Замѣтка о рѣшеніи двучленныхъ сравненій съ простымъ модулемъ по способу Коркина.

К. Поссе.

Въ посмертномъ мемуарѣ Коркина, напечатанномъ въ 1-мъ вып. XVII тома Математическаго Сборника, авторъ даетъ способъ рѣшенія двучленныхъ сравненій, безъ помощи таблицы индексовъ. Способъ этотъ, основанный на вполнѣ элементарныхъ соображеніяхъ, могъ-бы войти въ курсы теоріи чиселъ, читаемые въ университетахъ, и составить интересный отдѣлъ этихъ курсовъ.

Объёмистый мемуаръ, въ которомъ изложенъ этотъ способъ, содержитъ въ себѣ однако многое, не относящееся непосредственно къ рѣшенію двучленныхъ сравненій. Намъ кажется, что отдѣльное изложеніе этого способа, болѣе сжатое и упрощенное въ нѣкоторыхъ подробностяхъ, можетъ, до нѣкоторой степени, облегчить ознакомленіе съ его сущностью и способствовать введенію его въ предметъ преподаванія. Съ этой цѣлью и составлена настоящая замѣтка.

Способъ Коркина основанъ на разсмотрѣніи нѣкоторыхъ чиселъ, которымъ авторъ далъ названіе *характеровъ*. Въ первомъ параграфѣ мы даемъ опредѣленіе и указываемъ главныя свойства характеровъ, во второмъ— приложеніе ихъ къ рѣшенію двучленныхъ сравненій, въ третьемъ поясняемъ способъ рѣшенія примѣрами, пользуясь таблицею первообразныхъ корней и характеровъ, составленною Коркинымъ для всѣхъ простыхъ модулей, не превышающихъ 4000, и продолженною нами для всѣхъ простыхъ модулей, не превышающихъ 10000. (См. Математическій Сборникъ т. XVII, вып. 1 и 2), Послѣдній параграфъ заключаетъ въ себѣ нѣкоторыя замѣчанія о вычисленіи первообразныхъ корней и доказательство одной теоремы Коркина, связывающей вопросъ о разысканіи первообразныхъ корней съ рѣшеніемъ сравненій.

§ 1.

Положимъ, что p обозначаетъ данное простое число, q — какой нибудь простой дѣлитель $p-1$, и α — показатель его кратности, такъ что

$$p-1=q^\alpha \cdot N,$$

гдѣ N не дѣлится на q.

Главными характерами или характерами перваго порядка и степени q для даннаго числа p, называются рѣшенія сравненія

$$x^q - 1 \equiv 0 \pmod{p}; \quad \ldots\ldots (1)$$

число ихъ равно q, и обозначая ихъ черезъ

$$1,\ u_1,\ u_2, \ldots u_{q-1},$$

можемъ положить

$$u_i \equiv [u_1]^i \pmod{p}, \quad \ldots\ldots (2)$$

т. е. разсматривать нижній значекъ въ u_i, какъ показатель степени, въ которую надо возвысить u_1, чтобы получить число, сравнимое съ u_i по модулю p.

Замѣтимъ, что во всемъ послѣдующемъ, говоря о вычисленіи какого-нибудь цѣлаго числа A, мы будемъ подразумѣвать, что вычисляется не само число A, а абсолютно-наименьшій его вычетъ по модулю p, т. е. число, заключающееся въ ряду

$$0, \pm 1, \pm 2, \ldots \pm \frac{p-1}{2}$$

сравнимое съ A по модулю p. Для вычисленія главныхъ характеровъ мы можемъ положить

$$u_1 \equiv g^{\frac{p-1}{q}}, \quad \ldots\ldots (3)$$

гдѣ g — первообразный корень или, общнѣе, какой нибудь невычетъ степени q, простого числа p, и примѣнить затѣмъ формулу (2) для $i = 1, 2, \ldots (q-1)$. При $\alpha > 1$, кромѣ главныхъ характеровъ, существуютъ еще характеры 2-го, 3-го и т. д. порядковъ, до порядка α включительно, опредѣляемые слѣдующимъ образомъ. Характерами 2-го порядка, степени q, называются рѣшенія сравненія

$$\frac{x^{q^2} - 1}{x^q - 1} \equiv 0 \pmod{p} \quad \ldots\ldots (4)$$

Число ихъ равно $q(q-1)$; одинъ изъ нихъ, u_1', получимъ, положивъ

$$u_1' \equiv g^{\frac{p-1}{q^2}} \pmod{p}; \quad \ldots\ldots (5)$$

гдѣ g имѣетъ тоже самое значеніе, какъ въ формулѣ (3); а всѣ характеры 2-го порядка получимъ, давая значку i въ формулѣ

$$u_i \equiv [u_1']^i \pmod{p} \quad \ldots\ldots (6)$$

значенія 1, 2, 3, ... $q-1$ и умножая каждое изъ чиселъ

$$u_1', \ u_2', \ \dots u_{q-1}'$$

на всѣ характеры перваго порядка.

Вообще, характерами порядка μ, $(1 < \mu \leqq \alpha)$, называются рѣшенія сравненія

$$\frac{x^{q^\mu}-1}{x^{q^{\mu-1}}-1} \equiv 0 \pmod{p} \dots\dots\dots\dots\dots\dots\dots (7)$$

Число ихъ равно $q^{\mu-1}(q-1)$; одинъ изъ нихъ, $u_1^{(\mu-1)}$, получимъ, полагая

$$u_1^{(\mu-1)} \equiv g^{\frac{p-1}{q^\mu}} \pmod{p} \dots\dots\dots\dots\dots\dots (8)$$

гдѣ g имѣетъ тоже самое значеніе, какъ въ формулѣ (3); а всѣ характеры порядка μ найдемъ, давая значку i въ формулѣ

$$u_i^{(\mu-1)} \equiv [u_1^{(\mu-1)}]^i \pmod{p} \dots\dots\dots\dots (9)$$

значенія 1, 2, ... $q-1$ и умножая числа

$$u_1^{(\mu-1)}, \ u_2^{(\mu-1)}, \dots u_{q-1}^{(\mu-1)}$$

на всѣ характеры 1-го, 2-го, ... $(\mu-1)$-го порядка.

