ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

LIX 1974 1

УДК 511.2

МАТЕМАТИКА

Ю. А. Трахтман

О делимости некоторых разностей, составленных из биномиальных коэффициентов

(Представлено чл.-корр. АН Армянской ССР Р. А. Александряном 25/II 1974)

В статье Д. Б. Фукс и М. Б. Фукс [1] поставили вопрос о том, на какую степень числа m делится выражение $a_n(m) = \binom{m^{n+1}}{m^n} - \binom{m^n}{m^{n-1}}$ в случае, когда m просто. Они доказали, что $a_n(2)$ делится на 2^{4n+2} при $n>1$ и, на основе анализа числовых примеров, высказали следующие предположения.

1. $a_n(2)$ при $n>1$ делится на 2^{4n}.

2. Если p просто, то $a_n(p)$ также делится на высокую степень числа p.

3. Если число m является составным, то $a_n(m)$ не делится на высокую степень числа m.

В настоящей статье доказывается следующая

Теорема 1. *Для любого простого p и любого натурального l имеет место сравнение*

$$a_n(p^l) \equiv \begin{cases} B_{p-3}\, p^{l(3n-1)+3}/3 \mod p^{l(3n-1)+4} & \text{при } p>3 \\ 3^{l(3n-1)+2} \mod 3^{l(3n-1)+3} & \text{при } p=3 \\ 2^{l(3n-1)+1} \mod 2^{l(3n-1)+2} & \text{при } p=2,\ n>1 \\ 2^{l+1} \mod 2^{l+2} & \text{при } p=2,\ n=1 \end{cases}$$

Здесь B_{p-3} есть $(p-3)$-е число Бернулли (нумерация четная, то есть $B_0=1$, $B_1=1/2, \ldots$).

Следствие 1. *$a_n(p)$ при $p>3$ делится на p^{3n-1}, $a_n(3)$ делится на 3^{3n+1} и $a_n(2)$ при $n>1$ делится на 2^{3n}.*

Следствие 2. *Пусть m — степень простого числа, причем $m \neq 2^l$ при $n=1$. Тогда $a_n(m)$ делится на m^{3n-1}.*

Следствие 1 доказывает первые два из указанных предположе-

ний, а следствие 2 показывает, что третье предположение неверно, по крайней мере для случая, когда m есть степень простого числа.

Из теоремы следует, что $a_n(2^l)$ при $n>1$ делится точно на $|l(3n-1)+1|$-ю степень двойки, а $a_n(3^l)$ — на $|l(3n-1)+2|$-ю степень тройки. Ответ на вопрос, будет ли $a_n(p^l)$ при любом $p>3$ делиться точно на $|l(3n-1)+3|$-ю степень числа p зависит от того, может ли делиться на p числитель дроби B_{p-3}. По этому поводу можно сказать лишь, что подобная делимость не имеет места для чисел, регулярных в смысле Куммера. Кроме того, из таблиц (см. [2], стр. 561) можно заключить, что $B_{p-3} \not\equiv 0 \bmod p$ для простых $p \leqslant 4001$.

Доказательство теоремы. Положим $c_k\binom{p^{lk}}{p^{l(k-1)}\ i}$, $s_k(m)=\sum_{i=1}^{m} i^k$, $\sum i^k=\sum_k(m)$, $\prod i=\Pi(m)$, где в двух последних случаях i пробегает те натуральные числа $\leqslant m$, которые не делятся на p; через φ, как обычно, обозначается функция Эйлера. Обозначим, далее, через $P_i(\xi)$ следующую функцию целочисленного аргумента:

$$P_i(\xi)=\frac{\Pi(\xi)}{\Pi(\xi-p^{n_i})}, \tag{1}$$

где $n_i=ln-l+i$, $1\leqslant i\leqslant l$, $\xi>p^{ln}$. Очевидно,

$$a_n(p^l)=c_{n+1}-c_n=c_n\left(\frac{c_{n+1}}{c_n}-1\right). \tag{2}$$

Покажем, что

$$\frac{c_{n+1}}{c_n}=\prod_{i=1}^{l}\frac{P_i(x_i)}{\Pi(p^{n_i})}, \quad \text{где} \quad x_i=p^{ln+i}, \tag{3}$$

