III. 1-§.

159. Barcha butun sonlarni 1 ga bo'lsak 0 qoldiq qoladi, ya'ni barcha butun sonlar 1 moduli bo'yicha o'zaro taqqoslanuvchi.

160. 8 moduli bo'yicha taqqoslanuvchi sonlar $8q + r,\ 0 \le r < 8$; masalan $r = 1$ da 9,17 lar 8 moduli bo'yicha o'zaro taqqoslanadi, chunki $9 = 8 \cdot 1 + 1$ va $17 = 8 \cdot 2 + 1$.

161. a) $1 \equiv -5(mod6), 1 \equiv 6 - 5(mod6), 1 \equiv 1(mod6)$;

b) $546 \equiv 0(mod13), 546 \equiv 13 \cdot 42 + 0, 0 \equiv 0(mod13)$;

c) $2^3 \equiv 1(mod4), 8 \equiv 1(mod4),\ 0 \equiv 1(mod4)$?

d) $3m \equiv -1(modm), 0 \equiv m - 1(modm)$?

Demak, $a), b)$ taqqoslamalar o'rinli, $c), d)$ lar o'rinli emas.

162. $a \equiv b(modm)$ taqqoslamaning o'rinli ekanligini ko'rsatish uchun a va b larni m ga bo'lganda bir xil qoldiq qolishini yoki $(a - b) \vdots m$ ni ko'rsatish yetarli.

a) $121 \equiv 13145(mod2)$, chunki $121 \equiv 2 \cdot 60 + 1$ va $13145 \equiv 2 \cdot 6572 + 1$

Berilgan sonlarni 2 ga bo'lsak, bir xil qoldiq qoladi. Shuning uchun ham ular 2 moduli bo'yicha taqqoslanuvchi.

b) $121347 \equiv 92817(mod10)$, bu yerda $121347 = 12134 \cdot 10 + 7,\ 92817 = 9281 \cdot 10 + 7$. Demak ta'rifga ko'ra taqqoslama o'rinli.

c) $31 \equiv -9(mod10), 31 - (-9) \equiv 40 \vdots 10$. Demak, taqqoslama o'rinli.

d) $(m - 1)^2 \equiv 1(modm)$, bu yerda $(m - 1)^2 - 1 = m^2 - 2m = m(m - 2) \vdots m$. Demak, taqqoslama o'rinli.

e) $2m + 1 \equiv (m + 1)^2(modm)$, chunki $2m + 1 - (m + 1)^2 = 2m + 1 - m^2 - 2m - 1 = -m^2 \vdots m$. Demak, berilgan taqqoslama o'rinli.

163. *a)*$5^{1812} = (5^2)^{906} = (25 \cdot 1 + 0)^{906} \equiv 0(mod25)$. Shuningdek, $1964 = 1950 + 14 = 78 \cdot 25 + 14 \equiv 14(mod25)$, demak, bu sonlar 25 moduli bo'yicha teng qoldiqli emas, ya'ni$5^{1812} \not\equiv 1964(mod25)$.

b) agar $a \equiv b(modm)$bo'lsa, $(a, m) = (b, m)$ bo'lishi kerak. Bizning misolimizda $(7^{103}; 87) = 1;\ (3; 87) = 3$. Demak, $7^{103} \not\equiv 3(mod87)$.

c) $4^{1965} \equiv 25(mod10)$ da$(4^{1965}; 10) = 2$va$(25,10) = 5,\ 5 \ne 2$ bo'lgani uchun $4^{1965} \not\equiv 25(mod\ 10)$.

d) $30 \cdot 17 \equiv 81 \cdot 19(mod6)da\ 30 \cdot 17 \equiv 0(mod6), 81 \cdot 19 \not\equiv (mod6)$ demak, taqqoslama o'rinli emas.

e) $(2n + 1)(2m + 1) \equiv 2k(mod6)$. Bu yerdan tenglikga o'tsak,

$(2n + 1)(2m + 1) = 2k + 6t = 2(k + 3t)$. Bu tenglikning o'ng tomoni 2 ga bo'linadi, chap tomoni esa 2 ga bo'linmaydi. Shuning uchun ham taqqoslama o'rinli emas.

164. a butun soni va $m > 0$ butun soni berilgan bo'lsin. U holda qoldiqli bo'lish haqida teoremaga asosan $a = m \cdot q + r,\ 0 \le r < m$ deb yoza olamiz. Bundan $a - r = mq$, ya'ni$(a - r) \vdots m$. U holda ta'rifga asosan $a \equiv r(modm)$.

165. $x \equiv 2(mod10)$ ni tenglik ko'rinishida yozsak $x = 2 + 10t,\ t \in Z, x = 2, 12, 22, -8, -18$.

