# A prime congruence system

# A Prime Congruence Theorem

## 1. Introduction

The congruence theorem which we prove in this paper was discovered in attempting to establish a relationship between certain commutator elements of different weights in a standard wreath product of $p$-groups. The idea of forming matrix entries in the way described below was motivated as a method of collecting exponents of like commutator elements after each step in a rearrangement factorization process. While the matrix notation helps to motivate the proof, matrix operations are not utilized in the proof. It is still an open question as to whether a proof could be accomplished via matrix operations. The authors have not been successful in this regard.

**Definition 1.1.** Let $p$ denote any prime number and $A=(a_{i,j})$ be the $(p-1)$ by $(p-1)$ matrix with the column entries defined recursively as follows:

$$a_{i,1}=i, \qquad i=1,2,\ldots,p-1,$$

$$a_{i,k}=i\sum_{j=1}^{i} a_{j,k-1}, \qquad k>1 \text{ and } i=1,2,\ldots,p-1.$$

The entry $a_{i,k}$ is $i$ times the sum of the first $i$ entries of column $k-1$. Let $\bar{A}=(\bar{a}_{i,j})$ denote the matrix formed from $A$ by reducing all entries modulo $p$.

**Theorem 1.2.** All entries below the minor diagonal in $\bar{A}$ are 0. As an example, in the case $p=5$, the matrix $\bar{A}$ is

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 1 & 4 & 0 \\ 3 & 3 & 0 & 0 \\ 4 & 0 & 0 & 0 \end{pmatrix}$$

It is interesting to note that the entry $\bar{a}_{p-1,2}=0$ because of the formula for the sum of the first $k$ positive integers. Also, the entry $\bar{a}_{2,p-1}=0$ since, prior to being reduced modulo $p$, this entry is $2+2^2+\cdots+2^{p-1}=2(1+2+\cdots+2^{p-2})=-2(1-2^{p-1})$ which is congruent to 0 modulo $p$ by Fermat's Little Theorem. Perhaps other elementary and well known theorems can be cited to give partial results to this problem.

## 2. The Proof

The proof is by a double induction argument and is presented via a series of three Lemmas. The authors acknowledge and thank Professor J.M. Gandhi for suggesting the well know differentiation technique utilized in the proof of Lemma 2.2. In all statements of the sequel, $a_{i,j}$ and $\bar{a}_{i,j}$ denote matrix entries in $A$ and $\bar{A}$ respectively, according to Definition 1.1 with $1\leq i,j\leq p-1$.

**Lemma 2.1** $a_{k+1,n+1}=(k+1)\left((1/k)\,a_{k,n+1}+a_{k+1,n}\right)$

Proof. $$a_{k+1,n+1}=(k+1)\left(\sum_{j=1}^{k}a_{j,n}+a_{k+1,n}\right)$$
$$=(k+1)\left((1/k)\,k\sum_{j=1}^{k}a_{j,n}+a_{k+1,n}\right)$$
$$=(k+1)\left((1/k)\,a_{k,n+1}+a_{k+1,n}\right)$$

**Lemma 2.2** $$a_{k,n}=k\sum_{j=0}^{k-1}(-1)^j(k-j)^{n+k-2}/j!\,(k-1-j)!\,.$$

*Proof.* Proceeding with a double induction argument on $n$ and $k$, we first verify the formula

$$k=a_{k,1}=k\sum_{j=0}^{k-1}(-1)^j(k-j)^{k-1}/j!\,(k-1-j)!\,.$$

Beginning with the binomial identity

$$(1-x)^{k-1}=\sum_{i=0}^{k-1}(-1)^i(k-1)!x^i/i!\,(k-1-i)!$$

we multiply by $x$ and then differentiate with respect to $x$ to get

$$(1-x)^{k-1}-(k-1)x(1-x)^{k-2}=\sum_{i=0}^{k-1}(-1)^i(k-1)!\,(i+1)\,x^i/i!\,(k-1-i)!\,.$$

