

ON STEPHAN'S CONJECTURES CONCERNING PASCAL TRIANGLE MODULO 2

VLADIMIR SHEVELEV

ABSTRACT. We prove a series of Stephan's conjectures concerning Pascal triangle modulo 2.

1. INTRODUCTION

Consider Pascal triangle for binomial coefficient modulo 2. If to read every row of this triangle as a binary number, then we obtain the following sequence $\{c(n)\}_{n \geq 0}$ (cf. A001317 in [2]):

$$(1.1) \quad 1, 3, 5, 15, 17, 51, 85, 255, 257, 771, 1285, 3855, 4369, 13107, 21845, \dots$$

It is easy to see that

$$(1.2) \quad c(2n) \equiv 1 \pmod{4}, \quad n = 0, 1, \dots$$

Denote

$$(1.3) \quad l(n) = \frac{c(2n) - 1}{4}.$$

In 2004, for sequence $\{l(n)\}_{n \geq 0}$, R. Stephan formulated a series of the following conjectures (cf. his comments to A089893 in [2]):

Conjecture 1.

$$(1.4) \quad l(2^k) = 2^{2^{k+1}-2}.$$

Conjecture 2.

$$(1.5) \quad \lim_{n \rightarrow \infty} l(2n+1)/l(2n) = 5.$$

Conjecture 3.

$$(1.6) \quad \lim_{n \rightarrow \infty} l(4n+2)/l(4n+1) = 17/5.$$

Conjecture 4.

$$(1.7) \quad \lim_{n \rightarrow \infty} l(8n+4)/l(8n+3) = 257/85.$$

etc.

In this paper we prove these conjectures.

2. ON SEQUENCE A001317

Consider an infinite in both sides $(0, 1)$ -sequence with a finite set of 1's which we call C -sequence. Removing in it all 0's before the first 1 and after the last 1, we obtain some odd number which we call the kernel of C -sequence. Every C -sequence generates a new C -sequence, if to write sums of every pair of its adjacent terms modulo 2. If to consider infinite iterations of such process beginning with C -sequence with kern 1, then we obtain C -sequences, the kernels $\{c(i)\}_{i \geq 0}$ of which form Pascal's triangle for binomial coefficients modulo 2. Note that, $c(0) = 1$ and $c(i)$ contains $i + 1$ binary digits.

Consider now sequence $\{d(n)\}$ defined by the formula $d(0) = 1$; for $n \geq 1$, if binary expansion of n is

$$(2.1) \quad n = \sum_{i=1}^m 2^{k_i},$$

then

$$(2.2) \quad d(n) = \prod_{i=1}^m F(k_i),$$

where

$$(2.3) \quad F(n) = 2^{2^n} + 1, \quad n \geq 0,$$

is Fermat number. Such decomposition of $d(n)$ we call its *Fermat factorization*.

Note that sequence $\{d(i)\}$ possesses the following properties:

- 1) $d(n)$ is a binary number with $n + 1$ $(0, 1)$ -digits;
- 2) numbers $\{d(i)\}$ are 1 and all Fermat numbers or products of distinct Fermat numbers;
- 3) number of Fermat factors in the product equals to $d(n)$ is the number of 1's in the binary expansion of n .
- 4) $F(i)$ divides $d(n)$, $n > 1$, if and only if it is a factor in product (2.2).

Proofs of these properties is very easy: 1) follows from a simple induction; 2) and 3) follow from the definition; 4) follows from the well known fact (cf., e.g.,[3]) that every two Fermat numbers are relatively prime, in view of recursion

$$(2.4) \quad F(n) = 2 + \prod_{i=0}^{n-1} F(i).$$

Theorem 1. For $n = 0, 1, \dots$, we have

$$(2.5) \quad c(n) = d(n).$$

Proof. We use induction, the base of which is $c(0) = d(0) = 1$, $c(1) = d(1) = 3$, $c(2) = d_2 = 5$. Suppose that $c(i) = d(i)$, for $i \leq k$. Let m be the most number for which $F(m)$ divides $c(k) = d(k)$. In non-trivial case, when $c(k) \neq F(m)$, using property 4), for some $r < k$, we have $c(k) = d(r)F(m) = c(r)F(m)$. Furthermore, since, by the condition, $F(m)$ is the most Fermat divisor of $c(k)$ and, in view of (2.4), we have

$$(2.6) \quad c(r) = \frac{c(k)}{F(m)} \leq \prod_{i=0}^{m-1} F(i) = F(m) - 2.$$

Besides, since $c(r) < c(k)$, then, by the inductive supposition,

$$c(r + 1) = d(r + 1).$$

Adding the case when $c(k) = F(m)$, let us prove a recursion: $c(0) = 1, c(1) = 3, c(2) = 5$; for $k \geq 2$,

$$(2.7) \quad c(k + 1) = \begin{cases} 3F(m), & \text{if } c(k) = F(m), \\ F(m + 1), & \text{if } 1 < c(r) = F(m) - 2, \\ F(m)c(r + 1), & \text{if } 1 < c(r) < F(m) - 2. \end{cases}$$

Let $c(k) = F(m)$, $m \geq 1$. C -sequence with kernel $c(k)$ is

$$\dots 01 \underbrace{0\dots 0}_{2^{m-1}} 10\dots$$

Thus the following C -sequence with kernel $c(k + 1)$ is

$$\dots 011 \underbrace{0\dots 0}_{2^{m-2}} 110\dots$$

Comparing kernels $c(k)$ and $c(k + 1)$, we conclude that $c(k + 1) = 3c(k) = 3F(m)$.

Furthermore, if $c(r) = F(m) - 2$, then, by (2.6), we have

$$c(k) = F(m)c(r) = F(m)(F(m) - 2) = F(m + 1) - 2 = \underbrace{11\dots 1}_{2^{m+1}}.$$

Thus the C -sequence with kernel $c(k)$ is

$$\dots 0 \underbrace{11\dots 1}_{2^{m+1}} 0\dots$$

Therefore, by the definition, the C -sequence with kernel $c(k + 1)$ is

$$\dots 01 \underbrace{0\dots 0}_{2^{m+1}-1} 10\dots$$

and we see that $c(k+1) = F(m+1)$.