166. $a) x \equiv 0(mod3), x = 3t,\ t \in Z$; b) $x \equiv 1(mod2), x = 1 + 2t,\ t \in Z.$

167. $a)\ 20 \equiv 8(modm) \Rightarrow \left.\begin{matrix} 20 = mq + r \\ 8 = mq_1 + r \end{matrix}\right\} \Rightarrow 12 = m(q - q_1) \Rightarrow m =$ 1,2,3,4,6,12.

b) $3p + 1 \equiv p + 1(modm) \Rightarrow 3p + 1 - p - 1 \equiv 0(modm) \Rightarrow 2p \equiv 0(modm) \Rightarrow\ 2p \vdots m.$ $2p$ ning bo'luvchilari $m = 1, 2, p, 2p.$

168. $13 \equiv 5(modm) \rightarrow 13 - 5 \equiv 0(modm) \rightarrow 8 \equiv 0(modm) \Rightarrow m =$ 1,2,4,8.

169. Ta'rifga ko'ra 10 modul bo'yicha taqqoslanuvchi butun sonlarni 10 ga bo'lganda bir xil qoldiq qolishi kerak, ya'ni ular $a = 10 \cdot q + r, 0 \leq r < 10$ shartni qanoatlantirishi kerak. Misol uchun $r = 1$ deb olsak, barcha 10 ga bo'lganda $1, 11, 101,\ 1001, \ldots$ larga ega bo'lamiz.

170. Berilgan taqqoslamalardan qaysilari o'rinli ekanligini aniqlash uchun m modul bo'yicha taqqoslanuvchi sonlarning ayirmasi shu modulga qoldiqsiz bo'linishini tekshirib ko'rish kifoya.

a) da $1 - (-11) = 1 + 11 = 12$ va 12 soni 6 ga qoldiqsiz bo'linadi. Demak, berilgan taqqoslama o'rinli.

b) da $3n - n^2 = n(3 - n)$ va$n(3 - n)$ soni $n$ga qoldiqsiz bo'linadi. Demak, berilgan taqqoslama o'rinli.

c) da $2^6 - 1 = 63 = 7 \cdot 9$ va $7 \cdot 9$ soni 7 ga qoldiqsiz bo'linadi. Demak, berilgan taqqoslama o'rinli.

d) da $3m - 1 = 2m + (m - 1)$ va $2m + (m - 1)$ soni $m > 1$ga qoldiqsiz bo'linmaydi. Demak, berilgan taqqoslama o'rinli emas.

Shunday qilib berilgan taqqoslamalardan a), b), c) lar o'rinli, d) esao'rinli emas.

171. Berilgan taqqoslamani parametrik tenglik qilib yozsak, $x = 7 + 5t$, bunda t ixtiyoriy butun son. Bundan $x = 2 + 5 + 5t = 2 + 5(t + 1) = 2 + 5t_1,\ t_1$ - ixtiyoriy butun son. Demak x 5ga bo'lganda 2 qoldiq qoluvchi sonlardan $\cdots, -13, -8, -3, 2, 7, 12, 17, \cdots$ iborat bo'lar ekan.

172. Faraz etaylik $\left.\begin{matrix} x \equiv \alpha \\ y \equiv \beta \\ z \equiv \gamma \end{matrix}\right\}(modm)$ bo'lsin. U holda

$$\left.\begin{matrix} ax^3 \equiv a\alpha^3 \\ bx^2y \equiv b\alpha^2\beta \\ cxyzc = c\alpha\beta\gamma \\ dz \equiv d\gamma \end{matrix}\right\}(modm)$$

bajariladi. Bundan $F(x, y, z) \equiv\ F(\alpha, \beta, \gamma)(modm)$ kelib chiqadi.

173. $3^n \equiv -1(modm)$ ni $3^4 = 81 \equiv 1(mod10)$ taqqoslamaga hadlab ko'paytirsak, $3^{n+4} \equiv -1(mod10)$ hosil bo'ladi.

174. $2^{5n}-1=(2^5)^n-1=(31+1)^n-1\equiv(1^n-1)(mod31)\equiv 0(mod31)$demak$(2^{5n}-1):31$.

175. $x=3n+1$bo'lsa $1+3^x+9^x=1+3^{3n+1}+9^{3n+1}=1+3\cdot3^{3n}+9\cdot9^{3n}=1+3\cdot(3^3)^n+9\cdot(9^3)^n=1+3(26+1)^n+9(128+1)^n=1+3(13\cdot2+1)^n+9(13\cdot56+1)^n\equiv1+3\cdot1^n+9\cdot1^n(mod13)\equiv13(mod13)\equiv 0(mod13)$. Demak, $1+3^x+9^x$ soni $x=3n+1$ $(n=0,1,2,\dots)$ bo'lganda 13 ga bo'linadi.

176. $(a+b)^p$ ni Nyuton binomi formulasidan foydalanib yoyib, keyin p moduli bo'yicha taqqoslamaga o'tamiz. $(a+b)^p=\ a^p+pa^{p-1}b+\frac{p(p-1)}{2!}a^{p-2}b^2+\cdots+ab^{p-1}+b^p\equiv a^p+b^p(modp)$, ya'ni $(a+b)^p\equiv a^p+b^p(modp)$.

