О числахъ Бернулли.

Г. Θ. 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, B. 85, въ статьѣ: „Table of the values of the firs sixty two numbers of Bernoulli". Онъ говоритъ:

„Я доказалъ, что, если n простое число большее 3, то числитель n-го „Бернулліева 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 Бернулліево число $B_m = \frac{P_m}{\Theta_m}$, гдѣ $\frac{P_m}{\Theta_m}$ дробь не сократимая, то:

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

*) 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'а:

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

При доказательствѣ этихъ предложеній, я пользуюсь теоремой Штаудта относительно знаменателей Бернулліевыхъ 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:

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

гдѣ

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

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:

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

Легко видѣть, что

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

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

Поэтому:

$$\left.\begin{aligned} f'(x) = -\sum_{i=1}^{i=n}\frac{1}{i}f(x) + \frac{n}{1.1}f(x+1) - \frac{n(n-1)}{2.1.2}f(x+2) + \ldots \\ \ldots + (-1)^{i-1}\frac{n(n-1)\ldots(n-i+1)}{i.1.2\ldots i}f(x+i) + \ldots \\ \ldots + (-1)^{n-1}\frac{n(n-1)\ldots 1}{n.1.2\ldots n}f(x+n). \end{aligned}\right\}(2)$$

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

Сумма ряда

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

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

$$\left.\begin{aligned} \varphi_{k+1}(x) = \frac{x^{k+1}}{k+1} + \frac{1}{2}x^k + \frac{k}{1.2}B_1 x^{k-1} - \\ -\frac{k(k-1)(k-2)}{1.2.3.4}B_2 x^{k-3} + \ldots + (-1)^{\frac{k}{2}-1}B_{\frac{k}{2}}x \end{aligned}\right\}, \quad \ldots (3)$$

при k четномъ, и

$$\left.\begin{aligned} \varphi_{k+1}(x) = \frac{x^{k+1}}{k+1} + \frac{1}{2}x^k + \frac{k}{1.2}B_1 x^{k-1} - \frac{k(k-1)(k-2)}{1.2.3.4}B_2 x^{k-3} + \ldots \\ \ldots + (-1)^{\frac{k-1}{2}-1}B_{\frac{k-1}{2}}kx^2, \end{aligned}\right\}(4)$$

при k нечетномъ.

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

По формулѣ (2), при $x = 0$,

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

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

Изъ формулы (3) слѣдуетъ, что

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

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

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

Поэтому:

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

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

Примѣръ.

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

$$(-1)^2B_3=7-\frac{7.6}{2.1.2}\cdot 65+\frac{7.6.5}{3.1.2.3}\cdot 794+\frac{7.6.5.4}{4.1.2.3.4}\cdot 4890+$$

$$+\frac{7.6.5.4.3}{5.1.2.3.4.5}\cdot 20515-\frac{7.6.5.4.3.2}{6.1.2.3.4.5.6}\cdot 67171+\frac{1}{7}\cdot 184820.$$

$$B_3=7-682-\frac{1}{2}+9263+\frac{1}{3}-42787-\frac{1}{2}+$$

$$+86163-78366-\frac{1}{6}+26402+\frac{6}{7}=\frac{1}{42}.$$

§ 3. Теперь докажемъ нѣсколько леммъ *).

Лемма I.

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

Доказательство.

Если равенство

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

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

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

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

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

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

Лемма II.

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

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

Доказательство.

По предыдущей леммѣ:

$$S_n(a.b.c\ldots k.l) \equiv b.c\ldots k.l.S_n(a),\ (\text{mod.}\ a),$$

$$S_n(a.b.c\ldots k.l) \equiv a.c\ldots k.l.S_n(b),\ (\text{mod.}\ b),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$S_n(a.b.c\ldots l) \equiv a.b.c\ldots l.S_n(k),\ (\text{mod.}\ k),$$

$$S_n(a.b.c\ldots k) \equiv a.b.c\ldots k.S_n(l),\ (\text{mod.}\ l).$$

Поэтому, разность

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

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

Лемма III.