Let now $c(r) < F(m) - 2$. Since, by the supposition of induction, $c(r) = d(r)$. Therefore, $c(r)$ is a product of Fermat numbers and

$$c(r) \leq \frac{\prod_{i=0}^{m-1} F(i)}{F(0)} = \frac{F(m) - 2}{F(0)}.$$

Hence, $c(r)$ is not more than $(2^m - 1)$ -digits odd binary number. Since

$$c(k) = F(m)c(r) = 2^{2^m}c(r) + c(r),$$

then $c(k)$ has the binary expansion of the form

$$(2.8) \quad c(k) = \overbrace{c(r) \underbrace{0 \dots 0}_l c(r)},$$

where $l \geq 1$.

Passing on to the following kernel, we have:

$$c(k+1) = \overbrace{c(r+1) \underbrace{0 \dots 0}_{l-1} c(r+1)},$$

where $l-1 \geq 0$. Thus

$$c(k+1) = c(r+1)2^{2^m} + c(r+1) = c(r+1)F(m).$$

This completes formula (2.7). From this formula we conclude that $c(k+1)$ is a term of sequence $\{d(i)\}$. Moreover, since $c(k+1)$ contains $k+2$ binary digits, then, in view of property 1) of numbers $\{d(i)\}$, both of $c(k+1)$ and $d(k+1)$ contain $(k+2)$ binary digits. Therefore, $c(k+1) = d(k+1)$. ■

Remark 1. *In proof of Theorem 1, we essentially followed to our arguments from preprint [1], 1991.*

Denote $s(n)$ the number of 1's in the binary expansion of n .

Corollary 1. *a) Number of factors in Fermat factorization of $c(n)$ is $s(n)$.
b) Moreover, the following formula holds*

$$(2.9) \quad s(c(n)) = 2^{s(n)}.$$

Proof. a) follows from Theorem 1 and property 3) of numbers $\{d(n)\}$.

b) Let, firstly, $c(k)$ be not a Fermat number and, as in proof of Theorem 1, m be the most number for which $F(m)$ divides $c(k)$, such that $c(k) = F(m)c(r)$. Since the difference between numbers of factors in Fermat factorization of $c(k)$ and $c(r)$ is 1, then, according to a), we have

$$s(k) = s(r) + 1.$$

Now we use induction. If the statement is true for $i \leq k-1$, then, in particular, $s(c(r)) = 2^{s(r)}$. Therefore, by (2.8), we have

$$s(c(k)) = 2s(c(r)) = 2 \cdot 2^{s(r)} = 2^{s(r)+1} = 2^{s(k)}.$$

It is left to consider case $c(k) = F(l)$. Here, by a), $s(k) = 1$ and (2.9) satisfies trivially. ■

Corollary 2. *If $F(m)$ is the most Fermat divisor of numbers $c(k - 1)$ and $c(l - 1)$ from interval $(1, F(m) - 2)$, then*

$$(2.10) \quad c(k - 1)c(l) = c(l - 1)c(k).$$

Proof. Using (2.7), we have

$$c(k) = c(k - 1)F(m), \quad c(l) = c(l - 1)F(m)$$

and (2.10) follows. ■

Corollary 3. *If $n = 2^l + 2^{m-1}$, $m \geq 1$, then*

$$(2.11) \quad c(k) = c(2^{ml})F(m - 1).$$

Proof. From (2.1)-(2.2), we immediately have $d(k) = d(2^{ml})F(m - 1)$, and (2.11) follows from Theorem 1. ■

3. PROOF OF CONJECTURE 1

Now proof of Conjecture 1 is especially simple. Indeed, in view of (1.3) and (2.3), formula (1.4) of Conjecture 1 can be rewritten as

$$(3.1) \quad c(2^n) = F(n),$$

where $n = k + 1 \geq 1$.

According to Corollary 1a), number $c(2^n)$ has only one Fermat factor, i.e., for some t , we have $c(2^n) = F_t$. Besides, by the definition, $c(2^n)$ has $2^n + 1$ binary digits. It is left to notice that, the unique Fermat number having $2^n + 1$ binary digits is $F(n)$, i.e., $t = n$ and $c(2^n) = F(n)$. ■

In addition, prove that

$$(3.2) \quad c(2^n - 1) = F(n) - 2.$$

Indeed, by the definition of sequence $\{d(n)\}$ and (2.3), we conclude that $F(n) - 2$, as a product of *distinct* Fermat numbers, is a term of sequence $\{d(i)\}$ and thus, by Theorem 1, is a term of sequence $\{c(i)\}$. Now it is left to notice that numbers $c(2^n - 1)$ and $F(n) - 2$ have the same number (2^n) of binary digits. ■

4. PROOF OF CONJECTURES 2, 3, 4, etc.

Lemma 1. *For every $n \geq 0$, $t \geq 1$ we have identity*

$$(4.1) \quad (F(t-1) - 2)c(2^t n) = c(2^t n + 2^{t-1} - 1).$$

Proof. As in proof of (3.2), we conclude that $(F(t-1) - 2)c(2^t n)$ is a term of sequence $\{c(i)\}$. Note that number $c(2^t n + 2^{t-1} - 1)$ has $2^t n + 2^{t-1}$ binary digits. Besides, number $F(t-1) - 2 = \underbrace{1\dots 1}_{2^{t-1}}$ and $c(2^t n)$ has $2^t n + 1$ binary digits. Therefore, number $(F(t-1) - 2)c(2^t n)$ contains not less binary digits than number $\underbrace{1\dots 1}_{2^{t-1}} \underbrace{0\dots 0}_{2^t n}$, i.e. $(F(t-1) - 2)c(2^t n)$ has not less than $2^{t-1} + 2^t n$ binary digits. On the other hand, $(F(t-1) - 2)c(2^t n)$ contains not more binary digits than number

$$\underbrace{1\dots 1}_{2^{t-1}} \underbrace{1\dots 1}_{2^t n} = (2^{2^{t-1}} - 1)(2^{2^t n} - 1) \leq 2^{2^{t-1} + 2^t n} - 1,$$

i.e. $(F(t-1) - 2)c(2^t n)$ has not more than $2^{t-1} + 2^t n$ binary digits. Thus number $(F(t-1) - 2)c(2^t n)$ has exactly $2^{t-1} + 2^t n$ binary digits. Consequently, two terms $(F(t-1) - 2)c(2^t n)$ and $c(2^t n + 2^{t-1} - 1)$ of sequence $\{c(i)\}$ has the same number of digits. Therefore, equality (4.1) holds. ■

