BAKI UNİVERSİTETİNİN XƏBƏRLƏRİ
№3 *Fizika-riyaziyyat elmləri seriyası* 2006

SONLU MEYDAN VƏ QRUPLARDA ƏDƏDLƏR NƏZƏRİYYƏSİNİN BİR MƏSƏLƏSİ HAQQINDA

Y.R.BAXŞƏLİYEV
Azərbaycan Dövlət Pedaqoji Universiteti

İşdə sadə $p>2$ moduluna nəzərən ibtidai köklün xassələrinə əsaslanaraq yüksək dərəcəli çıxıqlar, Z_p meydanı və onun multiplikativ qrupu tədqiq edilir. Məqalə qruplar nəzəriyyəsi metodlarının müqayisələr nəzəriyyəsinə tətbiqinə həsr edilmişdir.

Cəbri tənliklərin radikallarla həlli məsələsi vaxtilə qruplar nəzəriyyəsinin yaranması və inkişafına təkan verdiyi kimi, qruplar nəzəriyyəsinin metodları da öz növbəsində müxtəlif tənliklərin tədqiqinə ciddi təkan vermişdir. Bu baxımdan müqayisələr nəzəriyyəsi çox səciyyəvidir. Məsələn, verilmiş meydanda hər hansı gətirilməyən çoxhədli moduluna nəzərən müqayisələrin bu meydanın genişlənməsi və ümumiyyətlə, meydanların cəbri genişlənməsilə sıx əlaqəsi vardır (bax: [1], [2]). Ümumiyyətlə, klassik ədədlər nəzəriyyəsinin əsas məsələlərinin müasir cəbrin metodları ilə həlli bir sıra məsələlərin şərhini xeyli asanlaşdırmış olur. Məqalə iki hissədən ibarətdir. Birinci hissədə qruplar nəzəriyyəsindən işdə istifadə edəcəyimiz əsas anlayış və təkliflər, eləcə də ədədlər nəzəriyyəsindən bəzi faktları verəcəyik. İkinci hissə bilavasitə yüksək dərəcəli çıxıqların bəzi əsas xassələrinin qruplar nəzəriyyəsinin dilində şərhinə həsr edilmişdir. Burada məqsəd, $p>2$ sadə moduluna nəzərən ibtidai köklərin varlığı, onların xassələri, sayı və bütün ibtidai köklərin tapılması haqda teoremlərin, həmçinin ikihədli müqayisələrin həllərinin varlığı və bütün həllərin tapılması haqda teoremlərin isbatının, Z_p meydanının multiplikativ qrupunun və bu qrupun morfizmlərinin köməyilə verməkdən ibarətdir.

Köməkçi faktlar və anlayışlar

Əvvəlcə qruplar nəzəriyyəsinə müraciət edək (bax: [3], [5], [6]). $G=<G;\cdot, e>$ qrupundan $a\in G$ elementini götürək. $a\in G$ elementi üçün elə ən kiçik müsbət tam n ədədi varsa ki, $a^n=e$ olsun, onda belə n ədədinə a ədədinin tərtibi deyilir və $ord(a)$ kimi

işarə olunur. Məlumdur ki, 1) $ord(a)=n$ isə, onda a, a^2,..., a^n elementləri öz aralarında müxtəlifdirlər; 2) $ord(a)=n$ və $a^k=e$ isə, onda $n \mid k$, yəni n ədədi k-nı bölür.

Şərtləşək ki, əgər G doğuranı a olan n- tərtibli dövri qrupdursa, onu $G=\{a\}^n$ ilə işarə edəcəyik. Aşkardır ki, $ord(a)=n$ isə, onda $G=\{a\}^n$.

Təklif 1. *$G=\{a\}^n$ olarsa, $b=a^k$ elementi onda və yalnız onda G qrupunun doğuranı olar ki, $(n,k)=1$ olsun.*

Qeyd edək ki, burada hər yerdə $(a,b)=1$ işarəsi a ilə b -nin qarşılıqlı sadə olduğunu göstərir. $A \subset G$ altçoxluğunun altqrup olmasını $A<G$ kimi işarə edək. Məlumdur ki, dövri $G=\{a\}^n$ qrupunun hər bir $A<G$ altqrupu dövridir və A-nın tərtibi n -in bölənidir, doğuranı isə, n -in hər bir d böləni üçün a^d ola bilər (bax: [3], [12]).