177. Masalaning sharti bo'yicha $a\equiv b(modp^n)$. Buni tenglik qilib yozsak, $a=b+p^n\cdot t,\ (t=0,\pm1,\pm2\dots)$. Bu tenglikni ikkala tomonini p-darajaga ko'taramiz, u holda $a^p=(b+p^nt)^p=b^p+p^{n+1}q,\ (q=0,\pm1,\pm2,\dots)$. Oxirgi tenglik esa $a^p\equiv b(modp^{n+1})$ taqqoslamaga teng kuchli.

178. Agar $(x;m)=1$ bo'lsa, $ax\equiv bx(modm)$ taqqoslamaning ikkala tomonini x ga qisqartirish mumkin, ya'ni $a\equiv b(modm)$, bundan $a\equiv b\left(mod\,\frac{m}{(x,m)}\right)$ taqqoslama o'rinli ekanligi kelib chiqadi. Agar $(x,m)=d>1$ bo'lsa, $x=dx_1$ va $m=dm_1$, $(m_1;x_1)=1$ deb yoza olamiz. Bulardan foydalanib, $ax\equiv bx(modm)$ taqqoslamani $adx_1\equiv bdx_1(modm_1d)$ deb yoza olamiz. Berilgan taqqoslamaning ikkala tomonini va modulini ularning umumiy bo'luvchisiga qisqartirish mumkin. Shuning uchun ham oxirgi taqqoslamani $ax_1\equiv bx_1(modm_1)$ ko'rinishda yozish mumkin. Bundan, $(x_1;m_1)=1$ bo'lgan uchun, $a\equiv b(modm_1)$ ga, ya'ni $a\equiv b(mod\,\frac{m}{d})$ ga ega bo'lamiz. Bunda $d=(m,x)$ bo'lgani uchun $a\equiv b\left(mod\,\frac{m}{(x,m)}\right)$ ni hosil qilamiz.

179. Bunda $\overline{a_4a_3a_2a_1a_0}\equiv0(mod33)$ taqqoslamani $a_410^4+\overline{a_3a_2}\cdot10^2+\overline{a_1a_0}\equiv0(mod33)$ ko'rinishda yozib olamiz va undan $9999a_4+99\overline{a_3a_2}\equiv 0(mod33)$ ayniy taqqoslamani hadlab ayiramiz. U holda isbotlanishi talab etilgan taqqoslama $a_410^4+\overline{a_3a_2}+\overline{a_1a_0}\equiv0(mod33)$ hosil bo'ladi.

180. 1). Berilgan taqqoslamalarni $p-1\equiv-1(modp),\ p-2\equiv -2(modp),\dots,p-n\equiv-n(modp)$ ko'rinishida yozib olib, hadlab ko'paytiramiz. U holda $(p-1)(p-2)\dots(p-n)\equiv(-1)^nn!\,(modp)$ hosil bo'ladi. Bunda $(n!,p)=1$ bo'lgani uchun oxirgi taqqoslamaning ikkala tomonini $n!$ ga bo'lib $\frac{(p-1)(p-2)\dots(p-n)}{n!}\equiv(-1)^n(modp)$ ni hosil qilamiz. Buning chap tomoni C_{p-1}^n ga teng. Shuning uchun ham $C_{p-1}^n\equiv(-1)^n(modp)$ bajariladi.

2) 22.1-misoldagi singari $p-2\equiv -2(modp),\dots,p-n\equiv -n(modp),\ p-(n+1)\equiv -(n+1)(modp)$ lardan $(p-2)(p-3)\dots(p-n)\big(p-(n+1)\big)\equiv(-1)^n(n+1)!\,(modp)$ ni, bundan esa $\frac{(p-2)(p-3)\dots(p-n)\big(p-(n+1)\big)}{n!}\equiv(-1)^n(n+1)(modp)$ ni hosil qilamiz. Shuning uchun ham $C_{p-2}^{n+1}\equiv(-1)^n(n+1)(modp)$.

181. 1). $9^{10}=(10-1)^{10}=100t+1\equiv 1(mod100)$ bo'lgani uchun $9^{10q+r}\equiv 9^r(mod100)$ bo'ladi. $9^9=(9^2)^4\cdot 9=81^4\cdot 9\equiv 9(mod10)$ dan $9^9=9+10t_1$; u holda $9^{9^9}\equiv 9^{9+10t_1}(mod100)\equiv 9^9(mod100)\equiv(9^3)^3\equiv 729^3(mod100)\equiv 29^3(mod100)\equiv 24389(mod100)\equiv 89(mod100)$. Demak, izlanayotgan oxirgi ikkita raqam 8 va 9.