Lemma 2. *For every $n \geq 0$, $t \geq 1$ we have identities*

$$(4.2) \quad (F(t-1) - 2)c(2^t n + 2^{t-1}) = F(t-1)c(2^t n + 2^{t-1} - 1),$$

$$(4.3) \quad (F(t-1) - 2)c(2^t n + 2^{t-1}) = 3F(t-1)c(2^t n + 2^{t-1} - 2).$$

Proof. Multiplying (4.1) by $F(t-1)$ and using formula (2.11) of Corollary 3 (for $l = n$ and $m = t$), we obtain (4.2). Furthermore, if to take in Corollary 3 $m = 1$, $l = 2^{t-1}n + 2^{t-2} - 1$, then, in view of $F(0) = 3$, we have $c(2^t n + 2^{t-1} - 1) = 3c(2^t n + 2^{t-1} - 2)$, and (4.3) follows. ■

Now we are able to get a proof of Conjectures 2, 3, 4, *etc.* According to (1.3), we have

$$(4.4) \quad c(2n) = 4l(n) + 1.$$

Let in (4.3) $t \geq 2$. Then, by (4.4), we have

$$(F(t-1) - 2)(4l(2^{t-1}n + 2^{t-2}) + 1) = 3F(t-1)(4l(2^{t-1}n + 2^{t-2} - 1) + 1),$$

or

$$\frac{4l(2^{t-1}n + 2^{t-2}) + 1}{4l(2^{t-1}n + 2^{t-2} - 1) + 1} = \frac{3F(t-1)}{F(t-1) - 2}.$$

Hence, we finally find

$$(4.5) \quad \lim_{n \rightarrow \infty} \frac{l(2^{t-1}n + 2^{t-2})}{l(2^{t-1}n + 2^{t-2} - 1)} = \frac{3F(t-1)}{F(t-1) - 2}. \blacksquare$$

So, if $t = 2, 3, 4, 5, \dots$, then the right hand side is

$$\frac{3 \cdot 5}{5 - 2} = 5, \quad \frac{3 \cdot 17}{17 - 2} = \frac{17}{5}, \quad \frac{3 \cdot 257}{257 - 2} = \frac{257}{85}, \quad \frac{3 \cdot 65537}{65537 - 2} = \frac{65537}{21845}, \dots$$

correspondingly.

REFERENCES

- [1] . V. S. Shevelev, *On a combinatorial-analytical identity and some analogs of Euler formula for zeta-function*, Deposited in VINITI, no.3481-B91 (1991), 1-6 (in Russian).
- [2] . N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences* (<http://www.research.att.com>)
- [3] . E. Trost, *Primzahlen*, Birkhäuser-Verlag, 1953.

DEPARTMENTS OF MATHEMATICS, BEN-GURION UNIVERSITY OF THE NEGEV, BEER-SHEVA 84105, ISRAEL. E-MAIL:SHEVELEV@BGU.AC.IL

ON STEPHAN'S CONJECTURES CONCERNING PASCAL TRIANGLE MODULO 2

VLADIMIR SHEVELEV

ABSTRACT. We prove a series of Stephan's conjectures concerning Pascal triangle modulo 2 and give a polynomial generalization.

1. INTRODUCTION

Consider Pascal triangle for binomial coefficient modulo 2. If to read every row of this triangle as a binary number, then we obtain the following sequence $\{c(n)\}_{n \geq 0}$ (cf. A001317 in [9]):

$$(1.1) \quad 1, 3, 5, 15, 17, 51, 85, 255, 257, 771, 1285, 3855, 4369, 13107, 21845, \dots$$

It is easy to see that

$$(1.2) \quad c(2n) \equiv 1 \pmod{4}, \quad n = 0, 1, \dots$$

Denote

$$(1.3) \quad l(n) = \frac{c(2n) - 1}{4}.$$

In 2004, for sequence $\{l(n)\}_{n \geq 0}$, R. Stephan formulated a series of the following conjectures (cf. his comments to A089893 in [9]):

Conjecture 1.

$$(1.4) \quad l(2^k) = 2^{2^{k+1}-2}.$$

Conjecture 2.

$$(1.5) \quad \lim_{n \rightarrow \infty} l(2n+1)/l(2n) = 5.$$

Conjecture 3.

$$(1.6) \quad \lim_{n \rightarrow \infty} l(4n+2)/l(4n+1) = 17/5.$$

Conjecture 4.

$$(1.7) \quad \lim_{n \rightarrow \infty} l(8n+4)/l(8n+3) = 257/85.$$

etc.

We add that Moscow PhD student S. Shakirov conjectured (private communication) that a generating function for sequence $\{c(n)\}$ is

$$(1.8) \quad \prod_{k=0}^{\infty} (1 + x^{2^k} + (2x)^{2^k}) = \sum_{n=0}^{\infty} c(n)x^n.$$

In this paper we prove these conjectures.

2. ON SEQUENCE A001317

Consider an infinite in both sides $(0, 1)$ -sequence with a finite set of 1's which we call C -sequence. Removing in it all 0's before the first 1 and after the last 1, we obtain some odd number which we call the kernel of C -sequence. Every C -sequence generates a new C -sequence, if to write sums of every pair of its adjacent terms modulo 2. If to consider infinite iterations of such process beginning with C -sequence with kern 1, then we obtain C -sequences, the kernels $\{c(i)\}_{i \geq 0}$ of which form Pascal's triangle for binomial coefficients modulo 2. Note that, $c(0) = 1$ and $c(i)$ contains $i + 1$ binary digits.