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

Доказательство.

Равенство

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

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

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

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

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

Лемма IV.

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

Доказательство.

На основаніи леммы I-й

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

Но

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

и потому

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

или

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

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 $r=\varrho$, то справедлива и для $r=\varrho+1$.

Въ самомъ дѣлѣ, по леммѣ IV-й.

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

Поэтому:

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

Слѣдствіе.

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

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

Лемма VI.

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

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

Доказательство.

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

$$x^n \equiv 1\,,\ (\mathrm{mod.}\ p).$$

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

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

или

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

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:

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

Доказательство.

При всякомъ x, не дѣлящемся на p:

$$x \equiv r_1, \ (\mathrm{mod.}\ p),$$

$$2x \equiv r_2, \ (\mathrm{mod.}\ p),$$

$$\cdots\cdots$$

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

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

Возвышая предыдущія сравненія въ степень n и складывая, найдемъ:

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

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

$$x^n \equiv 1, \ (\mathrm{mod.}\ p),$$

и потому, необходимо:

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

Лемма VIII.

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

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

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

Лемма IX.

При p простомъ имѣетъ мѣсто сравненiе:

$$\frac{m(m-1)\ldots(m-p+1)}{1.2\ldots p}-\frac{m(m-1)\ldots(m-2p+1)}{1.2\ldots(2p)}+\ldots$$

$$\ldots+\frac{m(m-1)\ldots(m-kp+1)}{1.2\ldots(kp)}\equiv 1\,,\ (\mathrm{mod}.\,p)\,,$$

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

Доказательство.

По формулѣ (2) § 1

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

$$\ldots\pm\frac{1}{n}f(x+n).$$

Функцiя $f(x)$ степени не выше n-й.

Пусть

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

$$f(0)=0\,,$$

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

Поэтому:

$$1=n(1-1^{p-1})-\frac{n(n-1)}{1.2}(1-2^{p-1})+\ldots\pm\frac{n(n-1)\ldots1}{1.2\ldots n}(1-n^{p-1}).$$

Здѣсь n больше или равно p.

Разсматривая это равенство, какъ сравненiе по модулю p, найдемъ:

$$\frac{n(n-1)\ldots(n-p+1)}{1.2\ldots p}-\frac{n(n-1)\ldots(n-2p+1)}{1.2\ldots 2p}+\ldots$$

$$\ldots\pm\frac{n(n-1)\ldots(n-kp+1)}{1.2\ldots kp}\equiv 1\,,\ (\mathrm{mod}.\,p)\,,$$

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

§ 4. Теорема Штаудта.

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

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

Доказательство.

Мы вывели для B_k въ § 2 слѣдующую формулу:

$$(-1)^{k-1} B_k = \frac{n}{1}\frac{S_{2k}(1)}{1} - \frac{n(n-1)}{1.2}\cdot\frac{S_{2k}(2)}{2} + \ldots \pm \frac{n(n-1)\ldots 1}{1.2\ldots n}\cdot\frac{S_{2k}(n)}{n},$$

n больше $2k$.

По леммѣ VIII-й.

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

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

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

$$-\left[\frac{n(n-1)\ldots(n-\alpha+1)}{1.2\ldots\alpha} - \frac{n(n-1)\ldots(n-2\alpha+1)}{1.2\ldots(2\alpha)} + \ldots \right.$$
$$\left. \ldots \pm \frac{n(n-1)\ldots(n-k\alpha+1)}{1.2\ldots(k\alpha)}\right],$$

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

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

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

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

или

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

T есть цѣлое число.

Числа α, $\beta \ldots \lambda$ опредѣляются такимъ образомъ:

Выписываются всѣ дѣлители числа k, затѣмъ всѣ они удваиваются и къ полученнымъ числамъ прибавляютъ по единицѣ; всѣ образованные такимъ образомъ простыя числа будутъ искомыя α, $\beta, \ldots \lambda$. Къ нимъ прибавляется еще 2.

