Rendiconti del Circolo Matematico di Palermo 58, 99 – 108 (2009)
DOI: 10.1007/s12215-009-0010-6

Balasubramanian Sury

Some number-theoretic identities from group actions

Received: October 27, 2008 / Accepted: February 14, 2009 – © Springer-Verlag 2009

Abstract. We apply group actions to some natural situations like the natural 'linear' action of $GL_r(\mathbf{Z}_n)$ and some of its subgroups to derive number-theoretic identities like

$$\sum_{t_1 \in (\mathbf{Z}_n)^*, t_2, \cdots, t_r \in \mathbf{Z}_n} GCD(n, t_1 - 1, t_2, \cdots, t_r) = \phi(n)\sigma_{r-1}(n).$$

Keywords Not-Burnside lemma · Cauchy-Frobenius formula · Linear action of $GL_r(\mathbf{Z}_n)$ · Generalized totient function

Mathematics Subject Classification (2000) 20D60 · 11A25

1 Introduction

The title "A lemma that is not Burnside's" was the fancy name of a paper by Peter Neumann [2] who revealed that this lemma was already used by Cauchy and Frobenius. He proposed the name Cauchy-Frobenius lemma but ironically, the name "not-Burnside lemma" seems to have stuck. We shall apply this lemma to the natural 'linear' action of $GL_r(\mathbf{Z}_n)$ and some of its subgroups and derive number-theoretic identities. For instance, applying the lemma to the action of a certain group of upper triangular matrices, we obtain the identity:

For any natural number n,

$$\sum_{t_1 \in (\mathbf{Z}_n)^*, t_2, \cdots, t_r \in \mathbf{Z}_n} GCD(n, t_1 - 1, t_2, \cdots, t_r) = \phi(n)\sigma_{r-1}(n).$$

B. Sury (Corresponding author)
Statistics and Mathematics Unit, Indian Statistical Institute, 8th Mile Mysore Road, Bangalore 560059, India
E-mail: sury@isibang.ac.in

Here $\sigma_k(m) := \sum_{d|m} d^k$ and, we use the notation $\mathbf{Z}_n$ for the group $\mathbf{Z}/n\mathbf{Z}$. In fact, this identity can be proved using elementary number theory but our stress is more on the fact that both sides drop out naturally from group actions. Probably, there is scope for the method to carry over to more general groups and hopefully give new identities. Note the special case $r = 1$ is the following beautiful identity due to P.K. Menon [1]:

Let n be a natural number. Then,

$$\sum_{GCD(a,n)=1} GCD(a-1,n) = \phi(n)d(n).$$

Here $d(n)$ is the divisor function. He had proved this by number-theoretic methods. In the last section where we analyze the action of $GL_r(\mathbf{Z}_n)$ on $(\mathbf{Z}_n)^r$, we obtain two sets

$$\{(a_1,\cdots,a_r) : a_i \leq n, GCD(a_1,\cdots,a_r,n) = 1\}$$

and

$$\{c \leq n^r : p^r \not| GCD(c,n^r)\ \forall\ prime\ p\}$$

which have the same cardinality but there doesn't seem to be an obvious bijection between them !

2 'Not-Burnside' lemma for the upper triangular group.

'Not-Burnside' lemma *Let a finite group G act on a finite set S with N orbits. Then,*

$$\sum_{g\in G} |S^g| = O(G)N.$$

This simple lemma is well-known to have applications, via Polya's theory of enumeration, to chemistry - in particular, to counting of isomers.

Before stating a more general result, we point out how a special case proves Menon's identity; this will set the tone for later computations which is slightly messier.

Proof of Menon's identity Let the group $G = \mathbf{Z}_n^*$ of integers coprime to n, under multiplication mod n, act on $S = \mathbf{Z}_n$ by $(a,b) \mapsto ab$. Now, for $a \in G$, $S^a = \{b \in \mathbf{Z}_n : ab \equiv b \ mod\ n\}$. We see that $(a-1)b \equiv 0$ mod n is equivalent to $\frac{a-1}{d}b \equiv 0$ mod $\frac{n}{d}$ where $d = (a-1,n)$ and has exactly the d solutions $\frac{n}{d}, \frac{2n}{d}, \cdots, 0$. Thus, the left hand side of the not-Burnside lemma gives the left hand side of Menon's identity.