2) $7^4=2401\equiv 1(mod100)$dan $7^{100}=(7^4)^{25}\equiv 1(mod100)$. Bu yerdan $7^{9^{9^9}}\equiv 7^{100q+89}(mod100)$ (1) $-$ misolga qarang) $7^{100q+89}\equiv(7^{100})^q\cdot 7^{89}(mod100)\equiv 7^{89}(mod100)\equiv 7^{88}\cdot 7(mod100)\equiv(7^4)^{22}7(mod100)\equiv 7(mod100)$. Demak, izlanayotgan oxirgi 2ta raqam 0 va 7.

182. $p>2$ – toq tub son bo'lgani uchun $p+2$ ham toq son bo'ladi, ya'ni $p\equiv p+2\equiv 1(mod2)$ (1) bajariladi. Bundan $p^{p+2}+(p+2)^p\equiv(2k+1)^{p+2}+(2q+1)^p\equiv 2(mod2)\equiv 0(mod2)$. Shuningdek tushunarliki, $p\equiv -1(mod\,p+1)$ va $p+2\equiv 1(mod\,p+1)$ bajariladi. Oxirgi 2 ta taqqoslamadan $p^{p+2}+(p+2)^p\equiv(-1)^{p+2}+1^p(mod\,p+1)\equiv -1+1(mod\,p+1)\equiv 0(mod\,p+1)$ (2). (1) va (2) dan$p^{p+2}+(p+2)^p\equiv 0(mod\ 2p+2)$ taqqoslama kelib chiqadi.

183. Qaralayotgan sonlarni juft-jufti bilan birlashtirib (noldan tashqarilarini) $\pm\frac{p-x}{2}$, $(x=1,2,\dots p-2)$ ko'rinishda yozish mumkin. Endi agarda bu sonlar ichida $p>2$ moduli bo'yicha o'zaro taqqoslanuvchilari bor desak, $\pm\frac{p-x}{2}\equiv 0(modp)$ yoki $\frac{p-x_1}{2}\equiv\pm\frac{p-x_2}{2}(modp)$ larning birortasi bajarilishi kerak. Bulardan $x\equiv p(modp)$va$x_1\equiv\pm x_2(modp)$ larga ega bo'lamiz. Birinchi holda $x=0$ (chunki $x<p$), ikkinchi holda esa $x_1=x_2$ yoki $x_1=-x_2$ga ega bo'lamiz. Bu esa qaralayotgan sonlar orasida o'zaro taqqoslanuvchilari yo'q ekanligini bildiradi.

184. Berilgan $i\equiv i-m(modm)$ taqqoslamadan $i=1,2,\dots,m$ da

$1\equiv 1-m, 2\equiv 2-m,\dots,m-2\equiv(m-2)-m\equiv 2, m-1\equiv m-1-m\equiv -1,\ \ m\equiv -m(modm)$ larga ega bo'lamiz. Bularning barchasini n-darajaga ko'tarib keyin hadlab qo'shsak:

$$1^n+2^n+\dots+m^n\equiv(-1)^n+(-2)^n+\dots+(-m)^n(modm)\qquad(1)$$

hosil bo'ladi. Bundan agar $n = 2k + 1$toq son bo'lsa (shart bo'yicha m va n lar toq sonlar), $1^n + 2^n + \cdots + m^n \equiv -(1^n + 2^n + \cdots + m^n)(mod m)$, yoki

$$2\sum_{i=1}^{m} i^n \equiv 0(mod m), \text{ya'ni} \sum_{i=1}^{m} i^n \equiv 0(mod m)$$

kelib chiqadi.

185. Taqqoslamaning o'rinli ekanligini matematik induksiya metodidan foydalanib isbotlaymiz. $n = 1$ da berilgan $2^{3^n} \equiv -1(mod 3^{n+1})$ taqqoslama $2^3 \equiv -1(mod 9)$ ko'rnishni oladi. Bu taqqoslama $2^3 \equiv 8(mod 9)$ ayniy taqqoslamaga teng kuchli. Demak, $n = 1$ da taqqoslama o'rinli. Endi faraz etaylik berilgan taqqoslama $n = k$ uchun$2^{3^k} \equiv -1(mod 3^{k+1})$ o'rinli bo'lsin va biz $n = k + 1$ uchun uning, ya`ni $2^{3^{k+1}} \equiv -1(mod 3^{k+2})$ ning o'rinli ekanligini ko'rsatamiz.

$$2^{3^{k+1}} + 1 = \left(2^{3^k}\right)^3 + 1^3 = \left(2^{3^k} + 1\right)\left(2^{3^k \cdot 2} - 2^{3^k} + 1\right)$$

bu yerda induktivlik farazimizga ko'ra $2^{3^k} + 1 \equiv 0(mod 3^{k+1})$ va $2 \equiv (-1)(mod 3)$ bo'lgani uchun $2^{2\cdot 3^k} - 2^{3^k} + 1 \equiv 0(mod 3)$bo'ladi. Bulardan $2^{3^k} + 1 \equiv 0(mod 3^{k+1})$ ning bajarilishi kelib chiqadi. Demak, matematik induksiya metodiga ko'ra berilgan taqqoslama ixtiyoriy natural n soni uchun o'rinli.