Tutaq ki, $\varphi: G \to G'$ inikası G qrupunun G' qrupuna homomorfizmidir və G dövri qrupdur, onda G qrupunun homomorf obrazı olan $\varphi(G)$ dövri qrupdur.

Təklif 2. *$\varphi: G \to G$, $G=\{a\}^n$ dövri qrupunun G qrupuna homomorfizmidirsə, $\varphi(G)<G$ altqrupunun doğuranı, n-in uyğun d böləni üçün, a^d elementi olar, yəni $\varphi(G)=\{a^d\}^{\frac{n}{d}}$* (bax: [3]).

φ inikası G qrupunun G' qrupuna homomorfizmidirsə, $y \in G'$ elementini qeyd etsək, $\varphi(x)=y$ (1) tənliyini alarıq. (1) tənliyini həll etmək məsələsi obraza görə, proobrazı tapmaq məsələsidir. Aşkardır ki, $y \in \varphi(G)$ olarsa, (1) tənliyinin həlli var, əks halda, həll yoxdur. $\varphi(x)=e'$ tənliyinə (1) tənliyinə uyğun bircins tənlik deyirlər, burada e', G' qrupunun vahididir.

Teorem 1. *φ, G qrupunun G' qrupuna homomorfizmidirsə və $y \in \varphi(G)$ G' qrupunun müəyyən elementidirsə, onda* (1) *tənliyinin bütün həlləri özünün bir xüsusi həlli ilə ona uyğun bircins tənliyin bütün həllərinə kompozisiyasından alına bilər.*

Tənliklər nəzəriyyəsinin əsaslandırılmasında bu teoremin fundamental əhəmiyyəti vardır. Ona görə də onu əsas teorem adlandıracağıq (bax: [7], [11]).

İndi isə ədədlər nəzəriyyəsindən aşağıdakı faktları verək (bax: [9]).

Tərif 1. $(a,m)=1$ isə, $a^x \equiv 1 \pmod{m}$ müqayisəsini ödəyən x-in ən kiçik müsbət tam δ qiymətinə a ədədinin (çıxığının) m moduluna nəzərən tərtibi deyilir və $ord_m(a)$ kimi işarə olunur.

a-nın m moduluna nəzərən tərtibi δ-dırsa, bu o deməkdir ki, $a^{\delta} \equiv 1 \pmod{m}$ müqayisəsi doğrudur və burada δ-ən kiçik müsbət tam ədəddir. Asanlıqla görmək olar ki, a-nın m moduluna nəzərən tərtibi δ-dırsa, onda a-nın daxil olduğu sinfin bütün elementlərinin də tərtibi δ olar. Ona görə də $\bar{a}$ sinfinin tərtibindən danışmaq olar. «a-nın m moduluna nəzərən tərtibi δ-dır» mülahizəsini $ord_m(a)=\delta$ kimi işarə edəcəyik. Tam ədədlərin additiv Z qrupunun mZ altqrupuna nəzərən $Z_m = Z/mZ$ faktor-qrupunu düzəldək. Başqa sözlə desək, Z tam ədədlər halqasının (m) baş idealına nəzərən Z_m-çıxıqlar halqasını düzəldək. Məlumdur ki, $p(z)=z+mZ$ düsturu ilə təyin olunan $p: Z \to Z_m$ inikası Z halqasının Z_m halqasına kanonik homomorfizmi epimorfizmdir (bax: [4], [6]), $ax \equiv b \pmod{m}$ müqayisəsi Z_m çıxıqlar halqasında $\bar{a}x=\bar{b}$ tənliyi ilə ekvivalentdir. Bu tənliyin həlli isə $\bar{a} \in Z_m$ çıxığının tərsinin varlığı məsələsinə gəlir. $U(k)$ ilə K halqasının vahidlər (və ya tərsi olan elementlər) qrupunu işarə edək (bax: [1], [3], [6]). $U(Z_m)$ qrupuna baxaq. Burada aşağıdakı təklif doğrudur.

Təklif 3. *$\bar{a} \in Z_m$ sinfinin onda və yalnız onda tərsi olar ki, $(a, m)=1$ olsun.*

$U(Z_m)$ qrupunun tərtibinin $\varphi(m)$ olması aşkardır (burada φ Eyler funksiyasıdır). Həmçinin məlumdur ki, Z_m halqası onda və yalnız onda meydana çıxar ki, $m=p$ sadə ədəd olsun.