To count the number N of orbits for our action, we observe that two elements b and c of $\mathbf{Z}_n$ have the same orbit if, and only if, $(b,n) = (c,n)$. In other words, orbits are

$$\Omega_d := \{a : (a,n) = d\}$$

for divisors d of n. Thus $N = d(n)$. Note also that $|\Omega_d| = \phi(n/d)$ and, since $\mathbf{Z}_n$ is the union of orbits, we have the well-known identity

$$n = \sum_{d|n} \phi(n/d).$$

The two sides of the not-Burnside lemma now give Menon's identity. □

Note that Menon's identity gives an immediate proof of the well-known inequality $d(n)\phi(n) \geq n$ as the left hand side of the not-Burnside lemma has n as a term (corresponding to $a = 1$).

Theorem 1 *Let n be a natural number. Consider the action of the group*

$$G = \{ \begin{pmatrix} t_1 & t_2 & t_3 & \cdots & t_r \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} : t_1 \in (\mathbf{Z}_n)^*, t_i \in \mathbf{Z}_n \ for\ all i > 1\}$$

on $S = (\mathbf{Z}_n)^r$ as matrix multiplication on the left on column vectors. Write

$$g(t_1, \cdots, t_r) = \begin{pmatrix} t_1 & t_2 & t_3 & \cdots & t_r \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \in G.$$

Then, we have:

(i) $|S^{g(t_1,\cdots,t_r)}| = n^{r-1} GCD(n, t_1 - 1, t_2, \cdots, t_r)$.
(ii) The number of orbits is $\sigma_{r-1}(n)$.
(iii) We have the identity :

$$\sum_{t_1 \in (\mathbf{Z}_n)^*, t_2, \cdots, t_r \in \mathbf{Z}_n} GCD(n, t_1 - 1, t_2, \cdots, t_r) = \phi(n)\sigma_{r-1}(n).$$

Although the proof is not different for different r, it is a bit more transparent when $r = 1$. We first discuss this case separately for clarity. So, we now write

$$G = \{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbf{Z}_n)^*, b \in \mathbf{Z}_n\}.$$

Proposition 1 *(i)* $|S^g| = n(n, a-1, b)$ *if* $g = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$.

(ii) The number of orbits is $\sigma(n)$.
(iii) $\sum_{a\in(\mathbf{Z}_n)^*}\sum_{b\in\mathbf{Z}_n}(n,a-1,b)=\phi(n)\sigma(n)$.

Proof Of course, (iii) follows from (i) and (ii) by the not-Burnside lemma. To prove (i), consider $g=\begin{pmatrix} a\ b \\ 0\ 1\end{pmatrix}\in G$ and $(a_1,a_2)^t\in S^g$. Then, we have :

$$(a-1)a_1+ba_2\equiv 0\ mod\ n.$$

If $GCD(n,a-1)=d$, we have $d|ba_2$ and so there are (d,b) solutions for a_2. Also, then a_1 can be arbitrary; hence $|S^g|=n(n,a-1,b)$.

Now, to prove (ii), look at the orbit $\Omega(a_1,a_2)=\{(aa_1+ba_2,a_2):(a,n)=1,b\leq n\}$ of any (a_1,a_2). Note that the second co-ordinate remains fixed. We observe that the cardinality of this is a multiplicative function of n, due to the following reason. Let $GCD(l,m)=1$ and look at the isomorphisms

$$\mathbf{Z}_l\times\mathbf{Z}_m\to\mathbf{Z}_{lm}$$

and

$$(\mathbf{Z}_l)^*\times(\mathbf{Z}_m)^*\to(\mathbf{Z}_{lm})^*$$

given by the Chinese remainder theorem. Evidently, the above isomorphism maps orbits to orbits. Therefore, it suffices to compute the number of orbits when $n=p^k$ for some prime p. Let $(p^k,a_2)=p^l$ with $l\leq k$. If $l=0$, then the set

$$\{(a_0,a_2):a_0\in\mathbf{Z}_n\}$$

is an orbit because one can solve for a,b with $aa_1+ba_2\equiv a_0$ mod p^k. Thus, each a_2 relatively prime to n gives one orbit. This contributes $\phi(p^k)$ orbits.
Next, look at any $pa_2\in\mathbf{Z}_n$ for which $(a_2,p)=1$. For any such fixed a_2, there are two orbits

$$\{(a_0,pa_2):a_0\in(\mathbf{Z}_{p^k})^*\}$$

and

$$\{(pa_0,pa_2):a_0\in\mathbf{Z}_{p^k}\}.$$

Thus, there are $\phi(p^{k-1})$ such a_2's and, for each one, there are two orbits; these contribute $2\phi(p^{k-1})$ orbits.
If we look at orbits of elements of the form $(*,p^2a_2)$ with $(a_2,p)=1$, we get the orbits