186. Masalaning shartiga ko'ra $2^{3^n} + 1 \equiv 0(mod 3^{n+1})$ bajariladi. U holda $2^{3^n} + 1 \equiv 0(mod 3^n)$ taqqoslama, albatta, bajariladi. Agar bundan $m = 3^n, (n = 1,2,3, \ldots)$ deb olsak, $2^m + 1 \equiv 0(mod m)$ taqqoslama kelib chiqadi. Bu yerda $m = 3^n, (n = 1,2,3, \ldots)$ bo'lgani uchun $2^m + 1 \equiv 0(mod m)$ taqqoslama, natural sonlarda cheksiz ko'p yechimga ega bo'ladi.

187. Taqqoslamaning o'rinli ekanligini n bo'yicha matematik induksiya metodini qo'llab isbotlaymiz. $n = 1$ da berilgan$(m-1)^{m^n} \equiv -1(mod m^{n+1})$ taqqoslama $(m-1)^m \equiv -1(mod m^2)$ ko'rinishni oladi. Bundan $(m-1)^m + 1 \equiv 0(mod m^2)$, yoki $(m > 1 - \text{toq son})(m - 1 + 1)((m-1)^{m-1} - (m-1)^{m-2} + \cdots + 1) \equiv 0(mod m^2)$. Bu taqqoslamaning ikkala tomoni va moduli m ga bo'lib,

$(m-1)^{m-1} - (m-1)^{m-2} + \cdots + 1 \equiv 0(mod m)$ga ega bo'lamiz. Bundan$(-1)^{m-1} - (-1)^{m-2} + \cdots + 1 \equiv 0(mod m)$. Yoki $\underbrace{1 + 1 + 1 + 1 + \cdots + 1}_{mta} \equiv 0(mod m) \to m \equiv 0(mod m)$. Shunday qilib berilgan taqqoslama $n = 1$ da o'rinli ekan. Endi faraz etaylik, $n = k$ uchun berilgan taqqoslama, ya'ni $(m-1)^{m^k} \equiv -1(mod m^{k+1})$ o'rinli bo'lsin. Biz berilgan taqqoslamaning $n = k + 1$ bo'lganda, ya'ni $(m-1)^{m^{k+1}} \equiv -1(mod m^{k+2})$ taqqoslamaning o'rinli ekanligini isbotlaymiz. Bu yerda$m$ $-$toq son va

$(m-1)^{m^{k+1}}+1=\left[(m-1)^{m^k}\right]^m+1=\left[(m-1)^{m^k}+1\right]\left((m-1)^{(m-1)m^k}-(m-1)^{(m-2)m^k}+\cdots+1\right)\equiv 0(modm^{k+2})$.

Oxirgi taqqoslamaning o'ng tomonidagi birinchi ko'paytuvchi uchun induktivlik farazimizga asosan $(m-1)^{m^k}+1\equiv 0(modm^{k+1})$ bajariladi. Ikkinchi ko'paytuvchi uchun esa $(m-1)^{(m-1)m^k}-(m-1)^{(m-2)m^k}+\cdots+1\equiv \underbrace{1+1+\cdots+1}_{mta}\equiv m(modm)\equiv 0(modm)$ bajariladi. Keyingi 2 ta taqqoslamadan $(m-1)^{m^{k+1}}\equiv -1(modm^{k+2})$ kelib chiqadi. Shunday qilib matematik induksiya prinspiga asosan berilgan taqqoslama ixtiyoriy n natural soni uchun o'rinli.

188. Masalaning shartiga ko'ra $(m-1)^{m^n}\equiv -1(modm^{n+1})$ taqqoslama o'rinli. Bundan $m=5$ da $4^{5^n}\equiv -1(mod5^{n+1})$, ya'ni $4^{5^n}+1\equiv 0(mod5^{n+1})$. Bu holda $4^{5^n}+1\equiv 0(mod5^n)$ taqqoslama albatta bajarilishi kerak. Endi agar biz $5^n\equiv x$ $(n=1,2,3,\dots)$ deb olsak, $2^{2x}+1\equiv 0(modx)$ taqqoslamaga ega bo'lamiz. Bu yerda $x=5^n$ $(n=1,2,3,\dots)$ bo'lgani uchun oxirgi taqqoslama natural sonlarda cheksiz ko'p yechimga ega.

