=1}^{n}\sum_{v_2=1}^{n}\cdots\sum_{v_q=1}^{n} F(\gcd(v_1,\dots,v_q)) = \sum_{d=1}^{n} f(d)\left\lfloor\frac{n}{d}\right\rfloor^{r} \tag{21}$$

where F is the summatory function of f.

The summatory function—a kind of number theoretic integral—is defined as sum over all divisors:

$$F(n) := \sum_{d|n} f(d)$$

Considering that $\gcd(v_1,\dots,v_q,n) = \gcd(\gcd(v_1,\dots,v_q),n)$ we can apply this result to the function $\nu_{q,1}$ by defining

$$F_n(m) := \gcd(m,n) \tag{22}$$

Then the left-hand side in (21) is identical to $\nu_{q,1}(n)$.

Now we only have to identify the corresponding function f_n. It is known that in general $f(p^k) = F(p^k) - F(p^{k-1})$. If p^k divides n then $F_n(p^k) = p^k$ and $F_n(p^{k-1}) = p^{k-1}$, hence $f_n(p^k) = p^{k-1}(p-1) = \varphi(p^k)$. On the other hand, if p^k does not divide n then $F_n(p^k) = F_n(p^{k-1})$ and therefore $f_n(p^k) = 0$. Since both F_n and φ are multiplicative, so is f_n and we have

$$f_n(m) = \begin{cases} \varphi(m) & \text{if } m|n \\ 0 & \text{otherwise} \end{cases} \tag{23}$$

This means that the summation on the right-hand side in (21) can be restricted to the divisors of n only, i.e.,

$$\nu_{q,1}(n) = \sum_{d|n} \varphi(d)\left(\frac{n}{d}\right)^{q} = \sum_{d|n} \varphi\left(\frac{n}{d}\right) d^{q} \tag{24}$$

In this form it becomes apparent that the sum evaluates to $\nu_{1,q}(n)$ since there are exactly $\varphi(n/d)$ numbers in $\mathbb{Z}_n$ which have d as greatest common divisor with n.

Acknowledgements

The authors want to thank an anonymous referee as well as J. Schulte for pointing out more recent references on the subject and for helpful remarks.

References

[Ces] CESARO, E. *Sur le plus grand diviseur de plusieurs nombres*, Ann. Mat. Pura e Appl., **13 (2)**, 291-294 (1885).

[GKP] GRAHAM, R.L., KNUTH, D.E., PATASHNIK, O. *Concrete Mathematics*, Addison-Wesley 1989.

[Kir62] KIRILLOV, A.A. *Unitary Representations of Nilpotent Lie Groups*, Russian Math. Survey **17**, 53-104 (1962).

[Kir76] KIRILLOV, A.A. *Elements of the Theory of Representations*, Springer-Verlag, Berlin Heidelberg 1976.

[Sche] SCHEMPP, W. *Group theoretical methods in approximation theory, elementary number theory and computational signal geometry*, pp. 129-171 in *Approximation Theory*, V.C.K. Chui, L.L. Schumaker, and J.D. Ward (eds.), Academic, Orlando, 1986.

[Schu] SCHULTE, J. *Zur harmonischen Analyse auf endlichen Heisenberggruppen*, Dissertation, Universität-GH Siegen, Shaker Verlag, Aachen, 2000

[Ser] SERRE, J.-P. *Linear Representations of Finite Groups*, Springer-Verlag, New York 1977.

[Ter] TERRAS, A. *Fourier Analysis on Finite Groups and Applications*, Cambridge University Press, Cambridge 1999.