

## О числахъ Бернулли.

Г. Ѳ. Вороного.

Замѣтка эта, почти исключительно, посвящена изслѣдованію нѣкоторыхъ свойствъ чиселъ Бернулли, на которыя въ первый разъ указалъ проф. I. C. Adams въ *Journal für die reine und angewandte Mathematik*, В. 85, въ статьѣ: „Table of the values of the first sixty two numbers of Bernoulli“. Онъ говоритъ:

„Я доказалъ, что, если  $n$  простое число большее 3, то числитель  $n$ -го Бернуллиева числа будетъ дѣлиться на  $n$ .

„Я также замѣтилъ, что если  $p$  такой простой дѣлитель  $n$ , который „не входитъ множителемъ въ знаменатель  $n$ -го числа Бернулли, то числитель этого числа дѣлится на  $p$ “ \*).

Я доказываю относительно чиселъ Бернулли слѣдующую теорему:

Если  $m$ -е Бернуллиево число  $B_m = \frac{P_m}{\Theta_m}$ , гдѣ  $\frac{P_m}{\Theta_m}$  дробь не сократимая, то:

$$\begin{aligned} (-1)^{m-1}(a^{2m} - 1)P_m \equiv 2ma^{2m-1}\Theta_m \left[ 1^{2m-1}E \frac{a}{N} + 2^{2m-1}E \frac{2a}{N} + \dots \right. \\ \left. \dots + (N-1)^{2m-1}E \frac{(N-1)a}{N} \right], \pmod{N}. \end{aligned}$$

\*) По поводу послѣдняго замѣчанія, онъ прибавляетъ: „I have not succeeded however, in obtaining a general proof of this proposition, though, I have no doubt of its truth“. Въ этой же статьѣ профессоръ Adams обѣщаетъ напечатать замѣтку о числахъ Бернулли въ appendix при 22-мъ томѣ *Cambridge Observations*. Ни въ Пулковской обсерваторіи, ни въ Академіи Наукъ этотъ томъ *Cambridge Observations* не былъ полученъ.

Здѣсь  $a$  и  $N$  произвольныя положительныя цѣлыя числа простыя между собой; символъ  $E \frac{ai}{N}$  обозначаетъ цѣлую часть дроби  $\frac{ai}{N}$ .

Изъ этой теоремы я вывожу нѣсколько слѣдствій и между прочимъ слѣдующую обобщенную теорему Adams'a:

*Если число  $m$ , значекъ  $m$ -го Бернуллиева числа, имѣетъ дѣлителемъ число  $k = p_1^\alpha p_2^\beta \dots p_l^\lambda$ , гдѣ  $p_1, p_2, \dots, p_l$  простыя числа, не дѣлящія знаменатель  $m$ -го Бернуллиева числа, то числитель его будетъ дѣлиться на  $k$ .*

При доказательствѣ этихъ предложеній, я пользуюсь теоремой Штаудта относительно знаменателей Бернуллиевыхъ чиселъ, но доказательство ея я значительно измѣнилъ.

§ 1. По формулѣ Лагранжа, для всякой цѣлой функціи  $f(z)$ , степени не выше  $n$ -й, имѣетъ мѣсто равенство:

$$f(z) = \sum_{i=0}^{i=n} \frac{f(x+i)}{z-x-i} \cdot \frac{F(z)}{F'(x+i)}, \dots \dots \dots (1)$$

гдѣ

$$F(z) = (z-x)(z-x-1)\dots(z-x-n).$$

Дифференцируемъ равенство (1) по  $z$

$$f'(z) = \sum_{i=0}^{i=n} \frac{f(x+i)}{z-x-i} \cdot \frac{F'(z)}{F'(x+i)} - \sum_{i=0}^{i=n} \frac{f(x+i)}{(z-x-i)^2} \cdot \frac{F(z)}{F'(x+i)}.$$

Въ этой формулѣ положимъ  $z = x$ .

Такъ какъ  $F(x) = 0$ , то получимъ:

$$f'(x) = \text{Lim} \left[ \frac{f(x)}{z-x} \cdot \frac{F'(z)}{F'(x)} - \frac{f(x)}{(z-x)^2} \cdot \frac{F(z)}{F'(x)} \right]_{z=x} - \sum_{i=1}^{i=n} \frac{f(x+i)}{i} \cdot \frac{F'(x)}{F'(x+i)}.$$

Легко видѣть, что

$$\frac{F'(x)}{F'(x+i)} = (-1)^i \frac{1.2\dots n}{1.2\dots i.1.2\dots(n-i)} = (-1)^i \cdot \frac{n(n-1)\dots(n-i+1)}{1.2\dots i},$$

$$\text{Lim} \left[ \frac{F'(z)}{(z-x)F'(x)} - \frac{F(z)}{(z-x)^2 F'(x)} \right]_{z=x} = - \left[ 1 + \frac{1}{2} + \dots + \frac{1}{n} \right].$$

Поэтому:

$$f'(x) = - \sum_{i=1}^{i=n} \frac{1}{i} f(x) + \frac{n}{1.1} f(x+1) - \frac{n(n-1)}{2.1.2} f(x+2) + \dots$$

$$\dots + (-1)^{i-1} \frac{n(n-1)\dots(n-i+1)}{i.1.2\dots i} f(x+i) + \dots$$

$$\dots + (-1)^{n-1} \frac{n(n-1)\dots 1}{n.1.2\dots n} f(x+n).$$
} (2)

§ 2. Примѣнимъ формулу (2) къ функциямъ Бернулли.