189. 1). Bu yerda $2^{4n+1}\equiv 2\cdot(2^4)^n(mod5)$, ya'ni $2^{4n+1}=2+5t, t\in N$ bo'lgani uchun $N=3^{2^{4n+1}}+2=3^{2+5t}+2=9\cdot(3^5)^t+2=9(243)^t+2\equiv 9(11\cdot 22+1)^t+2\equiv 9+2(mod11)\equiv 0(mod11)$, ya'ni $N>11$ va $N\vdots 11$. Demak, u murakkab son.

2).Bu yerda $3^{4n+1}=3\cdot(81)^n=3\cdot(8\cdot 10+1)^n\equiv 3(mod10)$, ya'ni $3^{4n+1}=3+10k$, $k\in N$. Shuning uchun ham $M=2^{3^{4n+1}}+3=2^{3+10k}+3=2^3\cdot(2^5)^{2k}+3=8(32)^{2k}+3\equiv 8(-1)^{2k}+3(mod11)\equiv 0(mod11)$. Bu yerdan $M>11$ bo'lgani uchun $M\vdots 11$ va u murakkab son degan xulosa kelib chiqadi.

190. 1).$2^x+7^y=19^z$ tenglamani qaraymiz. $19\equiv 1(mod3)$ bo'lganidan $19^z\equiv 1(mod3)$. Lekin $2^x\equiv(-1)^x(mod3)$ va $7^y\equiv 1(mod3)$ bo'lgani uchun $2^x+7^y\equiv(-1)^x+1(mod3)$. Bu yerdan, agar x juft son bo'lsa, $2^x+7^y\equiv 2(mod3)$; agarda $x-$toq son bo'lsa, $2^x+7^y\equiv 0(mod3)$ larga ega bo'lamiz. Shunday qilib $2^x+7^y\not\equiv 19^z(mod3)$. Bundan $2^x+7^y=19^z$ tenglama x,y,z natural sonlarda yechimga ega emas degan xulosaga kelamiz.

2). Endi $2^x+5^y=19^z$ tenglamani qaraymiz. Bu holda 1-misolga asosan $2^x+5^y=(-1)^x+(-1)^y(mod3)$. Agar bu yerda x va y larning ikkalasi ham toq son bo'lsa, $2^x+5^y\equiv -2\equiv 1(mod3)$ bo'ladi hamda $2^x+5^y=19^z(mod3)$ kelib chiqadi. Lekinda, agar $2^x+5^y=19^z$ tenglama x,y,z larning biror natural qiymatlarida o'rinli bo'lsa, 2^x+5^y va 19^z lar ixtiyoriy modul bo'yicha ham taqqoslanuvchi bo'lishi kerak $x=2n+1, y=2n+1$ bo'lsin. $2^x+5^y=19^z(mod5)$ taqqoslamani qaraymiz. $2^{2n+1}+5^{2n+1}=2\cdot 4^n+5^{2n+1}\equiv 2(-1)^n(mod5)$, qaralayotgan tenglamaning ikkinchi tomoni $19^z\equiv(-1)^z(mod5)$

bo'lgani uchun $2^{2n+1}+5^{2n+1}\not\equiv 19^z(mod5)$. Demak, $2^x+5^y=19^z$ tenglama x,y,z- natural sonlarda yechimga ega emas.

Izoh: Bu tenglamalarning yechimga ega emasligini taqqoslamalardan foydalanmasdan turib ham isbotlash mumkin. Masalan birinchi tenglamadan $2^x=19^z-7^y=(19^z-1)-(7^y-1)=18(19^{z-1}+19^{z-2}+\cdots+1)-6(7^{y-1}+7^{y-2}+\cdots+1)=3[6(19^{z-1}+19^{z-2}+\cdots+1)-2(7^{y-1}+7^{y-2}+\cdots+1)]$. Bu yerdan ko'rinadiki $(19^x-7^y)\vdots 3$. Lekinda 2^x soni 3 ga bo'linmaydi. Demak, $2^x\neq 19^z-7^y$, ya'ni $2^x-7^y\neq 19^z$.

191. Masala shartiga ko'ra $11\mathrm{a}+2b\equiv 0(mod\ 19)$ bo'lib, bu yerda taqqoslamalarning xossasiga ko'ra $30a+2b\equiv 0(mod\ 19)$ $=> 15a+b\equiv 0(mod\ 19)$ $=> b\equiv 4a(mod\ 19)$ ekanligini hosil qilamiz. Bunday holda $18\mathrm{a}+5b\equiv 18\mathrm{a}+20\mathrm{a}\equiv 38\mathrm{a}\equiv 0(mod\ 19)$ bo'lib, bundan esa

$18\mathrm{a}+5b\equiv 0(mod\ 19)$ ekanligi kelib chiqadi. Bu esa $\frac{18\mathrm{a}+5b}{19}$ ning ham butun son ekanligini isbotlaydi.