Примѣръ 1-й. $k=3$.

Дѣлители: 1, 3.

Числа 3, 7 простыя 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 простыя и потому:

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

Замѣчанiе.

Знаменатель всякаго Бернулліева числа, на основанiи теоремы Штаудта, равенъ произведенiю нѣкоторыхъ простыхъ чиселъ, взятыхъ множителями только по одному разу.

§ 5. Теорема.

При всякомъ N цѣломъ и положительномъ, имѣетъ мѣсто сравненiе:

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

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

Доказательство.

Мы имѣли (§ 2), что

$$\left.\begin{aligned} S_{2k}(N) = \frac{N^{2k+1}}{2k+1} + \frac{1}{2} N^{2k} + \frac{2k}{1.2} B_1 N^{2k-1} - \frac{2k.(2k-1).(2k-2)}{1.2.3.4} B_2 N^{2k-3} + \ldots \\ \ldots + (-1)^{k-2} \frac{2k.(2k-1)\ldots 4}{1.2\ldots(2k-2)} B_{k-1} N^3 + (-1)^{k-1} B_k N. \end{aligned}\right\} \quad (A)$$

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

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

$$N=b.d\,,$$

a и N числа взаимно простыя.

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

Получимъ:

$$a\Theta S_{2k}(N)=\Theta N^{2k}b+\frac{\Theta}{2}N^{2k}a+$$

$$+\frac{(2k+1)2k}{1.2}N^{2k-2}bB_1\Theta-\frac{(2k+1)\ldots(2k-2)}{1.2.3.4}N^{2k-4}bB_2\Theta+\ldots$$

$$\ldots+(-1)^{k-2}\frac{2k.(2k-1)}{1.2.3}aN^3B_{k-1}\Theta+(-1)^{k-1}B_k\Theta Na.$$

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

$$a.\Theta.S_{2k}(N)\equiv(-1)^{k-2}\frac{2k.(2k-1)}{1.2.3}aN^3B_{k-1}\Theta+(-1)^{k-1}B_k.\Theta.a.N,(\mathrm{mod.}\,N^3).$$

Умножаемъ обѣ части сравненія на 2.3, тогда будемъ имѣть:

$$2.3.a\Theta S_{2k}(N)\equiv(-1)^{k-1}2.3.a.N\Theta B_k\,,\ (\mathrm{mod.}\,N^3).$$

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

$$2.3.\Theta.S_{2k}(N)\equiv(-1)^{k-1}2.3.N\Theta B_k\,,\ (\mathrm{mod.}\,N^3).$$

Пусть

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

Замѣтимъ, что по теоремѣ Штаудта Θ_k всегда дѣлится на 2.3, а потому, Θ' не дѣлится на 2.3, такъ какъ Θ есть наименьшее кратное k знаменателей $\Theta_1, \Theta_2 \ldots \Theta_k$.

Такимъ образомъ:

$$2.3.\Theta'.\Theta_k.S_{2k}(N)\equiv(-1)^{k-1}2.3.\Theta'.N.P_k\,,\ (\mathrm{mod.}\,N^3).$$

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

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

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 разсматриваемъ, какъ сравненіе по модулю N^2; найдемъ:

$$6.S_2(N) \equiv N,\ (\text{mod. } N^2).$$

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

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

§ 6. Лемма X.

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

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

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

Доказательство.

Возьмемъ рядъ равенствъ:

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

Числа r_1, $r_2 \ldots r_{N-1}$ всѣ меньше N и всѣ между собой различны, а потому, r_1, $r_2 \ldots r_{N-1}$ представляютъ рядъ чиселъ: $1, 2, \ldots (N-1)$, только иначе расположенныхъ.