Действительно, легко усмотреть, что

$$(p^lm)!=m!\,p^{ms_l}\prod_{i=1}^{l}|\Pi(^l_m)|, \tag{4}$$

где $s_l=1+p+\ldots+p^{l-1}$; используя (4) с $m=p^{ln}$, p^{ln-l}, $p^{ln}-p^{ln-l}$, получаем:

$$\frac{c_{n+1}}{c_n}=\frac{p^{ln+l}!\,p^{ln-l}!\,(p^{ln}-p^{ln-l})!}{p^{ln}!\,(^{ln+l}-p^{ln}!\,p^{ln}!}=\prod_{i=1}^{l}\frac{\Pi(p^{ln-l+i})}{\Pi(p^{ln-l+i})\Pi(p^{ln+i}-p^{ln-l+i})}.$$

Отсюда, с учетом (1), получим (3).

Так как x_i делится на p, то из (1) следует, что

$$P(x_i)=(x_i-1)\ldots(x_i-p^{n_i}+1)=(-1)^{\varphi(p^{n_i})}a_{0i}-a_{1i}x_i+a_{2i}x_i^2-\ldots),$$

где количество скобок в произведении равно $\varphi(p^{n_i})$. Следовательно,

$$a_{0i}=\Pi(p^{n_i}),\ a_{1i}=a_{0i}\Sigma_{-1}(p^{n_i}),$$

$$a_{2i}=\frac{1}{2}\,a_{0i}\left|(\Sigma_{-1}(p^{n_i}))^2-\Sigma_{-2}(p^{n_i})\right|. \tag{5}$$

Формулу (3) можно теперь переписать в виде

$$\frac{c_{n+1}}{c_n} = \prod_{i=1}^{l} \frac{P_i(x_i)}{a_{0i}} \tag{6}$$

Так как $\varphi(p^{n_i}) = p^{n_i-1}(p-1)$ является нечетным только при $p=2$, $n_i=1$, а $n_i = l(n-1)+i$, то в этом случае $n=i=1$, $x_i = x_1 = 2^{l+1}$, $a_{0i} = a_{01} = 1$, $P_i(x_i) = P_1(x_1) = 2^{l+1}-1$, то есть

$$P_1(x_1) = 2^{l+1}-1 \quad \text{при} \quad p=2,\ n=1 \tag{7}$$

Исключая случай $n=1$, $p=2$, $i=1$, имеем:

$$P_i(x_i) = a_{0i} - a_{1i}x_i + a_{2i}x_i^2 - \dots$$

Отсюда $P_i(x_i) \equiv a_{0i} - a_{1i}x_i + a_{2i}x_i^2 \mod x_i^3$, то есть

$$P_i(x_i) - a_{0i} = a_{1i}p^{ln+i} + a_{2i}p^{2ln+2i} \pmod{p^{3ln+3i}} \tag{8}$$

Для дальнейшего нам понадобятся две леммы (их доказательство приведено в конце заметки):

Лемма 1:

$$\sum_{n-1}(p^n) \equiv \begin{cases} \frac{2}{3}B_{p-3}\,p^n \pmod{p^{n+1}} & \text{при } p>3, \\ -p^{n-1} \pmod{p^n} & \text{при } p=2,3. \end{cases}$$

Лемма 2:

$$\sum_{n-1}(p^n) \equiv \begin{cases} -\frac{1}{3}B_{p-3}\,p^{2n} \pmod{p^{2n+1}} & \text{при } p>3, \\ -3^{2n-1} \pmod{3^{2n}} & \text{при } p=3, \\ 2^{2n-2} \pmod{2^{2n-1}} & \text{при } p=2. \end{cases}$$

При доказательстве теоремы мы ограничиваемся случаем $p>3$; доказательство в случаях $p=2,3$ аналогично (в случае $p=2$, $n=1$ вместо (8) используется (7)).