İbtidai kök və yüksək dərəcəli çıxıqların xassələri

Burada əsas məqsədlərimizdən biri $U(Z_p)$ qrupunun xassələri və bu xassələr əsasında bir sıra məsələlərin həllini əsaslandırmaqdan ibarətdir.

Tərif 2. *Tərtibi m modulunun Eyler funksiyasına bərabər olan çıxığa m moduluna nəzərən ibtidai kök deyilir.*

Məsələn, 11 moduluna nəzərən 3 çıxığı ibtidai kök deyil, çünki $ord_{11}(3)=5<\varphi(11)=10$. Lakin $ord_{11}(2)=10$ olduğundan 2-ibtidai kökdür.

Burada bir sıra teoremlərin yeni isbatı verilir.

Teorem 2. *$p>2$ sadə ədəd, $(g,p)=1$ isə $g>1$ ədədi (çıxığı) p moduluna nəzərən onda və yalnız onda ibtidai kök olar ki, g-ni $1,2,\ldots,p-1$ dərəcələrdən qüvvətə yüksəltdikdə alınan $g, g^2, \cdots, g^{p-1}$* (2)

çıxıqlar sistemi p moduluna nəzərən çıxıqların gətirilmiş sistemi olsun.

İsbatı. g çıxığı p moduluna nəzərən ibtidai kökdürsə, g -nin p-yə nəzərən tərtibi $p-1$-dir. Tərtibin xassəsinə əsasən (2) sistemi öz aralarında müxtəlif olub, p moduluna nəzərən bir-birilə müqayisə olunmurlar. $(g,p)=1$ olduğundan (2)-dəki hər bir çıxıq p ilə qarşılıqlı sadədir. Onların sayı $p-1$ olduğundan hökm edərik ki, (2) sistemi p moduluna nəzərən çıxıqların gətirilmiş sistemidir. Tərsinə, g -ni $1,2,...,p-1$ dərəcədən qüvvətə yüksəltdikdə p moduluna nəzərən gətirilmiş sistem alınırsa, onda $p-1$-dən kiçik heç bir dərəcədən $g^x \equiv 1(\mathrm{mod}\, p)$ ola bilməz, deməli, yalnız $x=p-1$ olduqda bu müqayisə doğru olar. Bu isə o deməkdir ki, $ord_p g = p-1$ yəni g ibtidai kökdür.

Nəticə 1. *g çıxığı p moduluna nəzərən onda və yalnız onda ibtidai kök olar ki, g çıxığı p moduluna nəzərən çıxıqlar siniflərinin multiplikativ qrupunun doğuranı olsun.*

Məlumdur ki, p sadə moduluna nəzərən ibtidai kök var (bax: [9]). p moduluna nəzərən ibtidai kökların sayını tapmaq maraqlıdır.

Teorem 3. *Sadə p moduluna nəzərən ibtidai kökların sayı $\varphi(p-1)$-ə bərabərdir.*

İsbatı. g çıxığı p moduluna nəzərən ibtidai kökdürsə, g çıxığı (2) sisteminin doğuranı olur. Təklif 3-ə əsasən g^s çıxığı o zaman (2)-nin doğuranı olar ki, $(s,p-1)=1$ olsun, $1,2...,p-1$ ədədləri içərisində $p-1$-lə qarşılıqlı sadə olan ədədlərin sayı $\varphi(p-1)$ olduğundan teorem doğrudur.

Nəticə 2. *g çıxığı p moduluna nəzərən ibtidai kökdürsə, g^s çıxığı p moduluna nəzərən onda və yalnız onda ibtidai kök olar ki, $(s,p-1)=1$ olsun.*

Məlumdur ki, yalnız $m=2,4,p^\alpha,2p^\alpha (p>2,\alpha\in N)$ modullarına nəzərən ibtidai kök var. İbtidai kökləri tapmaq üçün aşağıdakı təklifin böyük əhəmiyyəti vardır (bax: [9]).

