UNIV. BEOGRAD. PUBL. ELEKTROTEHN. FAK.
Ser. Mat. 9 (1998), 51–53.

A REMARK ON THE LEFT-FACTORIAL HYPOTHESIS

Winfried Kohnen

An elementary reformulation of the left-factorial hypothesis is given.

1. INTRODUCTION

The so-called left-factorial hypothesis (a problem posed by Đ. KUREPA [**2**] and still open today) states that for every odd prime p one has

$$\sum_{\nu=0}^{p-1} \nu! \not\equiv 0 \pmod{p} \tag{1}$$

In [**1**] A. IVIĆ and Ž. MIJAJLOVIĆ discuss this hypothesis and some reformulations in detail. For example, according to [**3**], (1) is equivalent to

$$\sum_{\nu=0}^{p-1} \frac{(-1)^\nu}{\nu!} \not\equiv 0 \pmod{p} \tag{2}$$

(this, in fact, is not very difficult to see). Other elementary reformulations are due to Z. ŠAMI [**4**] and J. STANKOVIĆ [**5**].

In this short note, using the equivalence of (1) and (2) we would like to give another elementary reformulation of (1) in terms of certain recurrence sequences modulo p (resp. a certain matrix non-congruence modulo p).

2. STATEMENT OF RESULT AND PROOF

Theorem. *Let p be an odd prime. Then the following statemens are equivalent*:

i) The left-factorial hypothesis holds for p, i.e. one has

$$\sum_{\nu=0}^{p-1} \nu! \not\equiv 0 \pmod{p}$$

1991 Mathematics Subject Classification: 11B65, 05A10 *ii) For any given integers a_1, a_0 define a sequence $(a_n)_{n\geq 0}$ recurrently by*

$$a_n := \left(1-\frac{1}{n}\right)a_{n-1}+\frac{1}{n}a_{n-2} \qquad (n\geq 2). \tag{3}$$

Then

$$(a_{p-1},a_{p-2})\not\equiv(a_1,a_0)\,(\bmod\, p)$$

if and only if

$$a_1\not\equiv a_0\,(\bmod\, p).$$

iii) If

$$A_n := \begin{pmatrix} 1-\frac{1}{n} & \frac{1}{n} \\ 1 & 0 \end{pmatrix} \qquad (n\geq 2)$$

and

$$A := A_{p-1}\cdot A_{p-2}\cdots A_2,$$

then

$$A\not\equiv\begin{pmatrix}1&0\\0&1\end{pmatrix}\,(\bmod\, p)$$

Proof. With $a_1=0$, $a_0=1$ we find from (3) that

$$a_n=\sum_{\nu=0}^{n}\frac{(-1)^\nu}{\nu!}$$

for all n. Indeed, for $n\geq 2$ one has

$$\left(1-\frac{1}{n}\right)\sum_{\nu=0}^{n-1}\frac{(-1)^\nu}{\nu!}+\frac{1}{n}\sum_{\nu=0}^{n-2}\frac{(-1)^\nu}{\nu!}=\sum_{\nu=0}^{n-1}\frac{(-1)^\nu}{\nu!}-\frac{1}{n}\cdot\frac{(-1)^{n-1}}{(n-1)!}=\sum_{\nu=0}^{n}\frac{(-1)^\nu}{\nu!}\,.$$

In particular,

$$a_{p-1}=\sum_{\nu=0}^{p-1}\frac{(-1)^\nu}{\nu!}$$

and

$$a_{p-2}=a_{p-1}-\frac{1}{(p-1)!}\equiv a_{p-1}+1\,(\bmod\, p),$$

where in the last line we have used Wilson's congruence.

Since (1) is equivalent to (2), we therefore see that if *i)* fails then also *ii)* fails.

Let us look at *ii)*. Cleary, by definition (3), if $a_1\equiv a_0\,(\bmod\, p)$ then $(a_{p-1},a_{p-2})\equiv(a_1,a_0)\,(\bmod\, p)$.

Now suppose that *ii)* does not hold, i.e. we can find $(a_1,a_0)\in\mathbf{Z}^2$ with $a_1\not\equiv a_0\,(\bmod\, p)$ and such that $(a_{p-1},a_{p-2})\equiv(a_1,a_0)\,(\bmod\, p)$.

Then the matrix $\begin{pmatrix} 1 & a_1 \\ 1 & a_0 \end{pmatrix}$ is invertibile module p, hence there exists integers λ and μ such that

$$(0,1) \equiv \lambda(1,1) + \mu(a_1, a_0) \pmod{p}.$$

Applying (3) succesively we obtain from (4)

$$\sum_{\nu=0}^{p-1} \frac{(-1)^\nu}{\nu!} \equiv \lambda + \mu a_{p-1} \pmod{p} \equiv \lambda + \mu a_1 \pmod{p} \equiv 0 \pmod{p}.$$

Hence $i)$ fails.

The equivalence of $ii)$ and $iii)$ is obvious. Indeed, rewrite (3) as

$$\begin{pmatrix} a_n \\ a_{n-1} \end{pmatrix} = A_n A_{n-1} \dots A_2 \begin{pmatrix} a_1 \\ a_0 \end{pmatrix} \qquad (n \geq 2)$$

and observe that each of the matrices A_n fixes the column $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Hence if $ii)$ does not hold, then A modulo p fixes two modulo p linearly independent vectors, hence is congurent to the unit matrix modulo p, and the converse is equally true.

This proves the Theorem.

REFERENCES

1. A. Ivić, Ž. Mijajlović: *On Kurepa's problems in number theory*, Publ. Inst. Math. (Beograd) **57 (71)** (1995), 19–28.
2. Đ. Kurepa: *On the left-factorial function* $!n$, Math. Balkan. **1** (1971), 147–153.
3. Ž. Mijajlović: *On some formulas involving* $!n$ *and the verification of the* $!n$ *–hypothesis by use of computers*, Publ. Inst. Math. (Beograd) **47 (61)**, (1990), 24–32.
4. Z. Šami: *On the M-hypotesis of Kurepa*, Math. Balkan. **4** (1974), 530–532.
5. J. Stanković: *Über einige Relationen zwischen Fakultäten, und den linken Fakultäten*, Math. Balkan. **3** (1973), 488–497.

Mathematisches Institut,
Universtät Heidelberg,
Im Neuenheimer Feld 288,
D-69120 Heidelberg,
Germany

(Received December 24, 1997)