Сумма ряда

$$1^k + 2^k + \dots + x^k = S_k(x)$$

выражается цѣлой функцией отъ  $x$  степени  $k+1$ . Эта функция называется функцией Бернулли:  $\varphi_{k+1}(x)$ .

$$\varphi_{k+1}(x) = \frac{x^{k+1}}{k+1} + \frac{1}{2} x^k + \frac{k}{1.2} B_1 x^{k-1} -$$

$$- \frac{k(k-1)(k-2)}{1.2.3.4} B_2 x^{k-3} + \dots + (-1)^{\frac{k}{2}-1} \frac{B_{\frac{k}{2}} x}{2}$$
} \dots (3)

при  $k$  четномъ, и

$$\varphi_{k+1}(x) = \frac{x^{k+1}}{k+1} + \frac{1}{2} x^k + \frac{k}{1.2} B_1 x^{k-1} - \frac{k(k-1)(k-2)}{1.2.3.4} B_2 x^{k-3} + \dots$$

$$\dots + (-1)^{\frac{k-1}{2}-1} \frac{B_{\frac{k-1}{2}} k x^2}{2},$$
} (4)

при  $k$  нечетномъ.

Числа  $B_1, B_2 \dots$  называются числами Бернулли.

По формулѣ (2), при  $x=0$ ,

$$\varphi'_{2k+1}(0) = - \sum_{i=1}^{i=n} \frac{1}{i} \varphi_{2k+1}(0) + \frac{n}{1.1} \varphi_{2k+1}(1) - \frac{n(n-1)}{2.1.2} \varphi_{2k+1}(2) + \dots$$

$$\dots + (-1)^{n-1} \frac{1}{n} \varphi_{2k+1}(n).$$

Изъ формулы (3) слѣдуетъ, что

$$\varphi'_{2k+1}(0) = (-1)^{k-1} B_k,$$

$$\varphi_{2k+1}(0) = 0,$$

$$\varphi_{2k+1}(i) = S_{2k}(i) = 1^{2k} + 2^{2k} + \dots + i^{2k}.$$

Поэтому:

$$(-1)^{k-1} B_k = \frac{n}{1.1} S_{2k}(1) - \frac{n(n-1)}{2.1.2} S_{2k}(2) + \dots + (-1)^{n-1} \frac{1}{n} S_{2k}(n). \quad (5)$$

Въ этой формулѣ  $n$  должно быть больше  $2k$ .

Примѣръ.

$$k = 3, \quad n = 7.$$

$$\begin{aligned} (-1)^2 B_3 = 7 - \frac{7.6}{2.1.2} \cdot 65 + \frac{7.6.5}{3.1.2.3} \cdot 794 + \frac{7.6.5.4}{4.1.2.3.4} \cdot 4890 + \\ + \frac{7.6.5.4.3}{5.1.2.3.4.5} \cdot 20515 - \frac{7.6.5.4.3.2}{6.1.2.3.4.5.6} \cdot 67171 + \frac{1}{7} \cdot 184820. \end{aligned}$$

$$\begin{aligned} B_3 = 7 - 682 - \frac{1}{2} + 9263 + \frac{1}{3} - 42787 - \frac{1}{2} + \\ + 86163 - 78366 - \frac{1}{6} + 26402 + \frac{6}{7} = \frac{1}{42}. \end{aligned}$$

§ 3. Теперь докажемъ нѣсколько леммъ\*).

Лемма I.

$$S_n(ab) \equiv bS_n(a) + naS_{n-1}(a)S_1(b-1), \pmod{a^2}.$$

Доказательство.

Если равенство

$$(f + ga)^n = f^n + \frac{n}{1} f^{n-1} ga + \dots$$

разсматривать, какъ сравненіе по модулю  $a^2$ , то получимъ:

$$(f + ga)^n \equiv f^n + nf^{n-1}ga, \pmod{a^2}.$$

Давая  $f$  значенія  $1, 2, 3, \dots, a$ , для  $g$  значенія  $0, 1, 2, \dots, b-1$  и складывая полученные сравненія, найдемъ:

$$S_n(ab) \equiv bS_n(a) + naS_{n-1}(a)S_1(b-1), \pmod{a^2}.$$

\*) Доказательство первыхъ VIII леммъ заимствуемъ у Staudt'a Crelle's Journal, B. 21.

Лемма II.

Если  $a, b, c, \dots, k, l$  числа первыя между собой, то

$$\frac{S_n(a.b.c\dots k.l)}{a.b.c\dots k.l} - \frac{S_n(a)}{a} - \frac{S_n(b)}{b} - \dots - \frac{S_n(l)}{l} = \text{цѣлое число.}$$

Доказательство.

По предыдущей леммѣ:

$$S_n(a.b.c\dots k.l) \equiv b.c\dots k.l.S_n(a), \pmod{a},$$

$$S_n(a.b.c\dots k.l) \equiv a.c\dots k.l.S_n(b), \pmod{b},$$

.....

$$S_n(a.b.c\dots l) \equiv a.b.c\dots l.S_n(k), \pmod{k},$$

$$S_n(a.b.c\dots k) \equiv a.b.c\dots k.S_n(l), \pmod{l}.$$

Поэтому, разность

$$S_n(a.b.c\dots k.l) - b.c\dots k.l.S_n(a) - a.c\dots k.l.S_n(b) - \\ - a.b.c\dots l.S_n(k) - a.b.c\dots k.S_n(l)$$

дѣлится на  $a, b, c, \dots, k, l$  и, слѣдовательно, на ихъ произведение, такъ какъ числа  $a, b, \dots, k, l$  первыя между собой.

Лемма III.

$$2S_{2n+1}(a) \equiv (2n+1)aS_{2n}(a), \pmod{a^2}.$$

Доказательство.