Равенства (B) перепишемъ иначе:

$$a - NE\frac{a}{N} = r_1,$$

$$2a - NE\frac{2a}{N} = r_2,$$

$$\cdots\cdots\cdots$$

$$(N-1)a - NE\frac{(N-1)a}{N} = r_{N-1},$$

и возвысимъ обѣ части всѣхъ этихъ равенствъ въ степень m.

$$a^m - mNa^{m-1}E\frac{a}{N} + \ldots = r_1^m,$$

$$2^m a^m - mNa^{m-1}2^{m-1}E\frac{2a}{N} + \ldots = r_2^m,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$(N-1)^m a^m - mNa^{m-1}(N-1)^{m-1}E\frac{(N-1)a}{N} + \ldots = r_{N-1}^m.$$

Равенства эти разсматриваемъ, какъ сравненія по модулю N^2:

$$a^m - mNa^{m-1}E\frac{a}{N} \equiv r_1^m, \ (\text{mod. } N^2),$$

$$2^m a^m - mNa^{m-1}2^{m-1}E\frac{2a}{N} \equiv r_2^m, \ (\text{mod. } N^2),$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$(N-1)^m a^m - mNa^{m-1}(N-1)^{m-1}E\frac{(N-1)a}{N} \equiv r_{N-1}^m, \ (\text{mod. } N^2).$$

Складывая всѣ эти сравненія почленно, найдемъ:

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

или

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

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

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

§ 7. Теорема.

При произвольныхъ цѣлыхъ и положительныхъ числахъ a и N:

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

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

Доказательство.

По теоремѣ § 5:

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

По леммѣ X-й:

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

Умножаемъ обѣ части перваго сравненія на $(a^{2m} - 1)$, второго на Θ_m и вычитаемъ полученныя сравненія почленно. Найдемъ:

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

Или, сокращая на N, окончательно:

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

Слѣдствіе I.

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

$$P_m(a^{2m} - 1) \equiv 0, \text{ (mod. } m), \quad \ldots\ldots\ldots (*)$$

a есть произвольное цѣлое положительное число простое съ m.

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

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

$$a_1^{2m} - 1 \equiv 0, \ (\text{mod.}\, p_1).$$

Поэтому, на основаніи сравненія (*):

$$P_m \equiv 0, \ (\text{mod.}\, p_1^\alpha).$$

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

$$P_m \equiv 0, \ (\text{mod.}\, p_2^\beta)$$

и т. д. Наконецъ

$$P_m \equiv 0, \ (\text{mod.}\, p_l^\lambda).$$

Изъ этихъ сравненій слѣдуетъ, что P_m дѣлится на $p_1^\alpha\, p_2^\beta \ldots p_l^\lambda$ 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 Бернулліевыхъ чиселъ проф. Adams'a: $P_{25} = 4950572052410796482124775 25$, число дѣлящееся на 25.

Замѣчаніе.

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

Слѣдствіе II.

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

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

Если $N = p_1^\alpha\, p_2^\beta \ldots p_l^\lambda$, то $\varphi(N) = p_1^\alpha\, p_2^\beta \ldots p_l^\lambda\, \dfrac{p_1 - 1}{p_1} \cdot \dfrac{p_2 - 1}{p_2} \cdots \dfrac{p_l - 1}{p_l}$.

Примѣняя теорему § 7, найдемъ:

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

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

$$a^{2n-1} \equiv a^{2m-1}, \ (\text{mod.}\, N).$$

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

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

Предполагая, что это условіе выполнено, будемъ имѣть:

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

Поэтому, умножая обѣ части сравненія:

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

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

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

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

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

Замѣтимъ, что

$$a^{2m}-1 \equiv a^{2n}-1, \ (\text{mod.}\, N).$$

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

$$(-1)^{n-1}\frac{m.\Theta_m.P_n}{2.3}\equiv(-1)^{m-1}\frac{n.\Theta_n.P_m}{2.3},\ (\mathrm{mod.}\ N);\ \ .\ \ .\ \ .\ \ (^{**})$$

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

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

k есть произвольное цѣлое положительное число; $2m-1$ должно быть больше или равно наивысшему изъ показателей степеней α, β,...λ.