Təklif 4. *$\varphi(m)=c$ və $c=p_1^{\alpha_1},p_2^{\alpha_2},...,p_k^{\alpha_k}$ kanonik ayrılışdırsa, m ilə qarşılıqlı sadə olan g çıxığı onda və yalnız onda m moduluna nəzərən ibtidai kök olar ki, g çıxığı aşağıdakı müqayisələrdən heç birini ödəməsin:*

$$g^{\frac{c}{q_1}} \equiv 1(\mathrm{mod}\, m),\quad g^{\frac{c}{q_2}} \equiv 1(\mathrm{mod}\, m),...,\quad g^{\frac{c}{q_k}} \equiv 1(\mathrm{mod}\, m), \qquad (3)$$

Aşağıdakı məsələyə baxaq: $p=13$ moduluna nəzərən bütün ibtidai köklərin ümumi şəklini tapaq. Əvvəlcə təklif 4-dən istifadə edərək ibtidai köklərdən birini tapırıq: $\varphi(13)=12=2^2\cdot 3$. 13 modulu na nəzərən gətirilmiş sistemdən g=2-ni yoxlayaraq görərik ki, $2^{\frac{12}{2}}=2^6\equiv -1\not\equiv 1(\mathrm{mod}13)$, $2^{\frac{12}{3}}=2^4\equiv 3\not\equiv 1(\mathrm{mod}13)$. Deməli, 2-ibtidai kökdür. Qalan ibtidai kökləri tapmaq üçün nəticə 2-dən istifadə edək. $(12,s)=1\Leftrightarrow s=1,5,7,11$. Ona görə də taparıq: $2^1=2, 2^5\equiv 6(\mathrm{mod}13)$, $2^7\equiv 11(\mathrm{mod}13)$, $2^{11}\equiv 7(\mathrm{mod}13)$. Deməli, g=2,6,7,11 çıxıqları 13 moduluna nəzərən ibtidai köklərdir.

g çıxığı $p>2$ moduluna nəzərən ibtidai kökdürsə, onda g-nin müxtəlif qüvvətləri p moduluna nəzərən çıxıqların gətirilmiş sistemini əmələ gətirir (bax: teorem 2). Onda p ilə qarşılıqlı sadə olan a ədədi (çıxığı) üçün elə s natural ədədi varsa ki, $g^s\equiv a(\mathrm{mod}p)$ müqayisəsi doğru olsun, onda s ədədinə a çıxığının p moduluna nəzərən g əsasdan indeksi deyilir və $ind_g a$ kimi işarə olunur. Deməli, $g^{ind_g a}\equiv a(\mathrm{mod}\,p)$ (4) müqayisəsi doğrudur [bax: 10]. Buradan görünür ki, indeks anlayışı cəbr kursundan məlum olan loqarifm anlayışına analoji anlayışdır. (4) müqayisəsini indeksin tərifini ifadə edən müqayisə kimi qəbul etmək olar. Onda aşağıdakı müqayisələrin doğruluğunu alarıq:

1. $a\equiv b(\mathrm{mod}\,p)\Leftrightarrow ind_g a\equiv ind_g b(\mathrm{mod}\,p-1)$;
2. $ind_g 1\equiv 0(\mathrm{mod}\,p-1)$;
3. $ind_g ab...\ell\equiv ind_g a+ind_g b+...+ind_g \ell(\mathrm{mod}\,p-1)$;
4. $ind_g a^n\equiv n\ ind_g a(\mathrm{mod}\,p-1)$,

burada 3 müqayisəsi göstərir ki, $G=U(Z_p)$ - p moduluna nəzərən çıxıqlar siniflərinin multiplikativ qrupu, $C=Z_{p-1}$ $p-1$ moduluna nəzərən çıxıqlar siniflərinin additiv qrupudursa, onda $\forall a\in G$ sinfinə $inda\in C$ çıxığını qarşı qoysaq, nəticədə G qrupunun C qrupuna izomorfizmini almış olarıq. İndi yüksək dərəcəli çıxıqlar və yüksək dərəcəli ikihədli müqayisələrin həllini araşdıraq. Burada da modulun 2-dən böyük sadə p ədədi olduğunu qəbul edəcəyik.

Tərif 3. *$p>2$ sadə ədəd, $(a,p)=1$ isə, $x^n\equiv a(\mathrm{mod}\,p)$ (5) şəklindəki müqayisəyə ikihədli müqayisə deyilir.*

(5) müqayisəsinin o zaman həlli olar ki, a çıxığı $\varphi(x)=x^n(x\in G=<G,\cdot>)$ inikasının $\varphi(G)$ obrazına daxil olsun. g çıxığı p moduluna nəzərən ibtidai kökdürsə, onda məlumdur ki, G qrupu doğuranı g və tərtibi $p-1$ olan dövri qrupdur (bax: nəticə 1).