Равенство

$$v^{2n+1} + (a-v)^{2n+1} = a^{2n+1} - \frac{2n+1}{1} a^{2n}v + \dots + (2n+1)av^{2n}$$

разсматриваемъ, какъ сравненіе по модулю  $a^2$ . Получимъ:

$$v^{2n+1} + (a-v)^{2n+1} \equiv (2n+1)av^{2n}, \pmod{a^2}.$$

Давая  $v$  значенія  $0, 1, 2, \dots, a$  и складывая рядъ полученныхъ такимъ образомъ сравненій, найдемъ:

$$2S_{2n+1}(a) \equiv (2n+1)aS_{2n}(a), \pmod{a^2}.$$

Лемма IV.

$$S_{2n}(ab) \equiv bS_{2n}(a), \pmod{a^2}.$$

Доказательство.

На основаніи леммы I-й

$$S_{2n}(ab) \equiv bS_{2n}(a) + 2naS_{2n-1}(a)S_1(b-1), \pmod{a^2}.$$

Но

$$2S_{2n-1}(a) \equiv (2n-1)aS_{2n-2}(a), \pmod{a^2}$$

и потому

$$S_{2n}(ab) \equiv bS_{2n}(a) + n(2n-1)a^2S_{2n-2}(a)S_1(b-1), \pmod{a^2}$$

или

$$S_{2n}(ab) \equiv bS_{2n}(a), \pmod{a^2}.$$

Лемма V.

Если  $a, r, n$  цѣлыя положительныя числа, то

$$\frac{S_{2n}(a^r)}{a^r} - \frac{S_{2n}(a)}{a} = \text{цѣлое число}.$$

Доказательство.

Для  $r=1$  лемма справедлива; если же она справедлива для  $r=q$ , то справедлива и для  $r=q+1$ .

Въ самомъ дѣлѣ, по леммѣ IV-й.

$$S_{2n}(a^{q+1}) \equiv aS_{2n}(a^q), \pmod{a^{2q}}.$$

Поэтому:

$$\frac{S_{2n}(a^{q+1})}{a^{q+1}} - \frac{S_{2n}(a^q)}{a^q} = \text{цѣлое число}.$$

Слѣдствіе.

Если  $a, b, c, \dots, l$  числа простыя между собой и  $\alpha, \beta, \gamma, \dots, \lambda$  нѣкоторыя цѣлыя положительныя числа, то

$$\frac{S_{2n}(a^\alpha b^\beta \dots l^\lambda)}{a^\alpha b^\beta \dots l^\lambda} - \frac{S_{2n}(a)}{a} - \frac{S_{2n}(b)}{b} - \dots - \frac{S_{2n}(l)}{l} = \text{цѣлое число}.$$

Лемма VI.

Если  $n$  дѣлится на  $p-1$  при  $p$  простомъ, то

$$S_n(p) \equiv -1, \pmod{p}.$$

Доказательство.

По теоремѣ Фермата, если  $n$  дѣлится на  $p-1$ , то

$$x^n \equiv 1, \pmod{p}.$$

Давая  $x$  значенія  $1, 2, \dots, p-1$  и складывая полученныя сравненія, найдемъ:

$$S_n(p-1) \equiv p-1, \pmod{p}$$

или

$$S_n(p) \equiv -1, \pmod{p}.$$

Поэтому:

$$\frac{S_n(p)}{p} + \frac{1}{p} = \text{цѣлое число}.$$

Лемма VII.

Если  $p$  простое число и  $n$  не дѣлится на  $p-1$ , то имѣетъ мѣсто сравненіе:

$$S_n(p) \equiv 0, \pmod{p}.$$

Доказательство.

При всякомъ  $x$ , не дѣлящемся на  $p$ :

$$x \equiv r_1, \pmod{p},$$

$$2x \equiv r_2, \pmod{p},$$

.....

$$(p-1)x \equiv r_{p-1}, \pmod{p}.$$

Числа  $r_1, r_2, \dots, r_{p-1}$  положительные наименьшіе вычеты по модулю  $p$  и потому представляютъ рядъ чиселъ  $1, 2, \dots, p-1$ , только иначе расположенныхъ.

Возвышая предыдущія сравненія въ степень  $n$  и складывая, найдемъ:

$$x^n S_n(p) \equiv S_n(p), \pmod{p}.$$

Если  $x$  первообразный корень простого числа  $p$ , и  $n$  не дѣлится на  $p-1$ , то не можетъ имѣть мѣста сравненіе

$$x^n \equiv 1, \pmod{p},$$

и потому, необходимо:

$$S_n(p) \equiv 0, \pmod{p}.$$

Лемма VIII.

$$\frac{S_{2n}(u)}{u} + \frac{1}{a} + \frac{1}{b} + \dots + \frac{1}{h} = \text{цѣлое число},$$

гдѣ  $a, b, \dots, h$  простые дѣлители  $u$ , такіе, что  $2n$  дѣлится на  $a-1, b-1, \dots, h-1$ .

Эта лемма очевидна на основаніи леммъ V-й VI-й и VII-й.

Лемма IX.

При  $p$  простомъ имѣетъ мѣсто сравненіе:

$$\frac{m(m-1)\dots(m-p+1)}{1.2\dots p} - \frac{m(m-1)\dots(m-2p+1)}{1.2\dots(2p)} + \dots \\ \dots + \frac{m(m-1)\dots(m-kp+1)}{1.2\dots(kp)} \equiv 1, \pmod{p},$$

$k$  есть цѣлая часть дроби  $\frac{m}{p}$ , т. е.  $k = E \frac{m}{p}$ .

Доказательство.

По формулѣ (2) § 1

$$f'(x) = - \sum_{i=1}^{i=n} \frac{1}{i} f(x) + \frac{n}{1.1} f(x+1) - \frac{n(n-1)}{2.1.2} f(x+2) + \dots \\ \dots \pm \frac{1}{n} f(x+n).$$

Функция  $f(x)$  степени не выше  $n$ -й.