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

Примѣръ.

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

Рѣшеніе.

Пусть $N=200=2^3.5^2$; $\varphi(N)=2^2.5.4.1=80$; $m=3$;

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

$$n=43,\ \text{при}\ k=1.$$

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

Поэтому:

$$(-1)^{42}3.\frac{\Theta_3}{2.3}.P_{43}(a^{86}-1)\equiv(-1)^2 43.\frac{\Theta_{43}}{2.3}.P_3(a^6-1),\ (\mathrm{mod.}\ 200).$$

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

Дѣлители 43 суть 1 и 43.

Число $2.43+1=87$ не простое и потому, $\Theta_{43}=2.3$.

Итакъ:

$$3.\frac{42}{2.3}.P_{43}(a^{86}-1)\equiv 43.\frac{6}{2.3}.(a^6-1),\ (\mathrm{mod.}\ 200).$$

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

$$a^6-1\equiv a^{86}-1,\ (\mathrm{mod.}\ 200),$$

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

$$3.7.P_{43} \equiv 43\,, \text{ (mod. 50)}$$

или

$$21.P_{43} \equiv -7\,, \text{ (mod. 50)},$$

$$3.P_{43} \equiv -1\,, \text{ (mod. 50)},$$

$$P_{43} \equiv 33\,, \text{ (mod. 50)}.$$

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

$$N = P_m = p_1^{\alpha} p_2^{\beta} \cdots p_l^{\lambda},$$

$$(-1)^{n-1} \frac{m.\Theta_m}{2.3}.P_n \equiv 0\,, \text{ (mod. } P_m).$$

Θ_m не можетъ имѣть дѣлителей общихъ съ P_m и потому:

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

Примѣръ.

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

691 есть число простое и потому,

$$6.P_{6+k\frac{691-1}{2}} \equiv 0\,, \text{ (mod. 691)},$$

т. е. всѣ числа вида

$$P_{6+345.k}$$

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:

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

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

$$ax \equiv 1, \ (\mathrm{mod.}\ N).$$

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

$$a^2-1 \equiv 12a \sum_{i=1}^{i=N-1} iE\frac{ai}{N}, \ (\mathrm{mod.}\ N)$$

или

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

Очевидно, что

$$x \equiv a-12\sum_{i=1}^{i=N-1} iE\frac{ai}{N}, \ (\mathrm{mod.}\ N)$$

будетъ рѣшеніемъ сравненія

$$ax \equiv 1, \ (\mathrm{mod.\ N}).$$

Примѣръ.

Рѣшить сравненіе:

$$5x \equiv 1, \ (\mathrm{mod.}\ 13).$$

$$\sum_{i=1}^{i=12} iE\frac{5i}{13} = 1.0+2.0+3.1+4.1+5.1+6.2+7.2+8.3+$$

$$+9.3+10.3+11.4+12.4=211.$$

Поэтому

$$\sum_{i=1}^{i=12} iE\frac{5i}{13} \equiv 3, \ (\mathrm{mod.}\ 13)$$

и

$$x \equiv 5-12.3 \equiv 5+3 \equiv 8, \ (\mathrm{mod.}\ 13).$$

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

$$5x \equiv 1. \ (\mathrm{mod.}\ 13).$$

Формулу

$$x \equiv a-12\sum_{i=1}^{i=N-1} iE\frac{ai}{N}, \ (\mathrm{mod.}\ N)$$

можно преобразовать въ другую, болѣе удобную для вычисленій:

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

но мы не считаемъ нужнымъ на этомъ останавливаться.

Прилагая ее къ предыдущему примѣру, найдемъ:

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

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

Поэтому:

$$x \equiv -2.5 + 3 + 6.9 \equiv 8, \ (\text{mod.}\, 13).$$

Петербургъ.
5 Октября 1889 года.