Yuxarıda şərh etdiyimiz təкlif 2-dən, eləcə də ondan əvvəlкi şərhdən aydın olur кi, G dövri qrupunun özü-özünə homomorf obrazı da dövri altqrupdur və bu altqrupun tərtibi G qrupunun tərtibinin, yəni $p-1$-in bölənidir. Bu altqrup $p-1$-in hər bir böləni üçün var. Göründüyü кimi, bu $\varphi(G)$ obrazı ilə $p-1$-in bölünmə münasibətindən asılıdır. Həmin münasibətləri araşdıracağıq.

Tərif 4. *(5) müqayisəsinin həlli varsa, a-ya n-dərəcəli çıxıq, həlli yoxdursa, a-ya n-dərəcəli qeyri-çıxıq deyilir.*

Aşкardır кi, a, n-dərəcəli çıxıqdırsa, onda $\overline{a}$ sinfindən olan ixtiyari çıxıq da n-dərəcəli olar. Ona görə də n- dərəcəli çıxıqlar sinfindən danışmaq olar.

Teorem 4. *$p>2$ sadə ədəd və $d=(n,p-1)$ isə onda p moduluna nəzərən n-dərəcəli çıxıqların sayı $\frac{p-1}{d}$-yə bərabərdir.*

İsbatı. p moduluna nəzərən, p ilə qarşılıqlı sadə olan çıxıqların sayı $p-1$-ə bərabərdir. g ibtidai кökдürsə, onda (2) sistemi p moduluna nəzərən gətirilmiş sistem və doğuranı g olan, $p-1$ tərtibli dövri qrupdur (bax: nəticə 1). Digər tərəfdən, məlumdur кi, a çıxığı onda və yalnız onda ndərəcəli çıxıq olar кi, o $\varphi(g)=g^n$ iniкasının obrazına daxil olsun. Məhz bu obrazı tapaq. $(n,p-1)=d$ olduğunda alarıq кi, elə u və v var кi, $nu+(p-1)v=d$. Onda,

$$g^d=g^{nu+(p-1)v}=g^{nu}\cdot g^{(P-1)v}=g^{nu}\cdot\left(g^{P-1}\right)^v=g^{nu}. \qquad (5)$$

(5) bərabərliyi onu göstərir кi, $(n,p-1)=d$ olduqda doğuranı g^n olan dövri altqrup, doğuranı g^d olan dövri altqrupla üst-üstə düşür. Ona görə də $\varphi(g)=g^n$ iniкasının əvəzinə $\varphi(g)=g^d$ götürə biləriк. Bu zaman $\varphi(G)$ altqrupunun elementləri

$$g^d, g^{2d},\ldots, g^{\frac{p-1}{d}d} \qquad (6)$$

olar. Bu da onu göstərir кi, $\varphi(G)$ altqrupunun tərtibi $\frac{p-1}{d}$-dir. Beləliкlə, alırıq кi, $x^n\equiv a(\mathrm{mod}\,p)$ müqayisəsinin onda və yalnız onda həlli var кi, yəni a onda və yalnız onda n-dərəcəli çıxıqdır кi, a çıxığı (6) sisteminə daxil olsun. (6) sistemindəкi çıxıqların sayı $\frac{p-1}{d}$ olduğundan teorem doğrudur. Bu teoremdən aşağıdaкı nəticələr alınır.

Nəticə 3. *$p>2$ sadə ədəd və $(n,p-1)=d>1$ isə p ilə qarşılıqlı sadə olan a çıxığı onda və yalnız onda n-dərəcəli çıxıq olar кi, $a^{\frac{p-1}{d}}\equiv 1\ (\mathrm{mod}\,p)$ (7) müqayisəsi doğru olsun.*

Həqiqətən, a çıxığı onda və yalnız onda n-dərəcəli çıxıq olar ki, o, **(6)** sisteminə daxil olsun. **(6)** sistemi isə $\frac{p-1}{d}$ tərtibli dövri altqrupdur. Ona görə də $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$ olmalıdır.