В силу формулы (5) и лемм 1, 2,

$$a_{2i} \equiv 0 \mod p^{n_i}$$

$$a_{1i} \equiv -\frac{1}{3}a_{0i}B_{p-3}\,p^{2n_i} \mod p^{3n_i-1}$$

Так как $n_i = ln-l+i$, то отсюда

$$a_{2i}p^{2ln+2i} \equiv 0 \mod p^{3ln-l+3i}$$

Вместе с (8) это дает

$$P_i(x_i) - a_{0i} \equiv -a_{1i}p^{ln+i} \equiv \frac{1}{3}a_{0i}B_{p-3}p^{3ln-2l+3i} \mod p^{3ln-2l+3i+1}.$$

При $i=1$ отсюда следует, что

$$P_1(x_1) - a_{01} \equiv \frac{1}{3}a_{01}B_{p-3}p^{3ln-2l+3} \mod p^{3ln-2l+4}; \tag{9}$$

в случае же $i>1$

$$P_i(x_i) - a_{2i} \equiv 0 \mod p^{3ln-2l+4} \tag{10}$$

ибо в этом случае $3i>4$, а B_{p-3} не содержит p в знаменателе (в силу теоремы Штаудта, см. ниже).

Из (10) и (6) следует, что

$$\frac{c_{n+1}}{c_n} \equiv \frac{P_1(x_1)}{a_{01}} \mod p^{3n-2l+4} \tag{11}$$

Таким образом,

$$c_{n-1} - c_n = c_n\left(\frac{c_{n+1}}{c_n} - 1\right) \equiv c_n\left(\frac{P_1(x_1)}{a_{01}} - 1\right) \equiv c_n \frac{P_1(x_1) - a_1}{a_{01}} \mod p^{3n-2l+4}$$

то есть, в силу (9), $c_{n+1} \equiv c_n \mod p^{l+1}$. Отсюда

$$c_n \equiv c_1 = p^l \mod p^{l+1}. \tag{12}$$

Так как $x_n(p^l) = c_{n+1} - c_n$, то из (9) и (11) следует, что

$$\frac{x_n(p^l)}{c_n} \equiv \frac{P_1(x_1) - a_{01}}{a_{01}} \equiv \frac{1}{3} B_{p-3} p^{3n-2l+3} \mod p^{3n-2l+4}.$$

С учетом (12) окончательно получаем

$$x_n(p^l) \equiv \frac{1}{3} B_{p-3} p^{3n-l+3} \mod p^{3n-l+4},$$

что и требовалось.

Доказательство лемм 1 и 2. Напомним известные свойства чисел Бернулли:

(а) $B_{2k+1} = 0$ при $k \geqslant 1$; (13)

(б) $s_k(m) = (k+1)^{-1} \sum_{i=1}^{k+1} \binom{k+1}{i} B_{k+1-i} m^i$; (14)

(в) теорема Штаудта: пусть m — четное положительное число; если $m \not\equiv 0 \mod p-1$, B_m не содержит p в знаменателе, а если $m \equiv 0 \mod p-1$, то

$$pB_m \equiv -1 \mod p; \tag{15}$$

(г) сравнение Куммера: если m — четное положительное число с $m \not\equiv 0 \mod p-1$, то B_m/m не содержит p в знаменателе и

$$B_{m+p-1}/(m+p-1) \equiv B_m/m \mod p \tag{16}$$

(доказательства см. (8), стр. 505—509). Теперь докажем некоторые вспомогательные предложения.

I. Для любого r

$$\Sigma_{-2}(p^n) \equiv \Sigma r^{\varphi(p^{n+1})-2}(p^n) \mod p^{n+1}$$

Действительно, по теореме Эйлера, $i^{\varphi(p^{n+1})} \equiv 1 \mod p^{n+1}$ при $i \not\equiv 0 \mod p$. Следовательно, $i^{-2} \equiv i^{\varphi(p^{n+1})-2} \mod p^{n+1}$.