Изъ формулъ (3), (5), (8) и т. д. вытекаютъ слѣдующія основныя формулы

$$u_i^q \equiv 1, \ [u_i']^q \equiv u_i, \ [u_i'']^q \equiv u_i', \ \dots [u_i^{(\alpha-1)}]^q \equiv u_i^{(\alpha-2)} \pmod{p} \dots\dots (10)$$

$$(i = 1, \ 2, \ 3, \dots q-1)$$

а отсюда и болѣе общая формула

$$[u_l^{(\lambda)} u_m^{(\mu)} \dots u_n^{(\nu)}]^q \equiv u_l^{(\lambda-1)} u_m^{(\mu-1)} \dots u_n^{(\nu-1)} \pmod{p} \dots\dots (11)$$

въ которой нижніе значки (показатели степеней) могутъ имѣть любое изъ значеній 1, 2, ... $q-1$, а верхніе служатъ указателями порядковъ характеровъ.

Эта формула выражаетъ основное для рѣшенія двучленныхъ сравненій правило: *Если какое нибудь число U представлено въ видѣ произведенія характеровъ различныхъ порядковъ:*

$$U \equiv u_l^{(\lambda-1)} u_m^{(\mu-1)} \dots u_n^{(\nu-1)} \pmod{p.} \dots\dots\dots (12)$$

то, для полученія числа Ω, удовлетворяющаго сравненію

$$\Omega^q \equiv U \ (\text{mod. } p) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (13)$$

стоитъ только увеличить на одну единицу всѣ верхніе значки въ выраженіи U, оставляя нижніе безъ измѣненія.

Къ этому можно добавить, что всякое другое рѣшеніе сравненія (13) будетъ равно найденному указаннымъ путемъ, умноженному на одно изъ рѣшеній сравненія

$$x^q \equiv 1 \ (\text{mod. } p)$$

т. е. на одинъ изъ главныхъ характеровъ.

Замѣтимъ еще формулу

$$u_i^{(\mu)} u_{q-i}^{(\mu)} \equiv u_1^{(\mu-1)} \ (\text{mod. } p) \ldots\ldots\ldots\ldots\ldots (14)$$

вытекающую изъ формулъ

$$u_i^{(\mu)} \equiv [u_1^{(\mu)}]^i; \ [u_1^{(\mu)}]^q \equiv u_1^{(\mu-1)} \ (\text{mod. } p.$$

Кубическіе характеры, при $q = 3$, мы будемъ обозначать буквами z съ различными значками; главные кубическіе характеры

$$1, \ z_1, \ z_2$$

будутъ рѣшеніями сравненія

$$x^3 - 1 \equiv 0 \ (\text{mod. } p);$$

числа z_1 и z_2 — рѣшеніями сравненія

$$x^2 + x + 1 \equiv 0 \ (\text{mod. } p),$$

такъ что

$$z_2 \equiv z_1^2 \equiv -z_1 - 1 \ (\text{mod. } p) \ldots\ldots\ldots\ldots\ldots (15)$$

Квадратичные характеры, при $q = 2$, мы будемъ обозначатъ буквами f, f', f''......; главные квадратичные характеры суть 1 и —1, характеры 2-го порядка, $\pm f$, удовлетворяютъ сравненію

$$f^2 \equiv -1 \ (\text{mod. } p).$$

Если
$$p - 1 = 2^\alpha . \ 3^\beta . \ q^\gamma . \ r^\delta . \ s^\varepsilon,$$

(при $p < 10000$ больше трехъ различныхъ простыхъ множителей, отличныхъ отъ 2 и 3, въ разложеніе $p - 1$ не входитъ), и

$$3 < q < r < s,$$

то буквами u, v, w будутъ обозначены характеры степеней, соотвѣтственно, q, r, s. Въ таблицахъ помѣщено всегда только по одному характеру каждой степени и каждаго порядка,—

$$z,\ z',\ldots u,\ u',\ldots;\ v,\ v',\ldots$$

причемъ нижній значекъ 1 подразумѣвается; характеры

$$u_i,\ u'_i,\ldots v_i,\ v'_i,\ldots (i>1),$$

когда въ нихъ встрѣчается надобность, должны быть вычислены возвышеніемъ табличныхъ въ степень i; z_2 получается по табличному z по формулѣ (15).

§ 2.

1. Переходя къ рѣшенію двучленныхъ сравненій съ помощью характеровъ, мы можемъ ограничиться сравненіями

$$x^q \equiv a \pmod{p}, \ldots\ldots\ldots\ldots (16)$$

гдѣ q простой дѣлитель числа $p-1$, потому что, какъ извѣстно, къ этому случаю сводятся всѣ другіе.

Извѣстно, что сравненіе (16) имѣетъ рѣшенія тогда и только тогда, когда a вычетъ степени q простого числа p, т. е. когда

$$a^{\frac{p-1}{q}} \equiv 1 \pmod{p} \ldots\ldots\ldots\ldots (17)$$

Наконецъ извѣстно, что при выполненіи условія (17) сравненіе (16) имѣетъ q рѣшеній, получаемыхъ черезъ умноженіе одного изъ нихъ на всѣ рѣшенія сравненія

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

т. е. на всѣ главные характеры степени q. Остается показать, какъ найти одно рѣшеніе сравненія (16).