Пусть

$$f(x) = x(1 - x^{p-1}),$$

$$f(0) = 0,$$

$$f'(0) = 1.$$

Поэтому:

$$1 = n(1 - 1^{p-1}) - \frac{n(n-1)}{1.2} (1 - 2^{p-1}) + \dots \pm \frac{n(n-1)\dots 1}{1.2\dots n} (1 - n^{p-1}).$$

Здѣсь  $n$  больше или равно  $p$ .

Разсматривая это равенство, какъ сравненіе по модулю  $p$ , найдемъ:

$$\frac{n(n-1)\dots(n-p+1)}{1.2\dots p} - \frac{n(n-1)\dots(n-2p+1)}{1.2\dots 2p} + \dots \\ \dots \pm \frac{n(n-1)\dots(n-kp+1)}{1.2\dots kp} \equiv 1, \pmod{p},$$

$$k = E \frac{n}{p}.$$



§ 4. Теорема Штаудта.

$$(-1)^k B_k = \frac{1}{\alpha} + \frac{1}{\beta} + \dots + \frac{1}{\lambda} + T,$$

$\alpha, \beta, \dots, \lambda$  простые числа такія, что  $2k$  дѣлится на  $\alpha - 1, \beta - 1, \dots, \lambda - 1$ .  
 $T$  есть цѣлое число.

Доказательство.

Мы вывели для  $B_k$  въ § 2 слѣдующую формулу:

$$(-1)^{k-1} B_k = \frac{n}{1} \frac{S_{2k}(1)}{1} - \frac{n(n-1)}{1 \cdot 2} \cdot \frac{S_{2k}(2)}{2} + \dots + \frac{n(n-1)\dots 1}{1 \cdot 2 \dots n} \cdot \frac{S_{2k}(n)}{n},$$

$n$  больше  $2k$ .

По леммѣ VIII-й.

$$\frac{S_{2k}(u)}{u} = -\frac{1}{\alpha} - \frac{1}{\beta} - \dots - \frac{1}{\mu} + t,$$

$t$  число цѣлое, а  $\alpha, \beta, \dots, \mu$  простые дѣлители  $u$ , такіе, что  $2k$  дѣлится на  $\alpha - 1, \beta - 1, \dots, \mu - 1$ .

Поэтому, въ выраженіи  $B_k$  дробь  $+\frac{1}{\alpha}$  будетъ имѣть множителемъ слѣдующее выраженіе:

$$-\left[ \frac{n(n-1)\dots(n-\alpha+1)}{1 \cdot 2 \dots \alpha} - \frac{n(n-1)\dots(n-2\alpha+1)}{1 \cdot 2 \dots (2\alpha)} + \dots \right. \\ \left. \dots + \frac{n(n-1)\dots(n-k\alpha+1)}{1 \cdot 2 \dots (k\alpha)} \right],$$

$$k = E \frac{n}{\alpha}.$$

На основаніи леммы IX-й, это выраженіе равно  $-1 + \alpha \Theta_\alpha$ , гдѣ  $\Theta_\alpha$  цѣлое число.

Выше сказанное относится ко всѣмъ простымъ числамъ  $\alpha, \beta, \dots, \lambda$  такимъ, что  $2k$  дѣлится на  $\alpha - 1, \beta - 1, \dots, \lambda - 1$  и потому:

$$(-1)^{k-1} B_k = -\frac{1}{\alpha} + \Theta_\alpha - \frac{1}{\beta} + \Theta_\beta - \dots - \frac{1}{\lambda} + \Theta_\lambda + \Theta$$

или

$$(-1)^k B_k = \frac{1}{\alpha} + \frac{1}{\beta} + \dots + \frac{1}{\lambda} + T.$$

$T$  есть цѣлое число.

Числа  $\alpha, \beta, \dots, \lambda$  опредѣляются такимъ образомъ:

Выписываются все дѣлители числа  $k$ , затѣмъ все они удваиваются и къ полученнымъ числамъ прибавляютъ по единицѣ; все образованные такимъ образомъ простые числа будутъ искомыми  $\alpha, \beta, \dots, \lambda$ . Къ нимъ прибавляется еще 2.

Примѣръ 1-й.  $k = 3$ .

Дѣлители: 1, 3.

Числа 3, 7 простые и потому:

$$B_3 = T - \frac{1}{2} - \frac{1}{3} - \frac{1}{7}.$$

Но мы уже получили раньше, что

$$B_3 = \frac{1}{42}$$

и потому  $T = 1$ .

Примѣръ 2-й.  $k = 12$ .

Дѣлители 12-ти: 1, 2, 3, 4, 6, 12.

Въ ряду чиселъ 3, 5, 7, 9, 13, 25 числа 9 и 25 не простые и потому:

$$B_{12} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{13} + T.$$

Замѣчаніе.

Знаменатель всякаго Бернулліева числа, на основаніи теоремы Штаудта, равенъ произведенію нѣкоторыхъ простыхъ чиселъ, взятыхъ множителемъ только по одному разу.

§ 5. Теорема.

При всякомъ  $N$  цѣломъ и положительномъ, имѣетъ мѣсто сравненіе:

$$(-1)^{k-1} P_k N \equiv \Theta_k S_{2k}(N), \pmod{N^2},$$

$$B_k = \frac{P_k}{\Theta_k}, \text{ гдѣ } \frac{P_k}{\Theta_k} \text{ дробь не сократимая.}$$

Доказательство.