$$\{(a_0,p^2a_2):a_0\in(\mathbf{Z}_{p^k})^*\},$$

$$\{(pa_0,p^2a_2):a_0\in(\mathbf{Z}_{p^k})^*\};$$

$$\{(p^2a_0,p^2a_2):a_0\in\mathbf{Z}_{p^k}\}.$$

Thus, we get three orbits from each of the a_2's here, which are $\phi(p^{k-2})$ in number as $p^2a_2 \leq p^k$ and $(a_2,p)=1$. In this manner, we have $3\phi(p^{k-2})$ orbits. Proceeding in this manner, the total number of orbits is

$$\sum_{l=1}^{k} l\phi(p^{k-l+1}) = \sigma(p^k).$$

In fact, we can easily show that $\sigma(n) = \sum_{t|n} d(t)\phi(n/t)$ for any n, by looking at the corresponding Dirichlet series. Thus, (ii) is proved.

Then (iii) follows from the not-Burnside lemma because the order of G is $n\phi(n)$. The proof of the proposition is complete. □

Proof of Theorem 1 Once again (iii) is a consequence of (i) and (ii) from the not-Burnside lemma since the order of the group is $n^{r-1}\phi(n)$.

To prove (i), we need to compute $|S^{g(t_1,\cdots,t_r)}|$. Look at the number of solutions in $a_1,a_2,\cdots,a_r \in \mathbf{Z}_n$ for $g(a_1,\cdots,a_r)=(a_1,\cdots,a_r)$; that is,

$$(t_1-1)a_1+t_2a_2+\cdots+t_ra_r \equiv 0 \ mod\ n.$$

Claim : *For any $b_1,b_2\cdots,b_r \in \mathbf{Z}_n$, the cardinality of*

$$\{(x_1,\cdots,x_r) \in (\mathbf{Z}_n)^r : \sum_{i=1}^{r} b_ix_i = 0\}$$

equals $n^{r-1}GCD(n,b_1,b_2,\cdots,b_r)$.

This can be proved by induction on r. If $r=1$, clearly $b_1x_1 \equiv 0$ mod n has the (n,b_1) solutions $ln/(n,b_1)$ with $1 \leq l \leq (n,b_1)$. Assuming $r>1$ and that the result is true for $r-1$, we consider any possible solution $(x_1,\cdots,x_r)$ of $\sum_{i=1}^{r} b_ix_i \equiv 0$ mod n. So $\sum_{i=2}^{r} b_ix_i \equiv 0$ mod (n,b_1). By induction hypothesis, the number of tuples $(x_2,\cdots,x_r)$ with x_i varying mod (n,b_1) equals $(n,b_1)^{r-2}(n,b_1,b_2,\cdots,b_r)$. But, if $x_2,\cdots,x_r$ vary mod n, we are allowed to change each x_i by any one of the $n/(n,b_1)$ multiples of (n,b_1). Thus, the number of tuples $(x_2,\cdots,x_r)$ with x_i varying mod n is

$$(n,b_1)^{r-2}(n,b_1,b_2,\cdots,b_r)(n/(n,b_1))^{r-1}.$$

Now, when $(x_2,\cdots,x_r)$ is any one such tuple with $\sum_{i=2}^{r} b_ix_i \equiv 0$ mod (n,b_1), the equation

$$\frac{b_1}{(n,b_1)}x_1 + \frac{\sum_{i=2}^{r} b_ix_i}{(n,b_1)} \equiv 0 \ mod\ \frac{n}{(n,b_1)}$$

has a unique solution for x_1 modulo $\frac{n}{(n,b_1)}$. Thus, allowing for changing of x_1 by a multiple of $\frac{n}{(n,b_1)}$, we have (n,b_1) choices for x_1 mod n for each fixed $x_2,\cdots,x_r$. Therefore, the number of solutions is

$$(n,b_1)(n,b_1)^{r-2}(n,b_1,b_2,\cdots,b_r)(n/(n,b_1))^{r-1} = (n,b_1,b_2,\cdots,b_r)n^{r-1}.$$

Hence, the claim is proved and we have (i).