Полагая, какъ выше,

$$p-1 = q^\alpha N,$$

гдѣ N не дѣлится на q, положимъ, что

$$N = qN' + s, \text{ гдѣ } |s| < q.$$

Опредѣлимъ затѣмъ какія нибудь два числа τ и σ, цѣлыя и положительныя, удовлетворяющія уравненію

$$q\tau - s\sigma = 1; \ldots\ldots\ldots\ldots (18)$$

при $s = -1$, можно взять

$$\tau = 0,\ \sigma = 1,$$

а вообще выгодно за τ и σ принимать наименьшія числа, удовлетворяющія уравненію (18).

Положимъ далѣе, что нашли какимъ-нибудь образомъ число Ω, удовлетворяющее сравненію

$$\Omega^q \equiv a^N \ (\mathrm{mod.}\ p) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (19)$$

Тогда, опредѣливъ число φ, по сравненію

$$\varphi\Omega \equiv 1 \ (\mathrm{mod.}\ p) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (20)$$

мы найдемъ одно рѣшеніе x_1 сравненія (16), по формулѣ

$$x_1 \equiv a^{N'\sigma+\tau}\varphi^\sigma \ (\mathrm{mod.}\ p) \ldots\ldots\ldots\ldots\ldots\ldots (21)$$

Въ самомъ дѣлѣ

$$x_1^q \equiv a^{(N'\sigma+\tau)q}\varphi^{q\sigma},$$

или замѣчая, что

$$q\tau = s\sigma + 1,$$

$$x_1^q \equiv a.[a^{N'q+s}\varphi^q]^\sigma \equiv a.[a^N\varphi^q]^\sigma;$$

но

$$a^N\varphi^q \equiv [\Omega\varphi]^q \equiv 1 \ (\mathrm{mod.}\ p);$$

Слѣдовательно

$$x_1^q \equiv a, \ (\mathrm{mod.}\ p)$$

что и требовалось показать.

Итакъ, все дѣло сводится къ нахожденію числа Ω, удовлетворяющаго сравненію (19), а для этого и послужатъ характеры.

Вычисляемъ послѣдовательно числа

$$a^N,\ a^{qN},\ a^{q^2N}, \ldots a^{q^{\alpha-1}N}; \ldots\ldots\ldots\ldots\ldots\ldots (22)$$

Рано или поздно получимъ въ этомъ рядѣ число, сравнимое съ 1, потому что послѣднее изъ нихъ

$$a^{q^{\alpha-1}N} = a^{\frac{p-1}{q}},$$

по условію, сравнимо съ 1. Пусть первое изъ чиселъ ряда (22), сравнимое съ 1, есть

$$a^{q^{n-1}N},$$

такъ-что

$$a^{q^{n+1}N} \equiv 1,\ a^{q^nN} \text{не} \equiv 1 \ (\mathrm{mod.}\ p).$$

Положимъ, для сокращенія,

$$a^{q^n N} = U,\ a^{q^{n-1} N} = U',\ldots a^N = U^{(n)}.$$

Замѣчая, что

$$U^q = a^{q^{n+1} N} \equiv 1 \pmod{p}$$

найдемъ, что U сравнимо съ однимъ изъ главныхъ характеровъ

$$u_1,\ u_2,\ldots u_{q-1},$$

и, такъ-какъ U число намъ извѣстное, то будемъ знать, съ какимъ именно изъ этихъ характеровъ оно сравнимо; положимъ, что

$$U \equiv u_k \pmod{p}.$$

Замѣчая, что

$$[U']^q \equiv U \equiv u_k \pmod{p},$$

на основаніи правила § 1, найдемъ, что

$$U' = a^{q^{n-1} N} \equiv u_k'.\lambda \pmod{p}\ldots\ldots\ldots\ldots\ldots\ldots(23)$$

гдѣ λ равно одному изъ главныхъ характеровъ

$$1,\ u_1,\ u_2,\ldots u_{q-1}$$

и можетъ быть найдено рѣшеніемъ сравненія (23) или другимъ путемъ, о которомъ скажемъ дальше.

Если $\lambda = 1$, то

$$U' \equiv u_k' \pmod{p},$$

а замѣчая, что

$$[U'']^q \equiv U' \equiv u_k' \pmod{p},$$

найдемъ

$$U'' = a^{q^{n-2} N} \equiv u_k''.\mu \pmod{p},$$

гдѣ μ есть одно изъ чиселъ

$$1,\ u_1,\ u_2,\ldots u_{q-1},$$

такъ-что для U'' найдемъ

$$U'' \equiv u_k'' \text{ или } U'' \equiv u_k'' u_m.$$

Если $\lambda \equiv u_l$, то

$$U' \equiv u_k' u_l \pmod{p},$$

а

$$U'' \equiv u_k'' u_l' \nu \pmod{p},$$

гдѣ ν одинъ изъ главныхъ характеровъ, такъ-что

$$U'' \equiv u''_k u'_l \text{ или } U'' \equiv u''_k u'_l u_m \pmod{p}.$$

Такимъ путемъ мы выразимъ послѣдовательно всѣ числа ряда (22), до a^N включительно, въ видѣ произведенія характеровъ, а затѣмъ по формулѣ (11) § 1, получимъ и число Ω, а слѣдовательно и рѣшеніе даннаго сравненія. Можно замѣтитъ, что въ выраженіе a^N войдутъ характеры не выше n-го, и въ Ω не выше $(n+1)$-го порядка.

