EYLER HÁM FERMA TEOREMALARINIŃ QOLLANILIWLARI

[1]Yusupov Muzaffar Alliyar ulı,
[2]Satniyazova Indira Qaniyaz qızı,
[3]Maksatov Sunkat Muxit ulı
[1,2,3]Qaraqalpaq mámleketlik universiteti, student

Dáslep Eyler hám Ferma teoremaların keltirip óteyik.

1-teorema. (Eyler teoreması) Qálegen n modulı hám n menen óz ara ápiwayı bolǵan qálegen $a \geq 1$ sanı ushın

$$a^{\varphi(n)} \equiv 1 \,(\mathrm{mod}\, n) \tag{1}$$

salıstırıwı orınlı boladı.

Dálilleniwi. Haqıyqatında da, r_1, r_2, r_3, …, $r_{\varphi(n)}$ sanları n modulı boyınsha qandayda bir keltirilgen qaldıqlar sistemasın payda etetuǵın bolsın. Demek, $(a,n)=1$ bolǵan jaǵdayda ar_1, ar_2, ar_3, …, $ar_{\varphi(n)}$ sanları da n modulı boyınsha keltirilgen qaldıqlar sistemasın payda etedi. Sonlıqtan ar_1, ar_2, ar_3, …, $ar_{\varphi(n)}$ sanlarınıń hár qaysısına olar menen salıstırmalı bolǵan r_1, r_2, r_3, …, $r_{\varphi(n)}$ sistemasınıń sanların sáykes qoyıw r_1, r_2, r_3, …, $r_{\varphi(n)}$ hám ar_1, ar_2, ar_3, …, $ar_{\varphi(n)}$ sistemalarınıń arasında óz-ara bir mánisli sáykeslik ornatıwǵa boladı. Solay etip,

$$\begin{aligned} ar_1 &\equiv r_\alpha \,(\mathrm{mod}\, n) \\ ar_2 &\equiv r_\beta \,(\mathrm{mod}\, n) \\ &\dots\dots\dots\dots\dots \\ ar_{\varphi(n)} &\equiv r_\gamma \,(\mathrm{mod}\, n) \end{aligned} \tag{2}$$

salıstırıwlar sisteması, yaǵnıy r_1, r_2, …, $r_{\varphi(n)} = r_\alpha$, r_β, …, r_γ teńligi orınlı boladı. Bunda r_α, r_β, …, r_γ sanları r_1, r_2, …, $r_{\varphi(n)}$ sanlarınan qandayda bir orın almastırıw nátiyjesinde kelip shıǵadı. (2) sistemanıń salıstırıwların aǵzama-aǵza kóbeytiw arqalı

$$a^{\varphi(n)} \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(n)} \equiv r_\alpha \cdot r_\beta \cdot \ldots \cdot r_\gamma \,(\mathrm{mod}\, n) \tag{3}$$

salıstırıwına iye bolamız. Sonda, barlıq i ler ushın $(r_i,n)=1$ bolǵanlıqtan bizge belgili salıstırıwdıń qásiyetleri boyınsha (3) tıń eki tárepinde r_1, r_2, …, $r_{\varphi(n)}$ ge qısqartıwǵa boladı. Solay etip, biz $a^{\varphi(n)} \equiv 1(\mathrm{mod}\, n)$ salıstırıwına iye bolamız.

2-teorema. (Fermanıń kishi teoreması) Qálegen ápiwayı p hám p ǵa bólinbeytuǵın qálegen $a \geq 1$ sanı ushın

$$a^{p-1} \equiv 1 \,(\mathrm{mod}\, p) \tag{4}$$

salıstırıwı orınlı boladı.

Fermanıń kishi teoreması Eyler teoremasınıń dara jaǵdayınan ibarat.

Haqıyqatında da, Eyler teoremasında $n = p$ dep alsaq (bunda p sanı ápiwayı san), onda $(a, p) = 1$ shárti $a \not\vdots\, p$ shárti menen ekvivalent hám $\varphi(p) = p - 1$ boladı. Solay etip, $n = p$ bolǵan jaǵdayda Eyler teoreması $a \not\vdots\, p$ ushın $a^{p-1} \equiv 1 \pmod p$ salıstırıwına, yaǵnıy Fermanıń kishi teoremasına aylanadı.

3-teorema. (Ferma teoreması) Qálegen ápiwayı p hám natural a sanları ushın

$$a^p \equiv a \pmod p \qquad (5)$$

salıstırıwı orınlı boladı.