192. Berilgan taqqoslamada $n^2-1=(n-1)(n+1)$ bo'lib, *n* toq son bo'lgani uchun $(n-1)$ va $(n+1)$ lar ketma-ket keluvchi juft sonlar bo'ladi. Shuning uchun ham $n-1$ soni 2ga bo'linsa, $n+1$ soni 4ga bo'linadi. U holda ularning ko'paytmasi 8 ga bo'linadi. Shu tasdiqni taqqoslamalar tilida $n^2-1\equiv 0(mod8)$ ko'rinishda yoziladi.

193. Bu yerda $11\cdot 31-1=340=5\cdot 68$ va $2^5\equiv -1(mod11)$ bo'lgani uchun $2^{11\cdot 31-1}=(2^5)^{68}\equiv(-1)^{68}\equiv 1(mod11)$. Shuningdek $2^5\equiv 1(mod31)$ bo'lgani uchun $2^{11\cdot 31-1}=(2^5)^{68}\equiv 1^{68}\equiv 1(mod31)$.

Agar taqqoslama bir necha modul bo'yicha o'rinli bo'lsa, u shu modullarning eng kichik umumiy karralisi bo'yicha ham o'rinli bo'ladi (8-xossa). Shuning uchun ham $2^{11\cdot 31-1}\equiv 1(mod11\cdot 31)$. Bu oxirgi taqqoslamaning ikkala tomonini ayniy taqqoslama $2\equiv 2(mod11\cdot 31)$ga ko'paytirsak, isbotlanishi talab etilgan taqqoslama kelib chiqadi.

194. Bu yerda $1,2,3,\ldots,\frac{p-1}{2},\frac{p+1}{2},\ldots\ p-2,p-1$ sonlarini qarab ulardan quyidagi $\frac{p-1}{2}$ ta taqqoslamalarni tuzamiz:

$$1\equiv-(p-1)(modp),\ \ 2\equiv-(p-2)(modp),\ldots,\frac{p-1}{2}\equiv-\frac{p+1}{2}(modp).$$

Bu taqqoslamalarning har birini $2k+1$ darajaga ko'tarib qo'shamiz. U holda

$$1^{2k+1}+2^{2k+1}+3^{2k+1}+\cdots+\left(\frac{p-1}{2}\right)^{2k+1}\equiv-(p-1)^{2k+1}-(p-2)^{2k+1}-$$

$(p-3)^{2k+1}-\cdots-\left(\frac{p+1}{2}\right)^{2k+1}(modp)$ hosil bo'ladi. Bundan

$$1^{2k+1}+2^{2k+1}+3^{2k+1}+\cdots+\left(\frac{p-1}{2}\right)^{2k+1}+\left(\frac{p+1}{2}\right)^{2k+1}+\ \dots$$
$$+(p-3)^{2k+1}+(p-2)^{2k+1}+(p-1)^{2k+1}\equiv 0(modp).$$

III.2-§.

195. $m = 10$ moduli bo'yicha barcha sinflarni $x = 10\cdot q + r,\ 0\le r < 10$ ko'rinishda yozish mumkin. Bu tenglamani taqqoslama ko`rinishida yozsak $x\equiv r(mod10)$, bunda $r = 0,1,2,\dots,9$. Buni $x\equiv 0,1,2,\dots,9(mod10)$ ko`rinishida yozsak bo`ladi.

196. 1). $m = 9$ bo`lsa, $m$moduli bo`yicha chegirmalarning to`la sistemalari: $1,2,3,4,\ \dots,9$ 9 moduli bo`yicha eng kichik musbat chegirmalarining to`la sistemasi. $-9,-8,-7,\dots,-2,-1$ 9 moduli bo`yicha eng katta manfiy chegirmalarining to`la sistemasi; $0;\pm1;\ \pm2;\ \pm3;\ \pm4-$ 9 moduli bo`yicha absolyut qiymati jihatidan eng kichik chegirmalarining to`la sistemasi.

Endi $m=9$ modul bo`yicha chegirmalarning keltirilgan sistemalarini yozamiz. Ular mos ravishda quydagicha bo`ladi (buning uchun yuqorida yozilgan to`la sistemadagi chegirmalardan 9 bilan o`zaro tublarini ajratib olish kifoya):

$$1,2,4,5,7,8;\qquad -1,-2,-4,-5,-7,-8;\qquad \pm1;\ \pm2;\ \pm4.$$

2). $m=8$ – moduli bo`yicha chegirmalarning izlanayotgan to`lasi sistemalari: $1,2,3,4,\dots,8;$ $-8,-7,-6,-5,\dots,-2,-1;$ $\pm1;\ \pm2;\ \pm3;\ \pm4.$

$m=8$ – moduli bo`yicha chegirmalarning izlanayotgan keltirilgan sistemalari:

$$1,3,5,7;\ -1,-3,-5,-7;\quad \pm1;\ \pm3.$$

3). $p=13$ – moduli bo`yicha chegirmalarning izlanayotgan to`la sistemalari: $1,2,3,4,\dots,13;$ $-13,-12,-11,\dots,-2,-1;$ $0,\ \pm1,\ \pm2,\ \pm3,\ \pm4,\ \pm5,\ \pm6.$