2. Для нахожденія чиселъ λ, μ, ν, ... и φ нѣтъ надобности рѣшать сравненія первой степени, которыми эти числа опредѣляются. Можно примѣнить другой пріемъ, основанный на формулѣ (14) § 1, сущность котораго состоитъ въ постепенномъ пониженіи порядка характеровъ, входящихъ въ коеффиціентъ при искомомъ числѣ, пока не приведемъ этотъ коеффиціентъ къ 1. Пояснимъ этотъ пріемъ на опредѣленіи μ изъ сравненія

$$U'' \equiv u''_k \mu \pmod{p}$$

Умножая обѣ части сравненія на u''_{q-k} и замѣчая, что

$$u''_k u''_{q-k} \equiv [u''_1]^q \equiv u'_1 \pmod{p},$$

получимъ

$$u''_{q-k} U'' \equiv u'_1 . \mu \pmod{p};$$

умножая обѣ части этого сравненія на u'_{q-1}, получимъ

$$u'_{q-1} u''_{q-k} U'' \equiv u_1 . \mu \pmod{p},$$

и наконецъ

$$u_{q-1} u'_{q-1} u''_{q-k} U'' \equiv \mu \pmod{p}.$$

3. Въ частномъ случаѣ, когда

$$a^N \equiv 1 \pmod{p},$$

что всегда имѣетъ мѣсто при $\alpha = 1$, потому, что тогда

$$a^{\frac{p-1}{q}} = a^N,$$

а можетъ имѣть мѣсто и при $\alpha > 1$, рѣшеніе вопроса упрощается. Тогда, очевидно, можно положить

$$\Omega \equiv 1 \text{ и } \varphi \equiv 1$$

и одно рѣшеніе сравненія (1) будетъ

$$x_1 \equiv a^{N'\sigma+\tau},$$

а остальныя $q-1$ рѣшеній будутъ

$$x_1u_1,\ x_1u_2, \ldots x_1u_{q-1},$$

т. е. получаются съ помощью однихъ главныхъ характеровъ.

Для сравненій 2-й степени, т. е. при $q=2$, всегда можно положить

$$N=2N'-1,\ \tau=0,\ \sigma=1,$$

такъ что общая формула для рѣшеній сравненія 2-й степени

$$x^2\equiv a\ (\text{mod. } p)$$

будетъ

$$x\equiv\pm a^{\frac{N+1}{2}}\varphi\ (\text{mod. } p)$$

При $\alpha=1$, т. е. для чиселъ p вида

$$p=4n+3,\ p-1=2N,$$

гдѣ N — нечетное, получается извѣстная формула

$$x\equiv\pm a^{\frac{p+1}{4}}\ (\text{mod. } p).$$

При $\alpha=2$, $p-1=4N$, гдѣ N — нечетное, т. е. для чиселъ p вида

$$p=8n+5,$$

имѣемъ

$$a^{\frac{p-1}{2}}\equiv a^{2N}\equiv 1\ (\text{mod. } p)$$

откуда

$$1)\ a^N\equiv 1 \text{ или } 2)\ a^N\equiv -1.$$

Случай 1) уже разсмотрѣнъ, а во 2-мъ

$$\Omega\equiv f,\ \varphi\equiv -f$$

и

$$x\equiv\pm fa^{\frac{N+1}{2}}\ (\text{mod. } p)$$

гдѣ f — квадратный характеръ 2-го порядка. Этотъ случай разобранъ, между прочимъ въ сочиненіи J. Serret. Cours d' Algèbre supérieure, 4-me éd. T. II, pag. 125, но болѣе сложнымъ путемъ.

При $\alpha>2$, рѣшеніе сравненій 2-ой степени, если a^N не $\equiv 1$ (mod. p), требуетъ разсмотрѣнія характеровъ порядка выше 2-го. При этомъ полезно замѣтить слѣдующую формулу.

$$-f.f'f''\ldots f^{(n-1)}f^{(n)^2}\equiv 1\ (\text{mod. } p)\ldots\ldots(24)$$

вытекающую непосредственно изъ основныхъ

$$f^{(n)^2} \equiv f^{(n-1)}, \ldots f'^2 \equiv f,\ f^2 \equiv -1,$$

и дающую прямо выраженіе числа φ, удовлетворяющаго сравненію

$$\varphi\Omega \equiv 1 \pmod{p}$$

по данному Ω. Напр. если

$$\Omega \equiv f'' f^{IV}, \text{ то } \varphi \equiv -ff'f''' f^{IV}.$$

§ 3.

Примѣры *).

1. $$x^2 \equiv 2 \pmod{6337}.$$

$$p-1 = 2^6.3^2.11 = 2^6.N,\ N = 99,\ \frac{N+1}{2} = 50$$

$$x \equiv \pm\varphi.2^{50} \pmod{6337}.$$

Вычисленіе 2^{50} и $2^{99} = a^N$.

$$2^9 = 512,\ 2^{10} = 1024,\ 2^{19} \equiv -1683,\ 2^{20} \equiv 2971,$$

$$2^{40} \equiv -600,\ \underline{2^{50} \equiv 289},\ 2^{80} \equiv -1209,\ \underline{\underline{2^{99} \equiv a^N \equiv 570}}$$

Таблица характеровъ даетъ

$$f^{IV} \equiv -2521,\ f''' \equiv -570,\ f'' \equiv 1713,\ f' \equiv 338,\ f \equiv 178.$$

Поэтому

$$a^N \equiv -f''',\ \Omega \equiv ff^{IV}, \text{ откуда}$$

$$\varphi \equiv -f^{IV}f'''f''f' \equiv 2926,$$

$$x \equiv \pm 2926.289 \equiv \pm 2793.$$

---

*) Въ приложеніяхъ къ частнымъ примѣрамъ полезно въ каждомъ частномъ случаѣ предварительно выписать табличку чиселъ p, $2p$, $3p, \ldots 9p$, гдѣ p данный модуль, которая и послужитъ для дѣленія на p или, точнѣе, для вычисленія абсолютно—наименьшихъ вычетовъ по модулю p. Что касается умноженій, которыя надо выполнять надъ этими вычетами, то для сокращенія этихъ выкладокъ можно съ успѣхомъ пользоваться таблицами умноженія многозначныхъ чиселъ, напр. Neue Rechentafeln D-r. Peters, (Berlin, bei Reimer, 1909).