Nəticə 4. $p > 2$ sadə ədəd, $(n, p-1) = d > 1$ isə onda p moduluna nəzərən n dərəcəli çıxıqlar, d dərəcəli çıxıqlarla üst-üstə düşür (bax: **(5)** bərabərliyi). Məsələn, $p = 11$ moduluna nəzərən 4 dərəcəli çıxıqlar sistemi ilə 2-dərəcəli çıxıqlar sistemi üst-üstə düşürlər və $g^2, g^4, g^6, g^8, g^{10} = 1$ sistemindən ibarətdirlər.

Misal. $x^4 \equiv 5 (\mathrm{mod} 11)$ müqayisəsində $(10,2) = 4$ və $5^{\frac{10}{2}} = 5^5 \equiv 1 (\mathrm{mod} 11)$ olduğundan, 5 çıxığı 4 dərəcəli və eyni zamanda, 2 dərəcəli çıxıqdır. Ona görə də $x^4 \equiv 5 (\mathrm{mod} 11)$ və $x^2 \equiv 5 (\mathrm{mod} 11)$ müqayisələrindən hər ikisinin həlli var və hər ikisinin 2 həlli var. $x^2 \equiv 5 (\mathrm{mod} 11)$ müqayisəsinin həlləri, $x \equiv 4,7 (\mathrm{mod} 11)$ siniflərdir, $x^2 \equiv 5 (\mathrm{mod} 11)$ müqayisəsinin həlləri $x \equiv 2,9$ (mod 11) siniflərdir.

Xüsusi halda **(7)** müqayisəsində $n \mid p-1$ isə onda aşkardır ki, $(n, p-1) = n$ olur. Ona görə də teorem 4 və ondan çıxan nəticə 3 və 4-də hər yerdə d-nin yerinə n-yazsaq, alınan hökmlər yenə də doğru olar. İkihədli yüksək dərəcəli müqayisələrin həllində aşağıdakı iki teoremin xüsusi əhəmiyyəti vardır.

Teorem 5. *$p>2$ sadə ədəd, $(n,p-1)=d>1$ isə onda $x^n \equiv 1 (\mathrm{mod} p)$* **(8)** *müqayisəsi ilə $x^d \equiv 1 (\mathrm{mod} p)$* **(9)** *müqayisəsinin həllər çoxluğu üst-üstə düşür.*

İsbatı. Həqiqətən, hər iki halda həllər çoxluğu 1-in φ nəticəsindəki tam proobrazı, başqa sözlə desək, φ unikasının nüvəsindən ibarətdir. $(n,p-1)=d>1$ olduğundan $\varphi(x) = x^n$ və $\varphi(x) = x^d$ $\left(x \in G = \{g\}^{p-1}\right)$ inikaslarının obrazları eyni olduğundan, nəticə 4-ə əsasən, 1-in φ nəticəsindəki tam proobrazı da hər iki halda eyni olacaqdır. Digər tərəfdən, 1-in tam proobrazı $G = \{g\}^{P-1}$ qrupunun altqrupu olacaqdır və hər iki altqrupun doğuranı $g^{\frac{P-1}{d}}$, elementləri isə $g^{\frac{P-1}{d}}, g^{2\frac{P-1}{d}}, \ldots, g^{d\frac{P-1}{d}}$ **(10)** olar. Asanlıqla görmək olar ki, **(10)** sistemindən olan ixtiyari elementin n dərəcədən və d dərəcədən qüvvətləri 1 ilə müqayisə olunandırlar.

Misal. $x^4 \equiv 1 (\mathrm{mod} 11)$ müqayisəsinin həllər çoxluğu $x \equiv 1,10 (\mathrm{mod} 11)$ $x^2 \equiv 1 (\mathrm{mod} 11)$ müqayisəsinin həllər çoxluğu da $x \equiv \pm 1 (\mathrm{mod} 11)$ və ya $x \equiv 1,10 (\mathrm{mod} 11)$ olar.