Мы имѣли (§ 2), что

$$S_{2k}(N) = \frac{N^{2k+1}}{2k+1} + \frac{1}{2} N^{2k} + \frac{2k}{1 \cdot 2} B_1 N^{2k-1} - \frac{2k \cdot (2k-1) \cdot (2k-2)}{1 \cdot 2 \cdot 3 \cdot 4} B_2 N^{2k-3} + \dots \left. \vphantom{S_{2k}(N)} \right\} \text{(A)}$$

$$\dots + (-1)^{k-2} \frac{2k \cdot (2k-1) \cdot \dots \cdot 4}{1 \cdot 2 \cdot \dots \cdot (2k-2)} B_{k-1} N^3 + (-1)^{k-1} B_k N.$$

Положимъ, что  $2k + 1$  и  $N$  имѣютъ общаго наибольшаго дѣлителя  $d$  и пусть

$$2k + 1 = a \cdot d,$$

$$N = b \cdot d,$$

$a$  и  $N$  числа взаимно простыя.

Умножимъ обѣ части равенства (A) на  $a \cdot \Theta$ , гдѣ  $\Theta$  есть наименьшее кратное всѣхъ  $k$  знаменателей Бернулліевыхъ чиселъ  $B_1, B_2, \dots, B_k$ .

Получимъ:

$$\begin{aligned} a \Theta S_{2k}(N) &= \Theta N^{2k} b + \frac{\Theta}{2} N^{2k} a + \\ &+ \frac{(2k + 1)2k}{1 \cdot 2} N^{2k-2} b B_1 \Theta - \frac{(2k + 1) \dots (2k - 2)}{1 \cdot 2 \cdot 3 \cdot 4} N^{2k-4} b B_2 \Theta + \dots \\ &\dots + (-1)^{k-2} \frac{2k \cdot (2k - 1)}{1 \cdot 2 \cdot 3} a N^3 B_{k-1} \Theta + (-1)^{k-1} B_k \Theta N a. \end{aligned}$$

Въ правой части этого равенства все числа цѣлыя и потому, рассматривая его, какъ сравненіе по модулю  $N^3$ , найдемъ:

$$a \cdot \Theta \cdot S_{2k}(N) \equiv (-1)^{k-2} \frac{2k \cdot (2k - 1)}{1 \cdot 2 \cdot 3} a N^3 B_{k-1} \Theta + (-1)^{k-1} B_k \cdot \Theta \cdot a \cdot N \pmod{N^3}.$$

Умножаемъ обѣ части сравненія на  $2 \cdot 3$ , тогда будемъ имѣть:

$$2 \cdot 3 \cdot a \Theta S_{2k}(N) \equiv (-1)^{k-1} 2 \cdot 3 \cdot a \cdot N \Theta B_k \pmod{N^3}.$$

Такъ какъ  $a$  число простое съ  $N$ , то обѣ части сравненія сокращаемъ на  $a$ ;

$$2 \cdot 3 \cdot \Theta \cdot S_{2k}(N) \equiv (-1)^{k-1} 2 \cdot 3 \cdot N \Theta B_k \pmod{N^3}.$$

Пусть

$$\Theta = \Theta' \cdot \Theta_k.$$

Замѣтимъ, что по теоремѣ Штаудта  $\Theta_k$  всегда дѣлится на  $2 \cdot 3$ , а потому,  $\Theta'$  не дѣлится на  $2 \cdot 3$ , такъ какъ  $\Theta$  есть наименьшее кратное  $k$  знаменателей  $\Theta_1, \Theta_2, \dots, \Theta_k$ .

Такимъ образомъ:

$$2 \cdot 3 \cdot \Theta' \cdot \Theta_k \cdot S_{2k}(N) \equiv (-1)^{k-1} 2 \cdot 3 \cdot \Theta' \cdot N \cdot P_k \pmod{N^3}.$$

Число 2.3.  $\Theta'$  есть произведение нѣкоторыхъ простыхъ чиселъ, входящихъ въ него множителями не болѣе разу, и потому, хотя между ними и найдутся дѣлители числа  $N$ , но во всякомъ случаѣ:

$$(-1)^{k-1} N \cdot P_k \equiv \Theta_k \cdot S_{2k}(N), \pmod{N^2}.$$

При доказательствѣ теоремы мы предполагали, что  $k$  болѣе единицы, но легко видѣть, что теорема справедлива и для  $k = 1$ .

Въ самомъ дѣлѣ:

$$S_2(N) = \frac{N^3}{3} + \frac{1}{2} N^2 + \frac{1}{6} N.$$

Умножаемъ обѣ части равенства на 6 и рассматриваемъ, какъ сравненіе по модулю  $N^2$ ; найдемъ:

$$6 \cdot S_2(N) \equiv N, \pmod{N^2}.$$

Но  $P_1 = 1$ ,  $\Theta_1 = 6$ ,  $k = 1$  и предыдущее сравненіе можно такъ переписать:

$$(-1)^{1-1} N \cdot P_1 \equiv \Theta_1 \cdot S_2(N), \pmod{N^2}.$$

### § 6. Лемма X.

Если  $a$  и  $N$  цѣлыя положительныя числа взаимно простыя, то имѣетъ мѣсто, при  $m > 1$ , сравненіе:

$$(a^m - 1) S_m(N) \equiv m a^{m-1} N \sum_{i=1}^{i=N-1} i^{m-1} E \frac{ai}{N}, \pmod{N^2},$$

$E \frac{ai}{N}$  есть цѣлая часть дроби  $\frac{ai}{N}$ .

Доказательство.

Возьмемъ рядъ равенствъ:

$$\left. \begin{aligned} a &= N \cdot E \frac{a}{N} + r_1, \\ 2a &= N \cdot E \frac{2a}{N} + r_2, \\ &\dots \dots \dots \\ (N-1)a &= N \cdot E \frac{(N-1)a}{N} + r_{N-1}. \end{aligned} \right\} \dots \dots \dots (B)$$

Числа  $r_1, r_2 \dots r_{N-1}$  всё меньше  $N$  и всё между собой различны, а потому,  $r_1, r_2 \dots r_{N-1}$  представляют рядъ чисель:  $1, 2, \dots (N-1)$ , только иначе расположенныхъ.