2. $$x^2 \equiv 3 \pmod{8941}$$

$$p-1=2^2 3.5.149=2^2 N. \quad (p=8n+5)$$

$$N=2235, \quad \frac{N+1}{2}=1118, \quad x \equiv \pm \varphi . 3^{1118}.$$

Вычисленіе 3^{1118} и $a^N = 3^{2235}$.

$$3^9 \equiv 1801, \quad 3^{18} \equiv -1982, \quad 3^{36} \equiv 3225,$$

$$3^{37} \equiv 734, \quad 3^{74} \equiv 2296, \quad 3^{148} \equiv -3574,$$

$$3^{149} \equiv -1781 = \omega, \quad 1117 = 149.7 + 74,$$

$$3^{1117} \equiv \omega^7 . 3^{74}; \quad \omega^2 \equiv -2094, \quad \omega^3 \equiv 1017,$$

$$\omega^6 \equiv -2867, \quad \omega^7 \equiv 816, \quad 3^{1117} \equiv -4074.$$

$$\underline{3^{1118} \equiv -3281,} \quad 3^{2234} \equiv 4074^2 \equiv 2980,$$

$$a^N \equiv 3^{2235} \equiv 8940 \equiv -1 \pmod{8941}$$

Отсюда
$$\Omega \equiv f, \quad \varphi \equiv -f,$$

по таблицѣ
$$f \equiv -3080,$$

и потому
$$x \equiv \pm 3281.3080 \equiv \pm 2150.$$

---

3. $$x^2 \equiv 5 \pmod{9941}.$$

$$p-1=2^2 2485, \quad N=2485, \quad \frac{N+1}{2} \equiv 1243$$

Вычисленіе дастъ

$$5^{1243} \equiv 2351, \quad a^N \equiv 5^{2485} \equiv 1, \quad \varphi \equiv 1, \quad x \equiv \pm 2351.$$

---

4. $$x^3 \equiv 11 \pmod{8461}.$$

$$p-1=3^2 940, \quad N=940=3.313+1,$$

$$N'=313, \quad s=1, \quad q=3;$$

$$3\tau-\sigma=1, \quad \tau=1, \quad \sigma=2.$$

$$x_1 \equiv a^{N'\sigma+\tau}\varphi^2 \equiv 11^{627}\varphi^2 \pmod{8461}.$$

Вычисленіе 11^{627} и $a^N = 11^{940}$ даетъ

$$11^{627} \equiv 2908 \text{ и } a^N \equiv 1,\ \varphi = 1,$$

$$x_1 \equiv 2908.$$

Таблица характеровъ даетъ

$$z_1 \equiv -1777,\ z_2 \equiv 1776;$$

три рѣшенія будутъ

$$x_1 \equiv 2908,\ x_1 z_1 \equiv 2155,\ x_1 z_2 \equiv 3398.$$

---

5. $$x^3 \equiv 3 \pmod{6967}$$

$$p - 1 = 3^4 . 86,\ N = 86 = 3 . 29 - 1,$$

$$\tau = 0,\ \sigma = 1,\ x_1 \equiv 3^{29} . \varphi,$$

$$\Omega^3 \equiv a^N \equiv 3^{86},\ \varphi \Omega \equiv 1 \ (\text{mod. } p)$$

$$3^{29} \equiv 2213,\ a^N = 3^{86} \equiv 1810,$$

$$a^{3N} \equiv 1894,\ a^{3^2 N} \equiv -383,\ a^{3^3 N} \equiv 1.$$

Таблица характеровъ даетъ:

$$z_1''' \equiv -1559,\ z_1'' \equiv 1510,\ z_1' \equiv -1060,$$

$$z_1 \equiv -383,\ z_2 \equiv 382.$$

Слѣдовательно

$$a^{3^2 N} \equiv z_1,$$

отсюда

$$1894 \equiv a^{3N} \equiv z_1' \lambda, \ \ldots\ldots\ldots\ldots\ldots\ldots (25)$$

гдѣ

$$\lambda^3 \equiv 1.$$

По (25) находимъ

$$1894 z_2' \equiv z_1 . \lambda,\ 1894 z_2' . z_2 \equiv \lambda;$$

$$z_2' \equiv 1060^2 \equiv 1913,\ \lambda \equiv 1894 . 1913 . 282 \equiv -383 \equiv z_1.$$

Поэтому

$$a^{3N} \equiv z_1' . z_1$$

и

$$a^N \equiv z_1'' z_1' . \mu, \text{ гдѣ } \mu^3 \equiv 1.$$

Замѣчая, что

$$z_1'' z_1' \equiv 1810 \equiv a^N,$$

находимъ

$$\mu = 1,$$

и

$$a^N \equiv z''_1 z'_1.$$

Отсюда

$$\Omega \equiv z'''_1 z''_1,$$

и

$$z'''_1 z''_1 \varphi \equiv 1;\; z''_2 \varphi \equiv z'''_2,$$

$$z'''_1 z''_1 \varphi \equiv 1;\; z''_2 \varphi \equiv z'''_2,$$

$$z'_1 \varphi \equiv z'''_2 . z''_1$$

и наконецъ

$$\varphi \equiv z'''_2 z''_1 z'_2 . z_2 \ldots\ldots\ldots\ldots\ldots\ldots (26)$$

$$z'''_2 \equiv 1559^2 \equiv -1002,$$

$$\varphi \equiv -1002 . 1510 . 1913 . 382 \equiv 2479.$$

Рѣшенія:

$$x_1 \equiv 2479 . 2213 \equiv 2998.$$

$$x_2 \equiv z_1 x_1 \equiv 2189,\; x_3 \equiv x_1 z_2 \equiv 2648.$$

6.
$$x^7 \equiv 2 \pmod{6959}.$$

$$p - 1 = 7^2 142,\; N \equiv 142 \equiv 7 . 20 + 2,$$

$$7\tau - 2\sigma = 1,\; \tau = 1,\; \sigma = 3.$$

$$x_1 \equiv 2^{61} . \varphi^3 \pmod{p}.$$

$$2^{61} \equiv -1469,\; 2^{142} \equiv a^N \equiv -2158.$$

Таблица характеровъ даетъ

$$u_1 \equiv -2158,\; u'_1 \equiv -3475;$$

Слѣдовательно

$$a^N \equiv u_1,\; \Omega \equiv u'_1 \equiv -3475;$$

$$-3475 \varphi \equiv 1 \pmod{6959},$$

откуда

$$\varphi \equiv -773.$$

(Это число можно было вычислить и по формулѣ

$$\varphi \equiv u'_6 u_6,$$

вытекающей изъ выраженія

$$\Omega \equiv u_1').$$

$$\varphi^2 \equiv -945,\ \varphi^3 \equiv -210,$$

и

$$x_1 \equiv 1469\ \ 210 \equiv 2294.$$

Остальныя шесть рѣшеній найдемъ умножая x_1 на главные характеры:

$$u_1 \equiv -2158,\ u_2 \equiv u_1^2 \equiv 1393,$$

$$u_3 \equiv 194,\ u_4 \equiv -1112,\ u_5 \equiv -1159,\ u_6 \equiv 2841.$$

---

7. $$x^{19} \equiv 10 \ (\mathrm{mod.}\ 8779)$$

$$p-1 = 19N,\ N \equiv 462 \equiv 19.24+6,$$

$$19\tau - 6\sigma = 1,\ \tau = 1,\ \sigma = 3,$$

$$a^N = 10^{462} \equiv 1,\ \varphi \equiv 1,$$

$$x_1 \equiv 10^{73}.$$

Въ этомъ примѣрѣ вычислеіе упрощается, потому что получается

$$10^{11} \equiv -1,\ 10^{22} \equiv 1,\ 10^{22\cdot 21} \equiv 10^{462} \equiv 1,$$

$$10^{73} \equiv 10^9 \equiv 1668,$$

такъ что

$$x_1 \equiv 1668,$$

а остальныя найдемъ умножая x_1 на главные характеры, изъ которыхъ одинъ $w_1 \equiv -104$ дается таблицею.

---

8. $$x^3 \equiv 73 \ (\mathrm{mod.}\ 4483)$$

Рѣшенія:

$$x_1 \equiv 1234,\ x_2 \equiv 33,\ x_3 \equiv -1267.$$

---

9. $$x^5 \equiv 229 \ (\mathrm{mod.}\ 4751)$$

Рѣшенія:

$$x_1 \equiv 10,\ x_2 \equiv 525,\ x_3 \equiv 1432,\ x_4 \equiv 836,\ x_5 \equiv -1331.$$

---

10. $$x^3 \equiv 6 \pmod{4861}$$

Рѣшенія:

$$x_1 \equiv -2056,\ x_2 \equiv 1685,\ x_3 \equiv 371.$$

---

11. $$x^{13} \equiv 2 \pmod{8581}.$$

Рѣшенія:

$$x_1 \equiv 2252;$$

остальныя 12 рѣшеній получаются умноженіемъ x_1 на w, $w^2, \ldots w^{12}$, гдѣ $w \equiv 1046$ (по таблицѣ).

§ 4.

О вычисленіи первообразныхъ корней простого числа.

1. Наилучшій въ практическомъ отношеніи способъ розысканія первообразнаго корня даннаго простого числа p, при большой величинѣ p, состоитъ въ испытаніи послѣдовательныхъ квадратичныхъ невычетовъ этого числа. Испытаніе это заключается въ вычисленіи абсолютно-наименьшихъ вычетовъ чиселъ

$$A = a^{\frac{p-1}{2q}},\ B = a^{\frac{p-1}{2r}} \ldots C = a^{\frac{p-1}{2s}}$$

гдѣ $q, r, \ldots s$ обозначаютъ простыхъ дѣлителей числа $p-1$, а a — испытываемый квадратичный невычетъ. Если ни одно изъ чиселъ $A, B, \ldots C$ не сравнимо съ (-1) по mod. p, то ни одно изъ чиселъ

$$a^{\frac{p-1}{2}},\ a^{\frac{p-1}{q}},\ a^{\frac{p-1}{r}}, \ldots a^{\frac{p-1}{s}}$$

не сравнимо съ 1, и a — первообразный корень. Если 2 квадратичный невычетъ числа p, и испытаніе, при $a=2$, даетъ отрицательный результатъ, то надо перейти къ испытанію $a=3$ и т. д.

Для чиселъ вида $4n+3$ можно испытывать и квадратичные вычеты, потому что, если для нѣкотораго числа a ни одно изъ чиселъ $A, B, \ldots C$ не сравнимо ни съ 1, ни съ -1, а

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

то $(-a)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, такъ какъ для чиселъ p вида $4n+3$, $\frac{p-1}{2}$ — нечетное, и $(-a)$ будетъ первообразнымъ корнемъ. Такимъ путемъ мы всегда найдемъ наименьшій по абсолютной величинѣ первообразный корень числа p; этимъ путемъ мы и вычисляли первообразные корни для всѣхъ простыхъ чиселъ p, лежащихъ между 5000 и 10000.

Наибольшее значеніе абсолютно-наименьшаго изъ первообразныхъ корней получилось для числа $p = 5881$, а именно $g = 31$.

Квадратичными невычетами (не считая, конечно, точныхъ кубовъ 8 и 27), меньшими 31, оказались числа 11, 13, 19, 22 и 26, которые и надо было испытать, причемъ получилось, что

11 и 13 принадлежитъ къ показателю $\frac{p-1}{3}$,

19 и 26 „ „ „ $\frac{p-1}{5}$,

22 „ „ „ $\frac{p-1}{7}$.

Число испытаній, считая и $a = 31$, здѣсь равно 7, и было наибольшимъ въ предѣлахъ $p < 10000$.