Finally, (ii) can be proved once again by reducing to prime powers using the Chinese remainder theorem as before. Indeed, assume that $n = p^k$ and look at the orbit of any $(a_1, \cdots, a_r)$. The last $r-1$ co-ordinates are fixed and the first one runs over the set

$$\{(t_1a_1 + \cdots + t_ra_r : t_1 \in (\mathbf{Z}_n)^*, t_i \in \mathbf{Z}_n \; \forall \; 2 \leq i \leq r\}.$$

If $(p, a_i) = 1$ for some $2 \leq i \leq r$, then the set

$$\{(a_0, a_2, \cdots, a_r) : a_0 \in \mathbf{Z}_n\}$$

is a single orbit since one can solve the equation $t_1a_1 + \cdots + t_ra_r = a_0$ for $t_1 \in (\mathbf{Z}_{p^k})^*$ for suitable $t_2, \cdots, t_r \in \mathbf{Z}_{p^k}$ when a_0 is arbitrary. This is so, because if $(a_i, p) = 1$, then one may choose $t_i \in (\mathbf{Z}_{p^k})^*$ so that $a_0 - \sum_{i=2}^r t_ia_i$ is in $(\mathbf{Z}_{p^k})^*$. Thus, for each choice of $a_2, \cdots, a_r$ with at least one a_i a unit, one has one orbit. This gives $(p^k)^{r-1} - (p^{k-1})^{r-1}$ orbits.
Now, look at the orbit of an element of the form $(a_1, pa_2, pa_3, \cdots, pa_r)$. Clearly all the tuples $(a_0, pa_2, \cdots, pa_r)$ with $(a_0, p) = 1$ form an orbit as one can solve, for any a_0, a_1 relatively prime to p, the equality $t_1a_1 + \sum_{i=2}^r t_ipa_i \equiv a_0 \bmod p^k$ for $t_1 \in (\mathbf{Z}_{p^k})^*$. Thus, we have $(p^{k-1})^{r-1}$ orbits of this kind.
If $(a_i, p) = 1$ for some $2 \leq i \leq r$, then the set

$$\{(pa_0, pa_2, \cdots, pa_r) : a_0 \leq p^{k-1}\}$$

is a single orbit as argued in the beginning. This way provides $(p^{k-1})^{r-1} - (p^{k-2})^{r-1}$ orbits.

Proceeding in this manner, we see that there are two orbits of a tuple of the form $(a_1, 0, 0, \cdots, 0)$; these are

$$\{(a_0, 0, 0, \cdots, 0) : (p, a_0) = 1\}$$

and the singleton $\{(0, 0, \cdots, 0)\}$. Thus, the total number of orbits equals

$$((p^k)^{r-1} - (p^{k-1})^{r-1}) + (p^{k-1})^{r-1} + ((p^{k-1})^{r-1} - (p^{k-2})^{r-1}) + \cdots + (p^{r-1} - 1) + 2.$$

This simplifies to $p^{k(r-1)} + p^{(k-1)(r-1)} + \cdots + p^{r-1} + 1 = \sigma_{r-1}(p^k)$. The proof is complete. □

Problem worth further investigation: For the action on $(\mathbf{Z}_n)^r$ of the subgroup of upper triangular matrices contained in $GL_r(\mathbf{Z}_n)$, compute both sides of the not-Burnside lemma.

3 The general linear group over finite rings

Let us look at the 'linear' action of $G = GL_r(\mathbf{Z}_n)$ on the set S of r-tuples $\mathbf{Z}_n \times \mathbf{Z}_n \times \cdots \times \mathbf{Z}_n$, for any fixed natural numbers $n, r \geq 2$. We write the tuples as columns and take matrix multiplication on the left. The situation is more complicated. Before stating the results, for any $r \geq 1$, we recall the generalized totient function (sometimes called Jordan's totient) $\phi_r(n) = n^r \prod_{p|n}(1-1/p^r)$. Note ϕ_1 is the usual phi-function. The main result is :

Theorem 2 *(i) The orbits are parametrized by divisors d of n and are given as*

$$\Omega_d = \{(a_1, \cdots, a_r) \in S : GCD(a_1, \cdots, a_r, n) = d\}.$$

(ii) The cardinality $|\Omega_d| = \phi_r(n/d)$. *In particular,* $n^r = \sum_{d|n} \prod_{p|d} d^r(1-1/p^r)$.