Равенства (В) перепишемъ иначе:

$$\begin{aligned} a - NE \frac{a}{N} &= r_1, \\ 2a - NE \frac{2a}{N} &= r_2, \\ &\dots \dots \dots \\ (N-1)a - NE \frac{(N-1)a}{N} &= r_{N-1}, \end{aligned}$$

и возвысимъ обѣ части всёхъ этихъ равенствъ въ степень  $m$ .

$$\begin{aligned} a^m - mNa^{m-1}E \frac{a}{N} + \dots &= r_1^m, \\ 2^m a^m - mNa^{m-1}2^{m-1}E \frac{2a}{N} + \dots &= r_2^m, \\ &\dots \dots \dots \\ (N-1)^m a^m - mNa^{m-1}(N-1)^{m-1}E \frac{(N-1)a}{N} + \dots &= r_{N-1}^m. \end{aligned}$$

Равенства эти рассматриваемъ, какъ сравненія по модулю  $N^2$ :

$$\begin{aligned} a^m - mNa^{m-1}E \frac{a}{N} &\equiv r_1^m, \pmod{N^2}, \\ 2^m a^m - mNa^{m-1}2^{m-1}E \frac{2a}{N} &\equiv r_2^m, \pmod{N^2}, \\ &\dots \dots \dots \\ (N-1)^m a^m - mNa^{m-1}(N-1)^{m-1}E \frac{(N-1)a}{N} &\equiv r_{N-1}^m, \pmod{N^2}. \end{aligned}$$

Складывая всё эти сравненія почленно, найдемъ:

$$a^m \cdot S_m(N-1) - ma^{m-1}N \sum_{i=1}^{i=N-1} i^{m-1} E \frac{ai}{N} \equiv S_m(N-1), \pmod{N^2},$$

или

$$(a^m - 1)S_m(N-1) \equiv ma^{m-1}N \sum_{i=1}^{i=N-1} i^{m-1} E \frac{ai}{N}, \pmod{N^2}.$$

Если  $m > 1$ , то будетъ имѣть мѣсто также сравненіе:

$$(a^m - 1)S_m(N) \equiv ma^{m-1}N \sum_{i=1}^{i=N-1} i^{m-1} E \frac{ai}{N}, \pmod{N^2}.$$

§ 7. Теорема.

При произвольныхъ цѣлыхъ и положительныхъ числахъ  $a$  и  $N$ :

$$(-1)^{m-1}P_m(a^{2m}-1) \equiv 2ma^{2m-1}\Theta_m \sum_{i=1}^{i=N-1} i^{2m-1} E \frac{ai}{N}, \pmod{N},$$

гдѣ  $B_m = \frac{P_m}{\Theta_m}$  дробь не сократимая.

Доказательство.

По теоремѣ § 5:

$$(-1)^{m-1}P_m N \equiv \Theta_m S_{2m}(N), \pmod{N^2}.$$

По леммѣ X-й:

$$(a^{2m} - 1)S_{2m}(N) \equiv 2ma^{2m-1}N \sum_{i=1}^{i=N-1} i^{2m-1} E \frac{ai}{N}, \pmod{N^2}.$$

Умножаемъ обѣ части перваго сравненія на  $(a^{2m} - 1)$ , втораго на  $\Theta_m$  и вычитаемъ полученные сравненія почленно. Найдемъ:

$$(-1)^{m-1}P_m(a^{2m} - 1)N \equiv 2ma^{2m-1}N\Theta_m \sum_{i=1}^{i=N-1} i^{2m-1} E \frac{ai}{N}, \pmod{N^2}.$$

Или, сокращая на  $N$ , окончательно:

$$(-1)^{m-1}P_m(a^{2m} - 1) \equiv 2ma^{2m-1}\Theta_m \sum_{i=1}^{i=N-1} i^{2m-1} E \frac{ai}{N}, \pmod{N}.$$

Слѣдствіе I.

Пусть въ предыдущемъ сравненіи  $N = m$ . Тогда необходимо, чтобы

$$P_m(a^{2m} - 1) \equiv 0, \pmod{m}, \dots \dots \dots (*)$$

$a$  есть произвольное цѣлое положительное число простое съ  $m$ .

Пусть  $k = p_1^\alpha p_2^\beta \dots p_i^\lambda$  какой-нибудь дѣлитель числа  $m$  и пусть  $p_1, p_2, \dots, p_i$  такія простые числа, что  $2m$  не дѣлится на  $p_1 - 1, p_2 - 1, \dots, p_i - 1$ .

Пусть  $a_1$  первообразный корень простого числа  $p_1$ . Въ такомъ случаѣ, не можетъ имѣть мѣста сравненіе

$$a_1^{2m} - 1 \equiv 0, \pmod{p_1}.$$

Поэтому, на основаніи сравненія (\*):

$$P_m \equiv 0, \pmod{p_1^\alpha}.$$

Если возьмемъ другое простое число  $p_2$ , то выберемъ другой первообразный корень  $a_2$  и точно также докажемъ, что

$$P_m \equiv 0, \pmod{p_2^\beta}$$

и т. д. Наконецъ

$$P_m \equiv 0, \pmod{p_i^\lambda}.$$

Изъ этихъ сравненій слѣдуетъ, что  $P_m$  дѣлится на  $p_1^\alpha p_2^\beta \dots p_i^\lambda$  т. е. на  $k$ .

Примѣръ.  $m = 25$ .

Пусть  $k = 5^2, 2m = 50$ .

50 не дѣлится на  $5 - 1$  и потому  $P_{25}$  должно дѣлиться на 25.