II. Если $k \geqslant n+1$, то $\Sigma_k(p^n) \equiv s_k(p^n) \mod p^{n+1}$ (это очевидно).

III. Если k четно и больше 2 и $p>3$ при $n=1$, то

$$s_k(p^n) \equiv B_k p^n \pmod{p^{n+1}},$$

Действительно, в силу (14), $s_k(p^n)=(k+1)^{-1}\sum_{i=1}^{k+1}\binom{k+1}{i}B_{k+1-i}p^{ni}$

$=B_kp^n+\frac{k}{2}B_{k-1}p^{2n}+\frac{1}{k+1}\binom{k+1}{3}B_{k-2}p^{3n}+\ldots$ Так как k четно и $k-1\neq 1$, то $B_{k-1}=0$ (см. (13)). Так как, далее, $\binom{k+1}{i}=\frac{k+1}{i}\binom{k}{i-1}$, то $\frac{1}{k+1}\binom{k+1}{i}B_{k+1-i}p^{ni}=\frac{1}{i}\binom{k}{i-1}B_{k+1-i}p^{ni}$.

Таким образом, достаточно доказать, что если $i\geqslant 3$, то $k^{-1}B_{k+1-i}p^{ni}\equiv 0 \mod p^{n+1}$. Из теоремы Штаудта следует, что $i^2B_{k+1-i}\equiv 0 \mod p$. Если $i^{-1}p^{ni-2}\equiv 0 \bmod p^n$ при $i\geqslant 3$, то $p^2B_{k+1-i}i^{-1}p^{ni-2}\equiv 0 \mod p^{n+1}$ и требуемое доказано. Если же $i^{-1}p^{ni-2}\not\equiv 0 \mod p^n$ при $i>3$, то легко проверить, что $(n, p, i)=(1, 2, 4)$ или $(1, 3, 3)$, а оба эти равенства исключены условием.

IV. Если $p>3$, $r>0$, то

$$B_{r\varphi(p^n+1)-2}\equiv\frac{2}{3}B_{p-3} \mod p$$

Действительно, из (16) следует, что при четном положительном $m\not\equiv 0 \mod p-1$ и $s>0$ имеет место сравнение

$B_{m+s(p-1)}/(m+s(p-1))\equiv B_m/m \mod p$, или $B_{m+s(p-1)}\equiv(m-s)B_m/m \mod p$. Если $m=p-3$ и $s=rp^n-1$ то $m+s(p-1)=rp^n(p-1)-2=$ $=r\varphi(p^{n+1})-2$. Отсюда

$$B_{r\varphi(p^n+1)}-2\equiv\frac{p-3-(rp^n-1)}{p-3}B_{p-3}\equiv\frac{2}{3}B_{p-3} \mod p.$$

V.

$$\sum_{-1}(p^n)\equiv-\frac{1}{2}p^n\sum_{-2}(p^n) \mod \begin{cases}p^{2n+1} & \text{при } p>2,\\ 2^{2n} & \text{при } p=2,\ n>1.\end{cases}$$

Действительно, если $i\not\equiv 0 \mod p$ то по $\mod p^{2n}$ имеем:

$$\frac{1}{i^2}+\frac{1}{(p^n-i)^2}=\frac{p^{2n}-2p^ni+2i^2}{i^2(p^n-i)^2}\equiv-\frac{2i(p^n-i)}{i^2(p^n-i)^2}=-\frac{2}{p^n}\left(\frac{1}{i}+\frac{1}{p^n-i}\right).$$

Суммируя это сравнение по тем i, для которых $i\not\equiv 0 \mod p$ и $1\leqslant i<p^n/2$, получаем:

$$\sum_{-2}(p^n)\equiv-\frac{2}{p^n}\sum_{-1}(p^n) \mod p^{2n}.$$

Отсюда следует утверждение V.