(iii) For any r, n, *there is a bijection between the sets* Ω_1 *and*

$$\{c \leq n^r : p^r \not| GCD(c, n^r)\ \forall \text{ prime } p\}.$$

(iv) We have

$$\sum_{g \in G} |S^g| = d(n) n^{r^2} \prod_{p|n} \{(1-\frac{1}{p})(1-\frac{1}{p^2}) \cdots (1-\frac{1}{p^r})\}.$$

(iii) If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, *then*

$$\sum_{g \in G} |S^g| = \prod_{i=1}^{k} \sum_{g \in GL_r(\mathbf{Z}_{p_i^{\alpha_i}})} ((\mathbf{Z}_{p_i^{\alpha_i}})^r)^g|.$$

That is, the expressions given by the not-Burnside lemma is a product of corresponding expressions when n is a prime power.

Proof The Chinese remainder theorem tells us that the group G as well as the set $(\mathbf{Z}_n)^r$ breaks up into a Cartesian product corresponding to the prime powers dividing n and, the orbits themselves are products of the orbits of $GL_r(\mathbf{Z}_{p^k})$ on $(\mathbf{Z}_{p^k})^r$ for various prime powers dividing n. The Chinese remainder theorem also helps us compute the order of G. Indeed, it is easy to show that

$$O(GL_r(\mathbf{Z}_n)) = n^{r^2} \prod_{p|n} ((1-\frac{1}{p})(1-\frac{1}{p^2}) \cdots (1-\frac{1}{p^r})).$$

Hence, we have the assertion in (v). Moreover, the assertion (iv) follows from this excepting that one has to show that the number of orbits is $d(n)$. Let us now prove (i),(ii) and (iii). We start with various observations.

Observation 1 *Orbit of any* $(x_1, \cdots, x_r)$ *is the orbit of* $(d_1, \cdots, d_r)$ *where* $d_i = (x_i, n)$.

Proof It is easy to get even a diagonal matrix in G. □

Observation 2 *For divisors $d_1, \cdots, d_r$ and divisors $h_1, \cdots, h_r$ of n, if the orbits are the same, then $GCD(d_1, \cdots, d_r) = GCD(h_1, \cdots, h_r)$.*

Proof Let $g = (g_{ij}) \in G$ be such that

$$g \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = \begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_r \end{pmatrix} \ \ in \ \ \mathbf{Z}_n \times \cdots \times \mathbf{Z}_n.$$

Then, $\sum_{j=1}^{r} g_{ij} d_j = h_j + nc_j$ as integers where $c_j \in \mathbf{Z}$. Thus, the GCD of all the d_i's divides each right hand side above. As it certainly divides n, this GCD must divide each h_j. Hence $GCD(d_1, \cdots, d_r)$ divides $GCD(h_1, \cdots, h_r)$. By symmetry, the result follows. □

Observation 3 *For divisors $d_1, \cdots, d_r$ and divisors $h_1, \cdots, h_r$ of n, the orbits are the same, if $GCD(d_1, \cdots, d_r) = GCD(h_1, \cdots, h_r)$.*

Proof. Let $GCD(d_1, \cdots, d_r) = D$, say. Then, get integers $g_{11}, \cdots, g_{1r}$ such that $g_{11} d_1 + \cdots + g_{1r} d_r = D$. Now, one can complete this unimodular row to a matrix $g \in SL(r, \mathbf{Z})$. Then, $g \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix}$ is of the form $\begin{pmatrix} D \\ l_2 D \\ \vdots \\ l_r D \end{pmatrix}$ for some integers l_j. Left multiplying by the matrix $\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ -l_2 & 1 & 0 & \cdots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots \\ -l_r & 0 & 0 & \cdots & 1 \end{pmatrix}$, we get a matrix $A \in SL(r, \mathbf{Z})$ such that

$$A \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = \begin{pmatrix} D \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

One can evidently regard A as an element of G. This proves that the orbit of $(d_1, \cdots, d_r)$ is that of $(D, 0, \cdots, 0)$. The observation follows. □

Completion of proof of Theorem 2 By the last observation, the orbits are

$$\Omega_d(n) = \{(a_1, \cdots, a_r) : GCD(a_1, \cdots, a_r, n) = d\}$$

as d varies over divisors of n; the number of orbits is $d(n)$. This proves (i).