Repeating this process of multiplication and differentiation we have

$$(1-x)^{k-2}g(x)+(k-1)(k-2)x^2(1-x)^{k-3}$$
$$=\sum_{i=0}^{k-1}(-1)^i(k-1)!\,(i+1)^2x^i/i!\,(k-1-i)!\,.$$

After $k-1$ repetitions and replacement of 1 for $x$,

$$(-1)^{k-1}(k-1)!=\sum_{i=0}^{k-1}(-1)^i(k-1)!\,(i+1)^{k-1}/i!\,(k-1-i)!$$

which implies

$$1=\sum_{i=0}^{k-1}(-1)^{i-k+1}(i+1)^{k-1}/i!\,(k-1-i)!\,.$$

Setting $j=k-i-1$ this identity becomes

$$1=\sum_{j=0}^{k-1}(-1)^j(k-j)^{k-1}/(k-1-j)!\,j!$$

which establishes the formula for $n=1$ and all $k$.

The identity

$$a_{1,n} = 1 = \sum_{j=0}^{0} (-1)^j (1-j)^{n-1}/j!\,(-j)!$$

is clear and the proof is completed by verifying the formula for $a_{k+1,n+1}$ utilizing the formulas for $a_{k,n+1}$ and $a_{k+1,n}$ and Lemma 2.1. Before using Lemma 2.1, rewrite the expression for $(1/k)\,a_{k,n+1}$ as follows:

$$\begin{aligned}(1/k)\,a_{k,n+1} &= \sum_{j=0}^{k-1} (-1)^j (k-j)^{n+k-1}/j!\,(k-1-j)! \\ &= \sum_{j=1}^{k} (-1)^{j-1} (k-j+1)^{n+k-1}/(j-1)!\,(k-j)! \\ &= \sum_{j=0}^{k} -(-1)^j j\,(k-j+1)^{n+k-1}/j!\,(k-j)!\,.\end{aligned}$$

Now substituting into Lemma 2.1 we have

$$\begin{aligned}a_{k+1,n+1} &= (k+1)\Bigg[\sum_{j=0}^{k} -(-1)^j j\,(k-j+1)^{n+k-1}/j!\,(k-j)! \\ &\quad + (k+1)\sum_{j=0}^{k} (-1)^j (k-j+1)^{n+k-1}/j!\,(k-j)!\Bigg] \\ &= (k+1)\Bigg[\sum_{j=0}^{k} (-1)^j (k-j+1)^{n+k-1}/j!\,(k-j)!\Bigg](k+1-j) \\ &= (k+1)\sum_{j=0}^{k} (-1)^j (k-j+1)^{n+k}/j!\,(k-j)!\,.\end{aligned}$$

The proof of Theorem 1.2 follows directly from Lemma 2.2 and the next Lemma which verifies that the entries immediately below the minor diagonal in $\bar{A}$ are all zero.

**Lemma 2.3** $\bar{a}_{k,p-k+1} = 0$ for $k = 2, \ldots, p-1$.

Proof.
$$\begin{aligned}a_{k,p-k+1} &= k\sum_{j=0}^{k-1} (-1)^j (k-j)^{p-k+1+k-2}/j!\,(k-j-1)! \\ &= k\sum_{j=0}^{k-1} (-1)^j (k-j)^{p-1}/j!\,(k-1-j)! \\ &\equiv k\sum_{j=0}^{k-1} (-1)^j/j!\,(k-1-j)! \pmod{p} \\ &= \big(k/(k-1)!\big)\sum_{j=0}^{k-1} (-1)^j (k-1)!/j!\,(k-1-j)! \\ &= \big(k/(k-1)!\big)\,(1-1)^{k-1} \\ &= 0\end{aligned}$$

Larry J. Morley and Alan Bishop Western Illinois University, Macomb, USA