Приступим к доказательству леммы 1. Пусть $p>3$, $r\varphi(p^{n+1})-2>n+1$. Тогда, последовательно применяя I, II, III, IV, получаем:

$$\sum_{-2}(p^n)=\sum r_{\varphi(p^{n+1})-2}(p^n)\equiv s_{r\varphi(p^n+1)-2}(p^n)\equiv B_{r\varphi(p^n+1)-2}p^n$$

$$\equiv \frac{2}{3} B_{p-3} p^n \mod p^{n+1}.$$

Так как $\varphi(p^{n+1})-2 \equiv 0 \mod p-1$ при $p \neq 2, 3$, то из (15) следует, что $pB_{\varphi(p^{n+1})-2} \equiv -1 \mod p$. Пусть $p = 2, 3$ и $n > 1$. Учитывая утверждения I – III и последнее сравнение, получим:

$$\sum_{-2}(p^n) \equiv B_{\varphi(p^{n+1})-2} p^n \mod p^{n+1}$$

$$\equiv -p^{n-1} \mod p^n$$

Справедливость леммы при $p = 2, 3$, $n = 1$ проверяется прямым просчетом.

Лемма 1 доказана. Лемма 2 следует из леммы 1 и утверждения V.

Заключительные замечания. Аналогично доказывается следующее усиление теоремы 1.

Теорема 2. *Пусть p – простое число, $\varkappa_n(m, g, h) \equiv$*

$$\binom{gm^{n+1}}{hm^n} - \binom{gm^n}{hm^{n-1}}, \quad gh \not\equiv 0 \mod p \text{ и } \delta_p \text{ – показатель степени, с}$$

которым p входит в $\binom{gp^l}{h}$. Тогда

$$\varkappa_n(p^l, g, h) \equiv \begin{cases} \frac{1}{3} g h^3 B_{p-3} \binom{gp^l}{h} p^{l(3n-2)+3} \mod p^{l(3n-2)+\delta_p+4} & \text{при } p > 3, \\ g\left(\frac{g^{3l}}{h}\right) 3^{l(3n-2)+2} \mod 3^{l(3n-2)+\delta_3+3} & \text{при } p = 3, \\ 2^{l(3n-2)+\delta_2+1} \mod 2^{l(3n-2)+\delta_2+2} & \text{при } p=2,\ n>1, \\ 2^{\delta_2+1} \mod 2^{\delta_2+2} & \text{при } p=2,\ n=1 \end{cases}$$

Как мне стало известно во время оформления статьи, А. И. Ширшов доказал теорему 1 при $p=2, 3$, $l=1$; он получил также следствие 1.

Автор благодарит Ю. А. Брудного и Д. Б. Фукса за внимание к настоящей работе.

Московский государственный
университет им. М. В. Ломоносова

ՅՈՒ. Ա. ՏՐԱԽՏՄԱՆ

Երկանդամային գործակիցներից կազմված որոշ տարբերությունների բաժանելիության մասին

Ամփոփում ապացուցված է հետևյալ թեորեմը

Թեորեմ. Եթե $\varkappa_n(m) = \binom{m^{n+1}}{m_n} - \binom{m_n}{m^{n-1}}$: Ցանկացած պարզ p-ի և ցանկացած բնական l-ի համար տեղի ունի

$$\frac{1}{3}B_{p-3}p^{l(3n-1)+3} \pmod{p^{l(3n-1)+4}}, \text{ երբ } p>3$$

$$3^{l(3n-1)+2} \pmod{3^{l(3n-1)+3}}, \text{ երբ } p=3$$

$$2^{l(3n-1)+1} \pmod{2^{l(3n-1)+2}}, \text{ երբ } p=2,\ n>1$$

$$2^{l+1} \pmod{2^{l+2}}, \text{ երբ } p=2,\ n=1$$

համեմատությունը, որտեղ B_{p-3}-ը Բեռնուլիի $(p-3)$-րդ թիվն է:

Այս թեորեմը պատասխան է տալիս այն հարցերին, որոնք առաջ էին բաշված Դ. Բ. Ֆուքսի և Մ. Բ. Ֆուքսի կողմից (1).

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *Д. Б. Фукс, М. Б. Фукс.* Арифметика биномиальных коэффициентов, Квант, № 6, стр. 17—25, 1970. [2] *З. И. Боревич, И. Р. Шафаревич.* Теория чисел, «Наука», М., 1964.