Dálilleniwi. Eger $a \not\vdots\, p$ bolsa, onda biz (4) salıstırıwdıń eki bóleginde a ǵa kóbeytiw arqalı $a^p \equiv a \pmod p$ salıstırıwına iye bolamız. Eger $p|a$ bolsa, onda $p|(a^p - a)$ bolıp, taǵı da $a^p \equiv a \pmod p$ ekenligi kelip shıǵadı. Solay etip, (5) salıstırıw qálegen natural a ushın orınlı boladı.

Eyler hám Ferma teoremaların berilgen sannıń úlken dárejelerin modulge bólgende kelip shıǵatuǵın qaldıqtı tabıwda qollanıwǵa boladı.

Haqıyqatında da, $(a, n) = 1$ hám $N > \varphi(n)$ bolǵan jaǵdayda a^N dı n ge bólgende kelip shıǵatuǵın qaldıqtı tabıw ushın N dı

$$N = \varphi(n)q + r\,,\ 0 \le r < \varphi(n)$$

túrinde jaza alamız. Sonda, biz bunnan

$$a^N = a^{\varphi(n)q+r} = (a^{\varphi(n)})^q \cdot a^r \equiv a^r \pmod n$$

ekenligin payda etemiz. Bunda a^r sanı a^N ge salıstırǵanda aytarlıqtay kishi bolıp tabıladı. Eger $(a, n) = d > 1$ bolsa, onda $a = a_1 d$, $n = n_1 d$, $(a_1, n_1) = 1$ ekenligi kelip shıǵadı. Al, a^N dı n ge bólgende kelip shıǵatuǵın qaldıqtı x arqalı belgilesek, onda biz

$$a^{N-1} a_1 d \equiv x \pmod{n_1 d}$$

salıstırıwına iye bolamız. Bunnan $x = x_1 d$ hám $a^{N-1} a_1 \equiv x_1 \pmod{n_1}$ ekenligi payda etiledi. Bunda x_1 di a^{N-1} hám a_1 sanların n_1 ge bólgende kelip shıǵatuǵın qaldıqlardı kóbeytiw arqalı tabıwǵa boladı. a^N di n_1 ge bólgende payda bolatuǵın qaldıqtı tabıw ushın n_1 modulı ushın Eyler teoremasın paydalanıwǵa boladı.

1-mısal. 7^{112} sanın 11 ge bólgendegi qaldıqtı tabıń.

Sheshiliwi. $(7,11) = 1$ hám 11 sanı ápiwayı san bolsa, onda Ferma teoreması boyınsha

$$7^{11-1} \equiv 1 \pmod{11} \Rightarrow 7^{10} \equiv 1 \pmod{11} \Rightarrow (7^{10})^{11} \equiv 1^{11} \pmod{11} \Rightarrow$$
$$\Rightarrow 7^{110} \equiv 1 \pmod{11} \Rightarrow 7^{112} \equiv 7^2 \pmod{11} \Rightarrow 7^{112} \equiv 5 \pmod{11}$$

ekenligi kelip shıǵadı. Demek, qaldıq 5 ke teń.

2-mısal. 14^{131} sanın 9 ge bólgendegi qaldıqtı tabıń.

Sheshiliwi. $(14,9)=1$ hám 9 sanı ápiwayı san bolmaǵanlıqtan, onda Eyler teoreması boyınsha

$$14^{\varphi(9)} \equiv 1 \,(\mathrm{mod}\, 9)$$

qatnası orınlı boladı. Endi $\varphi(9)$ dı esaplaymız:

$$\varphi(9)=9\cdot\left(1-\frac{1}{3}\right)=9\cdot\frac{2}{3}=6\,.$$

Bunnan

$$14^{\varphi(9)} \equiv 1 \,(\mathrm{mod}\, 9) \Rightarrow 14^{6} \equiv 1 \,(\mathrm{mod}\, 9)$$

boladı hám salıstırıwdıń qásiyeti boyınsha

$$14^{6} \equiv 1 \,(\mathrm{mod}\, 9) \Rightarrow 14^{126} \equiv 1 \,(\mathrm{mod}\, 9) \Rightarrow 14^{131} \equiv 14^{5} \,(\mathrm{mod}\, 9)$$

hám

$$14 \equiv 5 \,(\mathrm{mod}\, 9) \Rightarrow 14^{2} \equiv 25 \,(\mathrm{mod}\, 9) \Rightarrow 14^{2} \equiv 7 \,(\mathrm{mod}\, 9) \Rightarrow$$

$$\Rightarrow 14^{4} \equiv 49 \,(\mathrm{mod}\, 9) \Rightarrow 14^{4} \equiv 4 \,(\mathrm{mod}\, 9) \Rightarrow$$

$$\Rightarrow 14^{5} \equiv 56 \,(\mathrm{mod}\, 9) \Rightarrow 14^{5} \equiv 2 \,(\mathrm{mod}\, 9)$$

boladı. Demek, $14^{131} \equiv 2 \,(\mathrm{mod}\, 9)$ ekenligi kelip shıǵadı.