Teorem 6. $n \mid p-1, (a,p)=1$ *və* $a^{\frac{P-1}{n}} \equiv 1 (\mathrm{mod}\, p)$ *isə, onda* $x^n \equiv a (\mathrm{mod}\, p)$ (11) *müqayisəsinin bütün halları özünün bir xüsusi həllinin* $x^n \equiv 1 (\mathrm{mod}\, p)$ (12) *müqayisəsinin bütün həllərinə hasilindən alına bilər.*

İsbatı. Şərtə görə, (12) müqayisəsinin həlli var. g çıxığı p moduluna nəzərən ibtidai köklərdən biri olsun. Onda $G = \{g\}^{P-1} = \{g, g^2, ..., g^{P-1}\}$ qrupu p moduluna nəzərən çıxıqlar siniflərinin multiplikativ qrupu olar. $\varphi(x) = x^n$ inikasını $\varphi(g) = g^n$ $\varphi(g) = g^n$ inikası ilə əvəz etsək, nəticədə G qrupunun özü-özünə homomorfizmini almış olarıq. Doğrudan da

$$\forall (g^k, g^l \in G),\ \varphi(g^k \cdot g^l) = \varphi(g^{k+l}) = g^{(k+l)n} = g^{kn} \cdot g^{ln} = \varphi(g^k) \cdot \varphi(g^l).$$

Bu isə φ-nin homomorfizm olduğunu göstərir. φ homomorfizminin obrazı isə $g^n, g^{2n}, ..., g^{\frac{P-1}{n}n} = 1$ elementləri çoxluğundan ibarətdir ki, o da G-nin $\frac{p-1}{n}$ tərtibli altqrupudur. Onda qruplar üçün yuxarıda söylədiyimiz əsas teoremdən bu teoremin isbatı birbaşa alınır. Doğrudan da x_0 çıxığı (11) müqayisəsinin bir xüsusi həlli, u isə (12) müqayisəsinin ixtiyari həllidirsə, onda $x_0 u$ hasili (11) müqayisəsini ödəyir, yəni $(x_0 u)^n = x_0^n \cdot u^n \equiv a \cdot 1 = a (\mathrm{mod}\, p)$ müqayisəsi doğrudur, yəni $x_0 u$ çıxığı (11) müqayisəsinin həllidir. u ixtiyari olduğundan teoremin doğruluğu alınır.

Teorem 4 və 5-dən nəticə olaraq, ədədlər nəzəriyyəsində məşhur olan aşağıdakı teoremi almış oluruq.

Teorem 7. $p > 2$ *sadə ədəd,* $(a,p)=1$ *və* $(n, p-1) = d$ *isə, onda* d *ədədi* $ind\, a$*-nı bölmürsə,* (11) *müqayisəsinin həlli yoxdur,* $d \mid ind\, a$ *isə, onda* (11) *müqayisəsinin həlli var* və d *saydadır.*

Qeyd edək ki, ikihədli müqayisə $Ax^n \equiv B (\mathrm{mod} p), (A,p) = (B,p) = 1$ (13) şəklində verilmişdirsə, onu özü ilə eyni güclü olan $x^n \equiv a (\mathrm{mod}\, p); (a,p) = 1$ (14) müqayisəsinə gətirmək olar. Doğrudan da (13)-nin hər tərəfini $Ay \equiv 1 (\mathrm{mod}\, p)$ müqayisəsini ödəyən α çıxığına vursaq, alarıq:

$A\alpha x^n \equiv B\alpha (\mathrm{mod}\, p)$ və ya $x^n \equiv B\alpha (\mathrm{mod}\, p)$, burada da $B\alpha = a$ götürsək, yəni $B\alpha = a (\mathrm{mod}\, p)$ götürsək, $x^n \equiv a (\mathrm{mod}\, p)$ müqayisəsini almış olarıq. Aşkardır ki, bu müqayisənin bütün həlləri (13) müqayisəsini ödəyəcəkdir.

Bir misala baxaq: $11x^{15} \equiv 7 (\mathrm{mod} 19)$ (15) müqayisəsini həll etmək tələb olunur. Əvvəlcə müqayisənin hər iki tərəfini $11y \equiv 1 (\mathrm{mod} 19)$

(16). Bu müqayisəsinin bir həlli olan $y \equiv 7(\mathrm{mod}19)$ çıxığına vursaq və $77 \equiv 1(\mathrm{mod}19)$ olduğunu nəzərə alsaq, **(16)** müqayisəsi aşağıdakı sadə şəklə düşər: $x^{15} \equiv 11(\mathrm{mod}19)$ və ya $x^{15} \equiv 11(\mathrm{mod}19)$ **(17)** . Bu müqayisəni həll edək. Bunun üçün $(15,18)=3$ olduğundan, və $11^{\frac{18}{3}} = 11^6 = \left(11^2\right)^3 \equiv 121^3 \equiv 7^3 \equiv 11 \cdot 7 \equiv 1(\mathrm{mod}19)$ olduğundan **(17)** müqayisəsinin həlli var və 3-saydadır. **(17)** müqayisəsinin bir xüsusi həllini tapaq. 19 moduluna nəzərən ibtidai köklərdən biri 2-dir.