Въ большинствѣ-же случаевъ наименьшій квадратичный невычетъ числа p оказывается и первообразнымъ его корнемъ.

Указаннымъ путемъ можно разыскивать первообразные корни чиселъ p, превышающихъ предѣлъ нашихъ таблицъ, но мы не имѣемъ никакихъ данныхъ для того, чтобы установить какой нибудь высшій предѣлъ для абсолютно наименьшаго первообразнаго корня числа p, не считая, конечно, предѣла $\frac{p-1}{2}$, служащаго предѣломъ всѣхъ вообще чиселъ, входящихъ въ вычисленіе, при данномъ модулѣ p.

2. Въ теоретическомъ отношеніи нѣкоторый интересъ представляетъ слѣдующее замѣчаніе. Въ началѣ нашей замѣтки было указано, что при вычисленіи характеровъ степени q, за основаніе g можно взять любой невычетъ степени q; съ измѣненіемъ основанія g измѣняется только порядокъ, въ которомъ являются характеры, совокупность-же всѣхъ характеровъ остается безъ измѣненія; слѣдовательно, характеры могутъ быть вычислены независимо отъ того, извѣстенъ или неизвѣстенъ первообразный корень даннаго числа p.

Найдя характеры высшаго порядка степеней, соотвѣтствующихъ всѣмъ простымъ дѣлителямъ числа $p-1$, мы тотчасъ найдемъ и первообразный корень этого числа. Въ самомъ дѣлѣ, положимъ, что

$$p - 1 = 2^{\alpha} q^{\beta} r^{\gamma} \ldots s^{\delta}.$$

По самому опредѣленію характеровъ выходитъ, что квадратичный характеръ наивысшаго порядка $f^{(\alpha-2)}$, или -1, при $\alpha = 1$, есть число, принадлежащее показателю 2^{α}, характеръ наивысшаго порядка степени q — число, принадлежащее показателю q^{β} и т.

Такъ какъ числа

$$2^{\alpha},\ q^{\beta},\ r^{\gamma}, \ldots s^{\delta}$$

—взаимно-простыя, то произведеніе характеровъ наивысшаго порядка, соотвѣтствующихъ всѣмъ простымъ дѣлителямъ числа $p-1$, принадлежитъ къ показателю

$$2^{\alpha} q^{\beta} r^{\gamma} \ldots s^{\delta} = p-1,$$

т. е. будетъ первообразнымъ корнемъ числа p.

3. Въ теоретическомъ отношеніи заслуживаетъ вниманія нижеслѣдующая теорема Коркина, высказанная имъ въ его посмертномъ мемуарѣ и устанавливающая связь между рѣшеніемъ двучленныхъ сравненій и разысканіемъ первообразныхъ корней.

Теорема. *Если въ сравненіи*

$$x^{\delta} \equiv a_i \ (\mathrm{mod.}\ p),$$

гдѣ p простое число, δ — дѣлитель числа $p-1$, простой или сложный, число a_i принадлежитъ къ показателю $\frac{p-1}{\delta}$, (или, по терминологіи Коркина, къ группѣ (δ)), то въ числѣ рѣшеній этого сравненія будетъ ровно λ первообразныхъ корней числа p, гдѣ $\lambda = \frac{\varphi(p-1)}{\varphi(\frac{p-1}{\delta})}$,

и $\varphi(N)$ обозначаетъ число чиселъ, меньшихъ N и простыхъ съ нимъ.

Доказательство. Замѣчая, что всякій первообразный корень числа p, по возвышеніи въ степень δ, даетъ число, принадлежащее къ показателю $\frac{p-1}{\delta}$, мы видимъ, что теорема будетъ доказана, если покажемъ, что, каково-бы ни было данное число a_i, принадлежащее къ показателю $\frac{p-1}{\delta}$, всегда будутъ существовать λ первообразныхъ корней, которые, по возвышеніи ихъ въ степень δ, даютъ числа, сравнимыя съ a_i. Чтобы это показать, замѣтимъ прежде всего, что

1) если всѣ простые дѣлители числа $p-1$ будутъ также дѣлителями числа $\frac{p-1}{\delta}$, то $\lambda = \delta$,

а 2) если простыя числа $a, b, \ldots l$, будучи дѣлителями $p-1$, не дѣлятъ $\frac{p-1}{\delta}$, то

$$\lambda = \delta . \frac{a-1}{a} . \frac{b-1}{b} \ldots \frac{l-1}{l}.$$

Это прямо слѣдуетъ изъ извѣстнаго выраженія

$$\varphi(N) = N . \frac{a-1}{a} . \frac{b-1}{b} \ldots \frac{l-1}{l} . \frac{q-1}{q} \ldots \frac{r-1}{r},$$

гдѣ a, $b, \ldots l$, $q, \ldots r$ обозначаютъ всѣхъ простыхъ дѣлителей числа N. Замѣтивъ это, обозначимъ черезъ

$$k_1,\ k_2, \ldots k_\nu, \text{ гдѣ}$$

$$\nu = \varphi\left(\frac{p-1}{\delta}\right)$$

числа простыя съ $\frac{p-1}{\delta}$ и меньшія $\frac{p-1}{\delta}$, и разсмотримъ ариѳметическую прогрессію

$$k_i,\ k_i + \frac{p-1}{\delta},\ k_i + 2\frac{p-1}{\delta}, \ldots k_i + (\delta - 1)\frac{p-1}{\delta} \ldots\ldots. (A)$$

гдѣ i обозначаетъ любое изъ чиселъ $1, 2, \ldots \nu$. Всѣ члены этой прогрессіи числа простыя съ $\frac{p-1}{\delta}$ и всѣ меньше $(p-1)$.

Сосчитаемъ, сколько между ними чиселъ, простыхъ съ $(p-1)$.