Дѣйствительно, изъ таблицъ Бернуллевыхъ чиселъ проф. Adams'a:  $P_{25} = 495057205241079648212477525$ , число дѣлящееся на 25.

Замѣчаніе.

Тѣ условія, которымъ должны удовлетворять числа  $p_1, p_2, \dots, p_i$ , простые дѣлители  $m$ , прямо указываютъ, на основаніи теоремы Штаудта (§ 4), что они не должны дѣлить знаменателя  $m$ -го Бернуллева числа.

Слѣдствіе II.

Пусть  $n = m + k \frac{\varphi(N)}{2}$ .

Символь  $\varphi(N)$  обозначаетъ, сколько въ ряду чиселъ  $1, 2, 3, \dots, N - 1$  простыхъ съ  $N$ .

Если  $N = p_1^\alpha p_2^\beta \dots p_i^\lambda$ , то  $\varphi(N) = p_1^\alpha p_2^\beta \dots p_i^\lambda \frac{p_1 - 1}{p_1} \frac{p_2 - 1}{p_2} \dots \frac{p_i - 1}{p_i}$ .

Примѣняя теорему § 7, найдемъ:

$$(-1)^{n-1}(a^{2n}-1)P_n \equiv 2na^{2n-1} \Theta_n \sum_{i=1}^{i=N-1} i^{2n-1} E \frac{ai}{N}, \pmod{N}.$$

По теоремѣ Эйлера, при  $a$  простомъ съ  $N$ , имѣетъ мѣсто сравненіе

$$a^{2n-1} \equiv a^{2m-1}, \pmod{N}.$$

Замѣтимъ, что это же сравненіе будетъ имѣть мѣсто и при  $a$  не простомъ съ  $N$ , при слѣдующемъ условіи:

Наибольшій изъ показателей степеней  $\alpha, \beta, \dots, \lambda$  въ  $N = p_1^\alpha p_2^\beta \dots p_l^\lambda$  не долженъ быть больше  $2m - 1$ .

Предполагая, что это условіе выполнено, будемъ имѣть:

$$\sum_{i=1}^{i=N-1} i^{2n-1} E \frac{ai}{N} \equiv \sum_{i=1}^{i=N-1} i^{2m-1} E \frac{ai}{N}, \pmod{N}.$$

Поэтому, умножая обѣ части сравненія:

$$(-1)^{m-1} P_m (a^{2m}-1) \equiv 2ma^{2m-1} \Theta_m \sum_{i=1}^{i=N-1} i^{2m-1} E \frac{ai}{N}, \pmod{N},$$

на  $n \frac{\Theta_n}{2.3}$ , а сравненія

$$(-1)^{n-1} P_n (a^{2n}-1) \equiv 2na^{2n-1} \Theta_n \sum_{i=1}^{i=N-1} i^{2n-1} E \frac{ai}{N}, \pmod{N}$$

на  $m \frac{\Theta_m}{2.3}$ , и вычитая ихъ почленно, найдемъ:

$$(-1)^{n-1} m \frac{\Theta_m}{2.3} P_n (a^{2n}-1) \equiv (-1)^{m-1} n \frac{\Theta_n}{2.3} P_m (a^{2m}-1), \pmod{N}.$$

Замѣтимъ, что

$$a^{2m}-1 \equiv a^{2n}-1, \pmod{N}.$$

Если  $p_1, p_2, \dots, p_l$ , простые дѣлители  $N$ , таковы, что  $2m$  не дѣлится на  $p_1-1, p_2-1, \dots, p_l-1$ , то легко убѣдиться указаннымъ уже выше способомъ, что



$$(-1)^{n-1} \frac{m \cdot \Theta_m \cdot P_n}{2 \cdot 3} \equiv (-1)^{m-1} \frac{n \cdot \Theta_n \cdot P_m}{2 \cdot 3}, \pmod{N}; \dots (**)$$

$$n = m + \frac{k\varphi(N)}{2}; \quad N = p_1^\alpha p_2^\beta \dots p_l^\lambda;$$

$$\varphi(N) = p_1^\alpha p_2^\beta \dots p_l^\lambda \cdot \frac{p_1-1}{p_1} \cdot \frac{p_2-1}{p_2} \dots \frac{p_l-1}{p_l}$$

$k$  есть произвольное цѣлое положительное число;  $2m - 1$  должно быть больше или равно наивысшему изъ показателей степеней  $\alpha, \beta, \dots, \lambda$ .

Послѣднее предложеніе представляет тотъ интересъ, что изслѣдованіе очень большихъ Бернулліевыхъ чиселъ, въ нѣкоторыхъ случаяхъ, сводитъ къ рѣшенію довольно простыхъ сравненій.

Примѣръ.

Какія двѣ послѣднія цифры въ числителѣ 43-го Бернулліева числа?

Рѣшеніе.

Пусть  $N = 200 = 2^3 \cdot 5^2$ ;  $\varphi(N) = 2^2 \cdot 5 \cdot 4 \cdot 1 = 80$ ;  $m = 3$ ;

$$n = 3 + \frac{k \cdot 80}{2} = 3 + k \cdot 40;$$

$$n = 43, \quad \text{при } k = 1.$$

Въ данномъ случаѣ  $\alpha = 3$ ,  $\beta = 2$  и  $2m - 1 > 3$ .

Поэтому:

$$(-1)^{423} \cdot \frac{\Theta_3}{2 \cdot 3} \cdot P_{43}(a^{86} - 1) \equiv (-1)^{243} \cdot \frac{\Theta_{43}}{2 \cdot 3} \cdot P_3(a^6 - 1), \pmod{200}.$$

Въ § 4 мы уже опредѣлили:  $P_3 = 1$ ,  $\Theta_3 = 42$ . Найдемъ  $\Theta_{43}$ .