Consider now sequence $\{d(n)\}$ defined by the formula $d(0) = 1$; for $n \geq 1$, if binary expansion of n is

$$(2.1) \quad n = \sum_{i=1}^m 2^{k_i},$$

then

$$(2.2) \quad d(n) = \prod_{i=1}^m F(k_i),$$

where

$$(2.3) \quad F(n) = 2^{2^n} + 1, \quad n \geq 0,$$

is Fermat number. Such decomposition of $d(n)$ we call its *Fermat factorization*.

From (2.1)-(2.2) immediately follows a generating function for $\{d(i)\}$:

$$(2.4) \quad \prod_{k=0}^{\infty} (1 + F(k)x^{2^k}) = \sum_{n=0}^{\infty} d(n)x^n, \quad 0 < x < \frac{1}{2}.$$

Note that sequence $\{d(i)\}$ possesses the following properties:

- 1) $d(n)$ is a binary number with $n + 1$ $(0, 1)$ -digits;
- 2) numbers $\{d(i)\}$ are 1 and all Fermat numbers or products of distinct Fermat numbers;

3) number of Fermat factors in the product equals to $d(n)$ is the number of 1's in the binary expansion of n .

4) $F(i)$ divides $d(n)$, $n > 1$, if and only if it is a factor in product (2.2).

Proofs of these properties is very easy: 1) follows from a simple induction; 2) and 3) follow from the definition; 4) follows from the well known fact (cf., e.g., [10]) that every two Fermat numbers are relatively prime, in view of recursion

$$(2.5) \quad F(n) = 2 + \prod_{i=0}^{n-1} F(i).$$

Theorem 1. For $n = 0, 1, \dots$, we have

$$(2.6) \quad c(n) = d(n).$$

Proof. We use induction, the base of which is $c(0) = d(0) = 1$, $c(1) = d(1) = 3$, $c(2) = d_2 = 5$. Suppose that $c(i) = d(i)$, for $i \leq k$. Let m be the most number for which $F(m)$ divides $c(k) = d(k)$. In non-trivial case, when $c(k) \neq F(m)$, using property 4), for some $r < k$, we have $c(k) = d(r)F(m) = c(r)F(m)$. Furthermore, since, by the condition, $F(m)$ is the most Fermat divisor of $c(k)$ and, in view of (2.5), we have

$$(2.7) \quad c(r) = \frac{c(k)}{F(m)} \leq \prod_{i=0}^{m-1} F(i) = F(m) - 2.$$

Besides, since $c(r) < c(k)$, then, by the inductive supposition,

$$c(r + 1) = d(r + 1).$$

Adding the case when $c(k) = F(m)$, let us prove a recursion: $c(0) = 1, c(1) = 3, c(2) = 5$; for $k \geq 2$,

$$(2.8) \quad c(k + 1) = \begin{cases} 3F(m), & \text{if } c(k) = F(m), \\ F(m + 1), & \text{if } 1 < c(r) = F(m) - 2, \\ F(m)c(r + 1), & \text{if } 1 < c(r) < F(m) - 2. \end{cases}$$

Let $c(k) = F(m)$, $m \geq 1$. C -sequence with kernel $c(k)$ is

$$\dots 01 \underbrace{0 \dots 0}_{2^m - 1} 10 \dots$$

Thus the following C -sequence with kernel $c(k + 1)$ is

$$\dots 011 \underbrace{0 \dots 0}_{2^m - 2} 110 \dots$$

Comparing kernels $c(k)$ and $c(k + 1)$, we conclude that $c(k + 1) = 3c(k) = 3F(m)$.

Furthermore, if $c(r) = F(m) - 2$, then, by (2.7), we have

$$c(k) = F(m)c(r) = F(m)(F(m) - 2) = F(m + 1) - 2 = \underbrace{11\dots1}_{2^{m+1}}.$$

Thus the C -sequence with kernel $c(k)$ is

$$\dots 0 \underbrace{11\dots1}_{2^{m+1}} 0 \dots$$

Therefore, by the definition, the C -sequence with kernel $c(k + 1)$ is

$$\dots 01 \underbrace{0\dots0}_{2^{m+1}-1} 10 \dots$$

and we see that $c(k + 1) = F(m + 1)$.

Let now $c(r) < F(m) - 2$. Since, by the supposition of induction, $c(r) = d(r)$. Therefore, $c(r)$ is a product of Fermat numbers and

$$c(r) \leq \frac{\prod_{i=0}^{m-1} F(i)}{F(0)} = \frac{F(m) - 2}{F(0)}.$$

Hence, $c(r)$ is not more than $(2^m - 1)$ -digits odd binary number. Since

$$c(k) = F(m)c(r) = 2^{2^m} c(r) + c(r),$$

then $c(k)$ has the binary expansion of the form

$$(2.9) \quad c(k) = \overline{c(r) \underbrace{0\dots0}_l c(r)},$$

where $l \geq 1$.

Passing on to the following kernel, we have:

$$c(k + 1) = \overline{c(r + 1) \underbrace{0\dots0}_{l-1} c(r + 1)},$$

where $l - 1 \geq 0$. Thus

$$c(k + 1) = c(r + 1)2^{2^m} + c(r + 1) = c(r + 1)F(m).$$

This completes formula (2.8). From this formula we conclude that $c(k + 1)$ is a term of sequence $\{d(i)\}$. Moreover, since $c(k + 1)$ contains $k + 2$ binary digits, then, in view of property 1) of numbers $\{d(i)\}$, both of $c(k + 1)$ and $d(k + 1)$ contain $(k + 2)$ binary digits. Therefore, $c(k + 1) = d(k + 1)$. ■

Remark 1. *In proof of Theorem 1, we essentially followed to our arguments from preprint [7], 1991.*

Corollary 1. *Conjectural generating formula (1.8) is true.*

Proof. According to (2.4) and Theorem 1, we have

$$(2.10) \quad \prod_{k=0}^{\infty} (1 + F(k)x^{2^k}) = \sum_{n=0}^{\infty} c(n)x^n, \quad 0 < x < \frac{1}{2}.$$

It is left to notice that

$$1 + F(k)x^{2^k} = 1 + x^{2^k} + (2x)^{2^k}. \blacksquare$$

Denote $s(n)$ the number of 1's in the binary expansion of n .