Если 1) всѣ простые дѣлители $p-1$ будутъ также дѣлителями $\frac{p-1}{\delta}$, то очевидно, всѣ члены прогрессіи, будучи простыми относительно $\frac{p-1}{\delta}$, будутъ простыми и относительно $p-1$, и число ихъ равно δ.

Если 2) простые дѣлители $a, b, \ldots l$ число $p-1$, не будутъ дѣлителями $\frac{p-1}{\delta}$, причемъ, конечно, всѣ они будутъ дѣлителями числа δ, то простыми относительно $p-1$ будутъ тѣ члены прогрессіи, которые не дѣлятся ни на одно изъ чиселъ $a, b, \ldots l$. По извѣстному свойству ариѳметической прогрессіи, разность которой не дѣлится ни на одно изъ простыхъ чиселъ $a, b, \ldots l$, а число всѣхъ членовъ прогрессіи δ—кратное отъ $a, b \ldots l$, мы заключаемъ, что въ прогрессіи (A) число чиселъ простыхъ съ $p-1$ будетъ

$$\delta . \frac{a-1}{a} . \frac{b-1}{b} \ldots \frac{l-1}{l}.$$

Сопоставляя это со сказаннымъ выше о числѣ λ, мы видимъ, что число членовъ прогрессіи (A), простыхъ съ $p-1$, всегда равно λ.

Обозначимъ эти числа черезъ

$$m_1,\ m_2, \ldots m_\lambda,$$

причемъ общій видъ этихъ чиселъ будетъ

$$m_j = k_i + \mu_j \frac{p-1}{\delta},\ j = 1,\ 2, \ldots \lambda,\ \mu_j < \delta.$$

Обозначая черезъ g любой первообразный корень числа p, разсмотримъ рядъ

$$g^{m_1},\ g^{m_2}, \ldots g^{m_\lambda}.$$

Всѣ числа этого ряда будутъ также первообразными корнями числа p, несравнимы между собой, и по возвышеніи въ степень δ даютъ числа, сравнимыя съ однимъ и тѣмъ-же числомъ

$$a_i \equiv g^{k_i \delta},$$

принадлежащимъ къ показателю (δ). Замѣнивъ въ прогрессіи (A) число k_i другимъ k_j изъ того-же ряда чиселъ

$$k_1,\ k_2, \ldots k_\nu,$$

мы такимъ же образомъ убѣдимся въ существованіи λ первообразныхъ корней, которые по возвышеніи ихъ въ степень δ дадутъ числа, сравнимыя съ другимъ числомъ

$$a_j \equiv g^{k_j \delta},$$

принадлежащимъ показателю $\frac{p-1}{\delta}$ и не сравнимому съ a_i, потому-что при

$$a_i \equiv a_j$$

получили-бы

$$g^{(k_i - k_j)\delta} \equiv 1 \ (\text{mod. } p),$$

гдѣ $|k_i - k_j| < \frac{p-1}{\delta}$, что невозможно. Число чиселъ, принадлежащихъ показателю $\frac{p-1}{\delta}$ равно $\nu = \varphi\left(\frac{p-1}{\delta}\right)$ и каждое изъ сравненій

$$x^\delta \equiv a_i \ (\text{mod. } p),\ i = 1,\ 2, \ldots \nu.$$

имѣетъ λ первообразныхъ корней въ числѣ своихъ рѣшеній. Теорема доказана.

Въ частномъ случаѣ, когда $\delta = q$ — простому дѣлителю число $p-1$,

$$\lambda = \frac{\varphi(p-1)}{\varphi(\frac{p-1}{q})} = q \text{ или } q-1$$

а именно $\lambda = q$, когда $p - 1 = q^\alpha N$, гдѣ N не дѣлится на q и $\alpha > 1$, и $\lambda = q - 1$, при $\alpha = 1$.

Поэтому, при $\alpha > 1$, *всѣ* рѣшенія сравненія

$$x^q \equiv a \ (\text{mod. } p),$$

гдѣ a — число, принадлежащее показателю $\frac{p-1}{q}$, будутъ первообразными корнями числа p, а при $\alpha = 1$, *всѣ*, кромѣ одного, которое будетъ вычетомъ степени q. Въ самомъ дѣлѣ, при $\alpha = 1$, $a^N \equiv 1$, $\varphi \equiv 1$ и $x_1 \equiv a^{N'\sigma+\tau}$ будетъ вычетомъ степени q, потому—что

$$x_1^{\frac{p-1}{q}} \equiv x_1^N \equiv a^{(N'\sigma+\tau)N} \equiv 1 \ (\mathrm{mod.}\ p).$$

Остальныя $q-1$ рѣшеній

$$x_1 u_1,\ x_1 u_2, \ldots x_1 u_{q-1},$$

гдѣ $u_1, u_2, \ldots u_{q-1}$ главные характеры, будутъ первообразными корнями.

4. Въ заключеніе замѣтимъ еще одну теорему, которая можетъ иногда служить для болѣе быстраго разысканія первообразнаго корня, чѣмъ пріемъ, изложенный въ началѣ этого параграфа.

Теорема. *Если число a принадлежитъ къ показателю m, а число b къ показателю n, по простому модулю p, и въ разложеніяхъ m и n на простые множители нѣтъ общихъ простыхъ множителей съ одинаковыми показателями степеней, то произведеніе $a\,b$ принадлежитъ къ показателю N, гдѣ N наименьшее кратное чиселъ m и n.*

Примѣчаніе. Въ случаѣ, когда $N = p-1$, число ab будетъ первообразнымъ корнемъ числа p.

Доказательство этой теоремы столь просто, что мы позволимъ себѣ на немъ не останавливаться и ограничимся однимъ примѣромъ.

При $p = 109$, $p-1 = 2^2.3^3$, 2 принадлежитъ къ показателю $2^2.3^2$, 3 къ показателю 3^3, число $6 = 2.3$ — принадлежитъ къ показателю $N = 2^2.3^3 = p-1$, 6 — первообразный корень.

24.XI.09.