Buna görə də $G = \{2\}^{18}$ qrupu 18 tərtibli dövri qrupdur. Bu qrupun $\varphi(g) = g^{15}$ inikasını qursaq, alarıq: $\varphi(G) = \{2^3, 2^6, 2^9, 2^{12}, 2^{15}, 2^{18}\}$. Bu çoxluq həmçinin $\varphi(g) = g^3$ inikasının da obrazıdır. Asanlıqla yoxlamaq olar ki, 11 çıxığı 2^{12} obrazı ilə bir sinfə düşür və 2^{12} – nin $\varphi(g) = g^{15}$ homomorfizmindəki proobrazı $2^2 = 4$ olduğundan alırıq ki, verilmiş müqayisənin bir xüsusi həlli $x_0 \equiv 4(\mathrm{mod}19)$ olur. Verilmiş müqayisənin digər həllərini tapmaq üçün: $x^3 \equiv 1(\mathrm{mod}19)$ **(18)** müqayisəsinin bütün həllərini tapaq. Bu müqayisənin həllər çoxluğu 1-in tam proobrazı olduğuna görə, o da G-nin altqrupudur. Bu altqrupun tərtibi 3 olduğundan onun doğuranı $2^{\frac{18}{3}} = 2^6$ olar. Ona görə də **(18)** müqayisəsinin həlləri, $\varepsilon_0 = 2^6 \equiv 7 \ (\mathrm{mod}19)$, $\varepsilon_1 = 2^{12} \equiv 11(\mathrm{mod}19), \varepsilon_2 = 2^{18} \equiv 1 \ (\mathrm{mod}19)$ çıxıqlar olar. Bu halda, teorem 6-ya əsasən **(21)** müqayisəsinin bütün həlləri $x \equiv 4 \cdot 1, \ 4 \cdot 7, \ 4 \cdot 11(\mathrm{mod}19)$ və ya $x \equiv 4,6,9(\mathrm{mod}19)$ olar.

ƏDƏBİYYAT

1. Боревич З.И., Шафаревич И.Р. Теория чисел. М., Наука, 1964.
2. Шафаревич И.Р. Основные понятия алгебры и современные проблемы математики. Фундаментальные направлении Т.11 (итоги науки и техники, ВИНИТИ) 1986.
3. Ленг С. Алгебра М., Мир, 1968.
4. Айерленд К., Роузен М. Классическое введение в современную теорию чисел. М., Мир, 1987.
5. Вандер-Варден, Б.Л. Алгебра. М., Мир 1967.
6. Qasımov V.Ə. Cəbr və ədədlər nəzəriyyəsi. II cild. Bakı, BDU, 1999.
7. Фор Р., Кофман А., Дени-Папен М. Современная математика. М., Мир, 1966.
8. Калужнин Л.А. Введение в общую алгебру. М., Наука. 1976.
9. Виноградов И.М. Основы теории чисел. М., Наука., 1976.
10. Бухштаб А.А. Теория чисел. М., 1960.
11. Baxşəliyev Y.R. Riyazi strukturlar. B., 1981.

12. Bахşəliyev Y.R. Qruplar nəzəriyyəsinin elementləri və ikihədli tənliklər. Azərbaycan Texniki Universitetinin elmi əsərləri (Fundamental elmlər), №2, cild 11(6), Bакı, 2003.

ОБ ОДНОЙ ЗАДАЧЕ ТЕОРИИ ЧИСЕЛ НАД КОНЕЧНЫМИ ПОЛЯМИ И ГРУППАМИ

Я.Р БАХШАЛИЕВ

РЕЗЮМЕ

В работе изучаются кольцо Z_p и его мультипликативная группа на основе свойств вычетов высших степеней по простому модулю $p > 2$.

ON ONE PROBLEM OF NUMBER THEORY WITH FINITE FIELDS AND GROUPS

Y.R.BAKSHALIYEV

SUMMARY

This work presents a study of Z_p-ring and its multiplicative group based on the properties of high degree subtracts with a simple module $p>2$.