Corollary 2. a) *Number of factors in Fermat factorization of $c(n)$ is $s(n)$.*
 b) *Moreover, the following formula holds*

$$(2.11) \quad s(c(n)) = 2^{s(n)}.$$

Proof. a) follows from Theorem 1 and property 3) of numbers $\{d(n)\}$.

b) Let, firstly, $c(k)$ be not a Fermat number and, as in proof of Theorem 1, m be the most number for which $F(m)$ divides $c(k)$, such that $c(k) = F(m)c(r)$. Since the difference between numbers of factors in Fermat factorization of $c(k)$ and $c(r)$ is 1, then, according to a), we have

$$s(k) = s(r) + 1.$$

Now we use induction. If the statement is true for $i \leq k - 1$, then, in particular, $s(c(r)) = 2^{s(r)}$. Therefore, by (2.9), we have

$$s(c(k)) = 2s(c(r)) = 2 \cdot 2^{s(r)} = 2^{s(r)+1} = 2^{s(k)}.$$

It is left to consider case $c(k) = F(l)$. Here, by a), $s(k) = 1$ and (2.9) satisfies trivially. \blacksquare

Note that point b) of Corollary 2 means that the number of odd binomial coefficient in n -th row of Pascal triangle is $2^{s(n)}$. It is known result of J.Glaisher [2]. His proof was based on well known Lucas (1878) comparison modulo 2: if the binary representations of numbers $m \geq t$ are $m = \overline{m_1 \dots m_k}$, $t = \overline{t_1 \dots t_k}$ (with, probably, some first $t_i = 0$), then

$$\binom{n}{t} \equiv \prod_{i=0}^m \binom{n_i}{t_i} \pmod{2}.$$

In [3] A.Granville gives a new interesting proof of Glaisher's result. Our proof is the third one. Generalizations in other directs see in [1], [3], [4], [6], [8].

Corollary 3. *If $F(m)$ is the most Fermat divisor of numbers $c(k - 1)$ and $c(l - 1)$ from interval $(1, F(m) - 2)$, then*

$$(2.12) \quad c(k - 1)c(l) = c(l - 1)c(k).$$

Proof. Using (2.8), we have

$$c(k) = c(k - 1)F(m), \quad c(l) = c(l - 1)F(m)$$

and (2.12) follows. ■

Corollary 4. *If $k = 2^m l + 2^{m-1}$, $m \geq 1$, then*

$$(2.13) \quad c(k) = c(2^m l)F(m - 1).$$

Proof. From (2.1)-(2.2), we immediately have $d(k) = d(2^m l)F(m - 1)$, and (2.13) follows from Theorem 1. ■

3. PROOF OF CONJECTURE 1

Now proof of Conjecture 1 is especially simple. Indeed, in view of (1.3) and (2.3), formula (1.4) of Conjecture 1 can be rewritten as

$$(3.1) \quad c(2^n) = F(n),$$

where $n = k + 1 \geq 1$.

According to Corollary 1a), number $c(2^n)$ has only one Fermat factor, i.e., for some t , we have $c(2^n) = F_t$. Besides, by the definition, $c(2^n)$ has $2^n + 1$ binary digits. It is left to notice that, the unique Fermat number having $2^n + 1$ binary digits is $F(n)$, i.e., $t = n$ and $c(2^n) = F(n)$. ■

In addition, prove that

$$(3.2) \quad c(2^n - 1) = F(n) - 2.$$

Indeed, by the definition of sequence $\{d(n)\}$ and (2.3), we conclude that $F(n) - 2$, as a product of *distinct* Fermat numbers, is a term of sequence $\{d(i)\}$ and thus, by Theorem 1, is a term of sequence $\{c(i)\}$. Now it is left to notice that numbers $c(2^n - 1)$ and $F(n) - 2$ have the same number (2^n) of binary digits. ■

4. PROOF OF CONJECTURES 2, 3, 4, etc.

Lemma 1. *For every $n \geq 0$, $t \geq 1$ we have identity*

$$(4.1) \quad (F(t - 1) - 2)c(2^t n) = c(2^t n + 2^{t-1} - 1).$$

Proof. As in proof of (3.2), we conclude that $(F(t - 1) - 2)c(2^t n)$ is a term of sequence $\{c(i)\}$. Note that number $c(2^t n + 2^{t-1} - 1)$ has $2^t n + 2^{t-1}$ binary digits. Besides, number $F(t - 1) - 2 = \underbrace{1 \dots 1}_{2^{t-1}}$ and $c(2^t n)$ has $2^t n + 1$ binary digits. Therefore, number $(F(t - 1) - 2)c(2^t n)$ contains not less binary digits than number

$\underbrace{1\dots 1}_{2^{t-1}}\underbrace{0\dots 0}_{2^t n}$, i.e. $(F(t-1) - 2)c(2^t n)$ has not less than $2^{t-1} + 2^t n$ binary digits. On the other hand, $(F(t-1) - 2)c(2^t n)$ contains not more binary digits than number

$$\underbrace{1\dots 1}_{2^{t-1}}\underbrace{1\dots 1}_{2^t n} = (2^{2^{t-1}} - 1)(2^{2^t n} - 1) \leq 2^{2^{t-1} + 2^t n} - 1,$$

i.e. $(F(t-1) - 2)c(2^t n)$ has not more than $2^{t-1} + 2^t n$ binary digits. Thus number $(F(t-1) - 2)c(2^t n)$ has exactly $2^{t-1} + 2^t n$ binary digits. Consequently, two terms $(F(t-1) - 2)c(2^t n)$ and $c(2^t n + 2^{t-1} - 1)$ of sequence $\{c(i)\}$ has the same number of digits. Therefore, equality (4.1) holds. ■