Дѣлители 43 суть 1 и 43.

Число  $2 \cdot 43 + 1 = 87$  не простое и потому,  $\Theta_{43} = 2 \cdot 3$ .

Итакъ:

$$3 \cdot \frac{42}{2 \cdot 3} \cdot P_{43}(a^{86} - 1) \equiv 43 \cdot \frac{6}{2 \cdot 3} \cdot (a^6 - 1), \pmod{200}.$$

Число  $a$  простое съ 200 и потому должно быть нечетнымъ.

$a^6 - 1$  и  $a^{86} - 1$  дѣлятся на 4, но не дѣлятся на 5, и такъ какъ

$$a^6 - 1 \equiv a^{86} - 1, \pmod{200},$$

то, сокращая обѣ части предыдущаго сравненія на  $a^6 - 1$ , получимъ:

или

$$3 \cdot 7 \cdot P_{43} \equiv 43, \pmod{50}$$

$$21 \cdot P_{43} \equiv -7, \pmod{50},$$

$$3 \cdot P_{43} \equiv -1, \pmod{50},$$

$$P_{43} \equiv 33, \pmod{50}.$$

По этому двѣ послѣднія цифры  $P_{43}$  должны быть либо 33, либо 83. Дѣйствительно, изъ таблицъ профессора Adams'a:

$$P_{43} = \{660\ 71461\ 94176\ 78653\ 57384\ 78474\ 26261\ 49627\ 78306\ 86653\ 38893\ 17619\ 96983\}.$$

Число  $P_{43}$  имѣетъ двѣ послѣднія цифры: 83. Слѣдствіе III.

Изъ сравненія (\*\*\*) слѣдуетъ, что, при

$$N = P_m = p_1^\alpha p_2^\beta \dots p_i^\lambda,$$

$$(-1)^{n-1} \frac{m \cdot \Theta_m}{2 \cdot 3} \cdot P_n \equiv 0, \pmod{P_m}.$$

$\Theta_m$  не можетъ имѣть дѣлителей общихъ съ  $P_m$  и потому:

$$(-1)^{n-1} \cdot m \cdot P_n \equiv 0, \pmod{P_m}.$$

Примѣръ.

$$m = 6, \quad P_6 = 691.$$

691 есть число простое и потому,

$$6 \cdot P_{6+k} \frac{691-1}{2} \equiv 0, \pmod{691},$$

т. е. всѣ числа вида

$$P_{6+345 \cdot k}$$

дѣлятся на 691.

Если  $k = 1$ , то получимъ, что  $P_{351}$  должно дѣлиться на 691.

Таблицы Бернулліевыхъ чиселъ профессора Adams'a доведены имъ только до 62-го, а потому повѣрить эту теорему на самомъ дѣлѣ мы не имѣемъ возможности.

#### § 8. Слѣдствіе IV.

Формула, выведенная въ § 7:

$$(-1)^{m-1} P_m (a^{2m} - 1) \equiv 2ma^{2m-1} \Theta_m \sum_{i=1}^{i=N-1} i^{2m-1} E \frac{ai}{N}, \pmod{N},$$

при  $m = 1$ , даетъ рѣшеніе сравненія первой степени при  $a$  простомъ съ  $N$ :

$$ax \equiv 1, \pmod{N}.$$

Въ самомъ дѣлѣ,  $P_1 = 1$ ,  $\Theta_1 = 6$  и потому

$$a^2 - 1 \equiv 12a \sum_{i=1}^{i=N-1} iE \frac{ai}{N}, \pmod{N}$$

или

$$a \left( a - 12 \sum_{i=1}^{i=N-1} iE \frac{ai}{N} \right) \equiv 1, \pmod{N}.$$

Очевидно, что

$$x \equiv a - 12 \sum_{i=1}^{i=N-1} iE \frac{ai}{N}, \pmod{N}$$

будетъ рѣшеніемъ сравненія

$$ax \equiv 1, \pmod{N}.$$

Примѣръ.

Рѣшить сравненіе:

$$5x \equiv 1, \pmod{13}.$$

$$\begin{aligned} \sum_{i=1}^{i=12} iE \frac{5i}{13} &= 1.0 + 2.0 + 3.1 + 4.1 + 5.1 + 6.2 + 7.2 + 8.3 + \\ &+ 9.3 + 10.3 + 11.4 + 12.4 = 211. \end{aligned}$$

Поэтому

$$\sum_{i=1}^{i=12} iE \frac{5i}{13} \equiv 3, \pmod{13}$$

и

$$x \equiv 5 - 12.3 \equiv 5 + 3 \equiv 8, \pmod{13}.$$

$x \equiv 8$ , дѣйствительно, есть рѣшеніе сравненія

$$5x \equiv 1, \pmod{13}.$$

Формулу

$$x \equiv a - 12 \sum_{i=1}^{i=N-1} iE \frac{ai}{N}, \pmod{N}$$

можно преобразовать въ другую, болѣе удобную для вычисленій:

$$x \equiv -2a + 3 + 6 \sum_{i=1}^{i=a-1} \left( E \frac{Ni}{a} \right)^2, \pmod{N},$$

но мы не считаемъ нужнымъ на этомъ останавливаться.

Прилагая ее къ предыдущему примѣру, найдемъ:

$$\sum_{i=1}^{i=4} \left( E \frac{13i}{5} \right)^2 = 2^2 + 5^2 + 7^2 + 10^2 = 178;$$

$$\sum_{i=1}^{i=4} \left( E \frac{13i}{5} \right)^2 \equiv 9, \pmod{13}.$$

Поэтому:

$$x \equiv -2 \cdot 5 + 3 + 6 \cdot 9 \equiv 8, \pmod{13}.$$

Петербургъ.

5 Октября 1889 года.