3-mısal. $53^{53}\cdot 38^{11}$ kóbeymeni 9 ǵa bólgendegi qaldıqtı tabıń.

Sheshiliwi. 53^{53} sanın 9 ǵa bólgendegi qaldıqtı anıqlap alamız: $(53,9)=1$ hám 9 sanı ápiwayı san bolmaǵanlıqtan, onda Eyler teoreması boyınsha

$$53^{\varphi(9)} \equiv 1 \,(\mathrm{mod}\, 9) \Rightarrow 53^{6} \equiv 1 \,(\mathrm{mod}\, 9) \Rightarrow (53^{6})^{8} \equiv 1^{8} \,(\mathrm{mod}\, 9) \Rightarrow$$

$$\Rightarrow 53^{48} \equiv 1 \,(\mathrm{mod}\, 9) \Rightarrow 53^{53} \equiv 53^{5} \,(\mathrm{mod}\, 9)$$

boladı. Bunnan

$$53 \equiv 8 \,(\mathrm{mod}\, 9) \Rightarrow 53^{2} \equiv 64 \,(\mathrm{mod}\, 9) \Rightarrow 53^{2} \equiv 1 \,(\mathrm{mod}\, 9) \Rightarrow$$

$$\Rightarrow 53^{4} \equiv 1^{2} \,(\mathrm{mod}\, 9) \Rightarrow 53^{5} \equiv 53 \,(\mathrm{mod}\, 9) \Rightarrow 53^{5} \equiv 8 \,(\mathrm{mod}\, 9)$$

boladı. Demek, $53^{53} \equiv 8 \,(\mathrm{mod}\, 9)$ ekenligi kelip shıǵadı.

Endi 38^{11} sanın 9 ǵa bólgendegi qaldıqtı anıqlaymız: $(38,9)=1$ hám 9 sanı ápiwayı san bolmaǵanlıqtan, onda Eyler teoreması boyınsha

$$38^{\varphi(9)} \equiv 1 \,(\mathrm{mod}\, 9) \Rightarrow 38^{6} \equiv 1 \,(\mathrm{mod}\, 9) \Rightarrow 38^{11} \equiv 38^{5} \,(\mathrm{mod}\, 9) \Rightarrow$$

$$\Rightarrow 38 \equiv 2 \,(\mathrm{mod}\, 9) \Rightarrow 38^{4} \equiv 16 \,(\mathrm{mod}\, 9) \Rightarrow 38^{4} \equiv 7 \,(\mathrm{mod}\, 9) \Rightarrow$$

$$\Rightarrow 38^{5} \equiv 266 \,(\mathrm{mod}\, 9) \Rightarrow 38^{5} \equiv 5 \,(\mathrm{mod}\, 9) \Rightarrow 38^{11} \equiv 5 \,(\mathrm{mod}\, 9)$$

ekenligi kelip shıǵadı. Bunnan

$$\begin{cases} 53^{53} \equiv 8 \,(\mathrm{mod}\, 9) \\ 38^{11} \equiv 5 \,(\mathrm{mod}\, 9) \end{cases} \Rightarrow 53^{53}\cdot 38^{11} \equiv 40 \,(\mathrm{mod}\, 9) \Rightarrow 53^{53}\cdot 38^{11} \equiv 4 \,(\mathrm{mod}\, 9)$$

boladı. Demek, $53^{53}\cdot 38^{11}$ kóbeymeni 9 ǵa bólgendegi qaldıq 4 ke teń.

Paydalanılǵan ádebiyatlar dizimi

1. Alauadinov A.K., Boranbaev O.B. «Arifmetikalıq funkciyalar». Nókis, 2024.
2. О. Сапарниязов. «Санлар теориясының тийкарлары». Нөкис, 1992.
3. А. А. Бухштаб. «Теория чисел». Москва, 1966.