Lemma 2. *For every $n \geq 0$, $t \geq 1$ we have identities*

$$(4.2) \quad (F(t-1) - 2)c(2^t n + 2^{t-1}) = F(t-1)c(2^t n + 2^{t-1} - 1),$$

$$(4.3) \quad (F(t-1) - 2)c(2^t n + 2^{t-1}) = 3F(t-1)c(2^t n + 2^{t-1} - 2).$$

Proof. Multiplying (4.1) by $F(t-1)$ and using formula (2.13) of Corollary 4 (for $l = n$ and $m = t$), we obtain (4.2). Furthermore, if to take in Corollary 4 $m = 1$, $l = 2^{t-1}n + 2^{t-2} - 1$, then, in view of $F(0) = 3$, we have $c(2^t n + 2^{t-1} - 1) = 3c(2^t n + 2^{t-1} - 2)$, and (4.3) follows. ■

Now we are able to get a proof of Conjectures 2, 3, 4, *etc.* According to (1.3), we have

$$(4.4) \quad c(2n) = 4l(n) + 1.$$

Let in (4.3) $t \geq 2$. Then, by (4.4), we have

$$(F(t-1) - 2)(4l(2^{t-1}n + 2^{t-2}) + 1) = 3F(t-1)(4l(2^{t-1}n + 2^{t-2} - 1) + 1),$$

or

$$\frac{4l(2^{t-1}n + 2^{t-2}) + 1}{4l(2^{t-1}n + 2^{t-2} - 1) + 1} = \frac{3F(t-1)}{F(t-1) - 2}.$$

Hence, we finally find

$$(4.5) \quad \lim_{n \rightarrow \infty} \frac{l(2^{t-1}n + 2^{t-2})}{l(2^{t-1}n + 2^{t-2} - 1)} = \frac{3F(t-1)}{F(t-1) - 2}. \blacksquare$$

So, if $t = 2, 3, 4, 5, \dots$, then the right hand side is

$$\frac{3 \cdot 5}{5 - 2} = 5, \quad \frac{3 \cdot 17}{17 - 2} = \frac{17}{5}, \quad \frac{3 \cdot 257}{257 - 2} = \frac{257}{85}, \quad \frac{3 \cdot 65537}{65537 - 2} = \frac{65537}{21845}, \dots$$

correspondingly.

5. SECOND PROOF OF KEY IDENTITY (4.3) BASED ON NOTION OF ORTHOGONALITY OF NONNEGATIVE INTEGERS

We can essentially simplify our proof of Stephan's conjectures by a simplification of key identity (4.3). Put to every nonnegative integer n to one-to-one correspondence $(0, 1)$ -vector \bar{n} by the rule: if the binary expansion of n is $n = \overline{n_1 \dots n_m}$, then

$$(5.1) \quad \bar{n} = \overline{\dots 0 \dots 0 n_1 \dots n_m}$$

with infinitive 0's before n_1 . For two integers $u \leq v$ with vectors $\bar{u} = \overline{\dots 0 \dots 0 u_1 \dots u_l}$ and $\bar{v} = \overline{\dots 0 \dots 0 v_1 \dots v_m}$, $l \leq m$ introduce "circ-product" by formula (which is, for the corresponding vectors, similar to dot-product)

$$(5.2) \quad u \circ v = \overline{uv} = u_l v_m + u_{l-1} v_{m-1} + \dots + u_1 v_{m-l+1}.$$

Definition 1. We call two non-negative integers u, v mutually orthogonal ($u \perp v$), if $u \circ v = 0$.

Note that if $(u \perp v)$, then the sets of positions of 1's in their binary representations do not intersect.

An important source for obtaining various identities for numbers $\{c(n)\}$ is the following exponential-like "addition theorem".

Lemma 3. If $n_1 \perp n_2$, then

$$(5.3) \quad c(n_1 + n_2) = c(n_1)c(n_2).$$

Proof. Let $n_1 \geq n_2$ and the binary expansions of n_1 and n_2 be $n_1 = \sum_{i=1}^m 2^{k_i}$ and $n_2 = \sum_{j=1}^m 2^{l_j}$ (with, probably, some first $l_i = 0$). Since $n_1 \perp n_2$, then $k_i \neq l_j$, $i, j = 1, \dots, m$. Thus the binary expansion of $n_1 + n_2$ is $\sum_{i=1}^m 2^{k_i} + \sum_{j=1}^m 2^{l_j}$. Therefore, according to (2.1)-(2.2), we have

$$c(n_1 + n_2) = \left(\prod_{i=1}^m F(k_i)\right) \left(\prod_{j=1}^m F(l_j)\right) = c(n_1)c(n_2). \blacksquare$$

Second proof of (4.3).

a)Using the notion of numbers orthogonality, we immediately obtain formula (4.2) by the following way.

By (3.2), we have

$$(5.4) \quad F(t - 1) - 2 = c(2^{t-1} - 1).$$

Since, evidently, $(2^{t-1} - 1) \perp (2^t n + 2^{t-1})$, then, using (5.3)-(5.4), we find

$$(F(t - 1) - 2)c(2^t n + 2^{t-1}) = c(2^t n + 2^{t-1} + 2^{t-1} - 1) = c(2^t n + 2^t - 1).$$

On the other hand, since $2^{t-1} \perp (2^t n + 2^{t-1} - 1)$, then

$$F(t-1)c(2^t n + 2^{t-1} - 1) = c(2^{t-1})c(2^t n + 2^{t-1} - 1) = c(2^t n + 2^t - 1).$$

Thus we conclude that (4.2) holds.

b) Note now that, $1 \perp 2^t n + 2^t - 2$. Thus $3c(2^t n + 2^{t-1} - 2) = c(2^t n + 2^{t-1} - 1)$ and (4.3) follows as well. ■

Further we consider a polynomial generalization.