Now, clearly

$$\Omega_d(n) = \{(da_1,\cdots,da_r) : a_i \leq n/d, GCD(a_1,\cdots,a_r,n/d) = 1\}.$$

Thus, one needs to compute only the cardinality of the set

$$\{(b_1,\cdots,b_r) : b_i \leq m, GCD(b_1,\cdots,b_r,m) = 1\}$$

for any m. Once again, the Chinese remainder theorem gives a bijection between $\Omega_1(l) \times \Omega_1(m)$ and $\Omega_1(lm)$. Indeed, if $lL + mM = 1$, then the map $(\mathbf{a},\mathbf{b}) \mapsto mM\mathbf{a} + lL\mathbf{b}$ mod lm gives such a bijection. Here, we have written **a** and **b** in short for $(a_1,\cdots,a_r)$ and $(b_1,\cdots,b_r)$ respectively. Thus,

$$|\Omega_1(p_1^{\alpha_1}\cdots p_k^{\alpha_k})| = \prod_{i=1}^{k} |\Omega_1(p_i^{\alpha_i})|.$$

Now, $(b_1,\cdots,b_r) \notin \Omega_1(p^k)$ if and only if $p|b_i$ for each i and $b_i \leq p^k$. Evidently, this has cardinality $(p^{k-1})^r$ which means

$$|\Omega_1(p^k)| = (p^k)^r - (p^{k-1})^r = p^{kr}(1-1/p^r).$$

Hence, $|\Omega_1(n) = n^r \prod_{p|n}(1-1/p^r)$. We have proved (ii).

Finally, to prove (iii), look at the set

$$\Phi(n) := \{c \leq n^r : p^r \not| GCD(c,n^r)\ \forall\ prime\ p\}.$$

To show that the cardinality $|\Phi(n)|$ is a multiplicative function of n, look at two relatively prime a,b. Then we have $Aa^n + Bb^n = 1$ for some integers A,B. We will define a one-to-one correspondence between $\Phi(a) \times \Phi(b)$ and $\Phi(ab)$. Indeed, if $u \in \Phi(a)$, and $v \in \Phi(b)$, consider $vAa^n + uBb^n$ (this is exactly the solution x mod a^nb^n produced by the Chinese remainder theorem given $x \equiv u$ mod a^n and $x \equiv v$ mod b^n). Adding a suitable multiple ka^nb^n, we get an element $t = \Phi(a)vAa^n + uBb^n + ka^nb^n$ in $\Phi(ab)$. Indeed, $(u,v) \mapsto t$ is the bijection we were looking for. This proves the multiplicativity. Now, a simple count gives the cardinality of $\Phi(p^k)$ to be $p^{kr} - p^{(k-1)r}$. Therefore, $|\Phi(n)| = n^r \prod_{p|n}(1-1/p^r) = \phi_r(n)$. Therefore, we have proved (iii) also. □

We have an
Intriguing question.
Proposition 2 (iii) proves equality of cardinalities of the sets

$$\{(a_1,\cdots,a_r) : a_i \leq n, GCD(a_1,\cdots,a_r,n) = 1\}$$

and

$$\{c \leq n^r : p^r \not| GCD(c,n^r)\ \forall\ prime\ p\}.$$

Is there a natural bijection between them ?

Note that the left hand side of the not-Burnside lemma in general seems difficult to compute. We look at the case when $n = p$, a prime and draw some corollaries.

Clearly, for $g \in G$, we have

$$S^g = \{(d_1, \cdots, d_r) : (g - I)(d_1, \cdots, d_r)^t = (0, \cdots, 0)^t\}$$

which is a vector space over $\mathbf{Z}_p$. Thus, $|S^g| = p^{dim(Ker(g-I))}$. If $N_t = |\{g \in G : rank(g-I) = t\}|$, then the not-Burnside lemma implies

$$2(p^r - 1)(p^r - p) \cdots (p^r - p^{r-1}) = \sum_{0 \leq t \leq r} N_t p^{r-t}$$

since the order of G is $(p^r - 1)(p^r - p) \cdots (p^r - p^{r-1})$.

Corollary 1 *For $r \geq 2$, p divides $|\{g \in GL_r(\mathbf{Z}_p) : g - I \in GL_r(\mathbf{Z}_p)\}|$.*

Acknowledgements This work began with coffee-time conversations when the author visited the Max Planck Institut Für Mathematik in Bonn. The author acknowledges its stimulating influence and Pieter Moree in particular. He is also indebted to Andrew Granville who showed how some of the number-theoretic identities derived here group-theoretically, follow purely number-theoretically.

References

1. Kesava Menon, P.: *On the sum* $\sum(a-1,n)[(a,n)=1]$, J.Indian Math. Soc., (N.S.) **29** (1965), 155–163
2. Neumann, P.: *A lemma that is not Burnside's*, Math. Sci., **4** (1979), 133–141