6. POLYNOMIALS $p_n(z)$, $q_n(z)$ AND THEIR PROPERTIES

Consider sequence of polynomials (cf.[3])

$$(6.1) \quad p_n(z) = \frac{1}{2} \sum_{i=0}^n (1 - (-1)^{\binom{n}{i}}) z^i, \quad n = 0, 1, \dots, \quad z \in \mathbb{C},$$

such that

$$(6.2) \quad p_n(0) = 1, \quad p_n(1) = 2^{s(n)}, \quad p_n(2) = c(n).$$

The second equality we have in view of (2.9).

By the same way, one can prove a generalization of Theorem 1.

Theorem 2. *For $n \geq 1$, we have the following decomposition of $p_n(z)$:*

$$(6.3) \quad p_n(z) = \prod_{i=0}^m (z^{2^{k_i}} + 1),$$

if the binary expansion of n is

$$(6.4) \quad n = \sum_{i=0}^m 2^{k_i}.$$

Thus a generating function for polynomials $\{p_n(z)\}$ is

$$(6.5) \quad \prod_{k=0}^{\infty} (1 + (z^{2^k} + 1)x^{2^k}) = \sum_{n=0}^{\infty} p_n(z)x^n, \quad 0 < x < \frac{1}{|z|}.$$

In particular, we have

$$(6.6) \quad p_{2^n}(z) = z^{2^n} + 1.$$

Note that, if n has binary expansion (6.4), then $2n = \sum_{i=0}^m 2^{k_i+1}$. Since $z^{2^{k_i+1}} = (z^2)^{2^{k_i}}$, then we have

$$(6.7) \quad p_{2n}(z) = \prod_{i=0}^m ((z^2)^{2^{k_i}} + 1) = p_n(z^2).$$

Analogously, since $2n + 1 = 1 + \sum_{i=0}^m 2^{k_i+1}$, then

$$(6.8) \quad p_{2n+1}(z) = (z + 1) \prod_{i=0}^m ((z^2)^{2^{k_i}} + 1) = (z + 1)p_n(z^2).$$

Formulas (6.7)-(6.8) give a simple recursion for polynomials $\{p_n(z)\}$, which recently were obtained by S. Northshield (cf. [5], Lemma 3.1) by quite another way.

Note that every two different polynomials in sequence $\{p_{2^i}(z) = z^{2^i} + 1\}_{i \geq 0}$ are respectively prime. It follows from the identity

$$(6.9) \quad p_{2^n}(z) = 2 + (z - 1) \prod_{i=0}^{n-1} p_{2^i}(z).$$

Put

$$(6.10) \quad F_n(z) = p_{2^n}(z) = z^{2^n} + 1.$$

The following identity holds (cf. [7])

$$(6.11) \quad \sum_{n=0}^{\infty} \frac{1}{p_n(z)^s} = \prod_{k=0}^{\infty} (1 + F_k(z)^{-s}), \quad |z| > 1, \quad \Re s > 0.$$

In particular, for $z = 2$, $s = 1$, we have

$$(6.12) \quad \sum_{n=0}^{\infty} \frac{1}{c(n)} = \prod_{k=0}^{\infty} (1 + F_k^{-1}) = 1.700735495\dots$$

According to Theorem 2 and in view that $s(n) \equiv m_n \pmod{2}$, where $m_n = 0, 1, 1, 0, 1, 0, 0, 1, 1, \dots$ is Thou-Morse sequence, together with (6.11), we have also

$$(6.13) \quad \sum_{n=0}^{\infty} \frac{(-1)^{m_n}}{p_n(z)^s} = \prod_{k=0}^{\infty} (1 - F_k(z)^{-s}), \quad |z| > 1, \quad \Re s > 0.$$

Let us show that, in particular, for $s = 1$, we have

$$(6.14) \quad \sum_{n=0}^{\infty} \frac{(-1)^{m_n}}{p_n(z)} = 1 - \frac{1}{z}, \quad |z| > 1.$$

Indeed, since

$$1 - \frac{1}{F_n(z)} = \left(1 + \frac{1}{z^{2^n}}\right)^{-1},$$

then

$$\prod_{k=0}^{\infty} (1 - F_k(z)^{-1}) = \prod_{k=0}^{\infty} \left(1 + \frac{1}{z^{2^k}}\right)^{-1}$$

and it is left to note that

$$(6.15) \quad \prod_{n=0}^{\infty} \left(1 + \frac{1}{z^{2^n}}\right) = 1 - \frac{1}{z}.$$

In particular, together with (6.12), for $z = 2$, we find

$$(6.16) \quad \sum_{n=0}^{\infty} \frac{(-1)^{m_n}}{c(n)} = \frac{1}{2}.$$

In addition, note that, if to consider all different finite products of not necessarily distinct polynomials from sequence $\{p_n(z)\}$, then we obtain a sequence of polynomials $q_n(z)$:

$$(6.17) \quad \begin{aligned} q_0(z) &= 1, \quad q_1(z) = z + 1, \quad q_2(z) = z^2 + 1, \quad q_3(z) = (z + 1)^2, \\ q_4(z) &= (z + 1)(z^2 + 1), \quad q_5(z) = z^4 + 1, \quad q_6(z) = (z^2 + 1)^2. \end{aligned}$$

For these polynomials, together with (6.11), we have the following analog of Euler identity for primes:

$$(6.18) \quad \prod_{F \in F(z)} (1 - F^{-s})^{-1} = \sum_{n=0}^{\infty} \frac{1}{q_n(z)^s}, \quad |z| > 1, \quad \Re s > 0,$$

where

$$F(z) = \{F_n(z)\}_{n \geq 0}.$$

In particular, for $s = 1$, using (6.15), we have

$$(6.19) \quad \begin{aligned} \sum_{n=0}^{\infty} \frac{1}{q_n(z)} &= \prod_{F \in F(z)} (1 - F^{-1})^{-1} = \\ &= \prod_{n=0}^{\infty} \left(1 + \frac{1}{z^{2^n}}\right)^{-1} = \frac{z}{z-1}, \quad |z| > 1. \end{aligned}$$

Furthermore, introducing an analog of Möbius function

$$(6.20) \quad \nu(n) = \begin{cases} (-1)^{m_n}, & \text{if } n \text{ is squarefree,} \\ 0, & \text{otherwise,} \end{cases}$$

we get

$$(6.21) \quad \sum_{n=0}^{\infty} \frac{\nu(n)}{q_n(z)^s} = \prod_{F \in F(z)} (1 - F^{-s}), \quad |z| > 1, \quad \Re s > 0.$$

In particular, for $s = 1$, we have

$$(6.22) \quad \sum_{n=0}^{\infty} \frac{\nu(n)}{q_n(z)} = 1 - \frac{1}{z}, \quad |z| > 1.$$

7. POLYNOMIAL GENERALIZATION

Now we consider a polynomial generalization of formulas of the previous sections which leads us to the corresponding generalization of the Stephan's relations. Since proof of the generalized formulas is quite analogous, then we restrict ourself only by writing of the chain of them. For $|z| > 1$, we have

$$(7.1) \quad p_{2^n-1} = \frac{F_n(z) - 2}{z - 1}.$$

This formula generalizes (3.2). Furthermore, the following generalization of (2.13) holds:

$$(7.2) \quad p_{2^m l + 2^{m-1}}(z) = p_{2^m l}(z) F_{m-1}(z).$$

In particular, taking in (7.2) $m = 1$, $l = 2^{t-1}n + 2^{t-2} - 1$, in view of $F_0(z) = z + 1$, we find

$$(7.3) \quad p_{2^t n + 2^{t-1} - 1}(z) = (z + 1) p_{2^t n + 2^{t-1} - 2}(z).$$

After that the corresponding generalization of formulas (4.1)-(4.3) is obtained:

$$(7.4) \quad (F_{t-1}(z) - 2) p_{2^t n}(z) = p_{2^t n + 2^{t-1} - 1}(z),$$

$$(7.5) \quad (F_{t-1}(z) - 2) p_{2^t n + 2^{t-1}}(z) = (z - 1) F_{t-1}(z) p_{2^t n + 2^{t-1} - 1}(z),$$

$$(7.6) \quad (F_{t-1}(z) - 2) p_{2^t n + 2^{t-1}}(z) = (z^2 - 1) F_{t-1}(z) p_{2^t n + 2^{t-1} - 2}(z).$$

Note that

$$(7.7) \quad p_{2n}(z) \equiv 1 \pmod{z^2}.$$

Put

$$(7.8) \quad l_n(z) = \frac{p_{2n}(z) - 1}{z^2}.$$

Let in (7.6) $t \geq 2$. Then we have

$$(7.9) \quad (F_{t-1}(z) - 2)(z^2 l_{2^{t-1}n + 2^{t-2}}(z) + 1) = (z^2 - 1) F_{t-1}(z) (z^2 l_{2^{t-1}n + 2^{t-2} - 1}(z) + 1),$$

or

$$(7.10) \quad \frac{z^2 l_{2^{t-1}n + 2^{t-2}}(z) + 1}{z^2 l_{2^{t-1}n + 2^{t-2} - 1}(z) + 1} = \frac{(z^2 - 1) F_{t-1}(z)}{F_{t-1}(z) - 2}$$

and, consequently,

$$(7.11) \quad \lim_{n \rightarrow \infty} \frac{l_{2^{t-1}n + 2^{t-2}}(z)}{l_{2^{t-1}n + 2^{t-2} - 1}(z)} = \frac{(z^2 - 1) F_{t-1}(z)}{F_{t-1}(z) - 2}.$$

In particular, for $t = 2$,

$$\lim_{n \rightarrow \infty} \frac{l_{2n+1}(z)}{l_{2n}(z)} = z^2 + 1;$$

for $t = 3$,

$$\lim_{n \rightarrow \infty} \frac{l_{4n+2}(z)}{l_{4n+1}(z)} = \frac{z^4 + 1}{z^2 + 1};$$

for $t = 4$,

$$\lim_{n \rightarrow \infty} \frac{l_{8n+4}(z)}{l_{8n+3}(z)} = \frac{z^8 + 1}{(z^4 + 1)(z^2 + 1)}, \text{ etc.}$$

REFERENCES

- [1] . W. B. Everett, *Number of binomial coefficients divisible by a fixed power of a prime*, INTEGERS, **8** (2008), #A11.
- [2] . J. Glaisher, *On the residue of a binomial-theorem coefficient with respect to a prime modulus*, Quarterly J. of Pure and Applied Math., **30** (1899), 150-156.
- [3] . A. Granville, *Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's triangle*, Amer. Math. Monthly, **99** , no. 4 (1992), 318-331; **104** , no. 9 (1997), 848-851.
- [4] . J. G. Huard, B. K. Spearman, K. S. Williams , *Pascal's triangle (mod 8)* , Europ. J. Combin., **19** , no.1 (1998), 45-62.
- [5] . S. Northshield, *Sums across Pascal's triangle modulo 2*, Congressus Numerantium, **200** (2010), 35-52.
- [6] . E. S. Rowland, *The number of nonzero binomial coefficients modulo p^α* , arXiv: 1001.1783v2 (2010).
- [7] . V. S. Shevelev, *On a combinatorial-analytical identity and some analogs of Euler formula for zeta-function*, Deposited in VINITI, no. 3481-B91 (1991), 1-6 (in Russian).
- [8] . V. Shevelev, *Binomial predictors*, arXiv: 0907.3302v4 (2009)
- [9] . N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences* (<http://www.research.att.com>)
- [10] .E. Trost, *Primzahlen* Birkhäuser-Verlag, 1953.

DEPARTMENTS OF MATHEMATICS, BEN-GURION UNIVERSITY OF THE NEGEV, BEER-SHEVA 84105, ISRAEL. E-MAIL:SHEVELEV@BGU.AC.IL