$p=13$ - moduli bo`yicha chegirmalarning izlanayotgan keltirilgan sistemalari: $1,2,3,4,\dots,12;$ $-12,-11,\dots,-2,-1;$ $\pm1,\ \pm2,\ \pm3,\ \pm4,\ \pm5,\ \pm6.$ 4). $m=12$ – moduli bo`yicha chegirmalarning izlanayotgan to`la sistemalari: $1,2,3,4,\dots,12;$ $-12,-11,-10,\dots,-2,-1;$ $\pm1,\ \pm2,\ \pm3,\ \pm4,\ \pm5,\ \pm6.$

$m=12$ – moduli bo`yicha chegirmalarning izlanayotgan keltirilgan sistemalar $1,5,7,11;$ $-1,-5,-7,-11;$ $\pm1;\ \pm5.$

5). $p=7$-moduli bo`yicha chegirmalarning izlanayotgan to`la sistemalari:

$$1,2,3,4,5,6,7;\quad -7,-6,-5,-4,-3,-2,-1;\quad 0,\pm1,\pm2,\pm3.$$

$p=7$ – moduli bo`yicha chegirmalarning izlanayotgan keltirilgan sistemalari:

$$1,2,3,4,5,6;\qquad -7\ -6,-5,-4,-3,-2,-1;\quad \pm1,\pm2,\pm3.$$

6). $m=10$ – moduli bo`yicha chegirmalarning izlanayotgan to`la sistemalari: $1,2,3,4,\dots,10;$ $-10,-9,-8,\dots,-2,-1;$ $\pm1,\ \pm2,\ \pm3,\ \pm4,\ \pm5,$

$m = 10$ – moduli do`yicha chegirmalarning izlanayotgan keltirilgan sistemalari:

$$1, 3, 7, 9; \quad -9, -7, -3, -1; \quad \pm 1,\ \pm 3.$$

197. $x = 10q + r, 0 \leq r < 10$ dan $x = 10q,$ $x = 10q + 1,$ $x = 10q + 2,$ $x = 10q + 3,$ $x = 10q + 4,$ $x = 10q + 5,$ $x = 10q + 6, x = 10q + 7, x = 10q + 8,$ $x = 10q + 9.$

198. *a)* $(10, x) = 1$ va $x \leq 10$ bo`lishi kerak. Ularning soni $\varphi(10) = 4$ ta va ular $x = 10q + 1, x = 10q + 3, x = 10q + 7,$ $x = 10q + 9,$ bularni taqqoslama ko`rinishida yozsak. $x \equiv 1(mod10), x \equiv 3(mod10), x \equiv 7(mod10),$ $x \equiv 9(mod10),$ yoki qisqacha yozsak $x \equiv 1, 3, 7, 9(mod10).$

b) $(10, x) = 2$ va $x \leq 10$ bo`lishi kerak, 3 – misoldan $x = 10q + 2,$ $x = 10q + 4,$ $x = 10q + 6,$ $x = 10q + 8,$ yoki bulardan $x \equiv 2, 4, 6, 8(mod10).$

c) $(10, x) = 5$ va $x \leq 10$ bo`lishi kerak, ya`na 3-misoldan $x = 10q + 5,$ ya`ni $x \equiv 5(mod10).$

d) $(10, x) = 10$ va $x \leq 10$ bo`lishi kerak, 3-misoldan $x = 10q,$ ya`ni $x \equiv 0(mod10).$

199. Buni isbotlash uchun quyidagi 2 ta holatni e'tiborga olish kifoya. Birinchidan *md* modul bo'yicha sinflar soni, *m* modul bo'yicha sinflar sonidan *d* marta ko'p. Ikkinchidan *m* modul bo'yicha taqqoslanmaydigan sonlar *md* modul bo'yicha ham taqqoslanmaydi.

200. Masalan:
$1, 2, 3, 4, 5, 6, 7, 8, 9, 10; -10, -9, -8, -7, -6, -5, -4, -3, -2, -1;$
$\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 5,$ umumiy holda $x = 10q + r, 0 \leq r < 10$ va $q \in Z.$

201. $\frac{Z}{10Z} = \{C_0,\ C_{1,} C_2, \dots, C_9\}$ to`plamlarni qarasak va bu to`plamda qo`shish hamda ko`paytirish amallarini (2) va (3) tengliklar yordamida aniqlash bu to`plam shu amallarga nisbatan yopiq ekanligini jadvallardan ko`rish qiyin emas.

+	C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9
C_1	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_0
C_2	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_0	C_1
C_3	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_0	C_1	C_2
C_4	C_4	C_5	C_6	C_7	C_8	C_9	C_0	C_1	C_2	C_3
C_5	C_5	C_6	C_7	C_8	C_9	C_0	C_1	C_2	C_3	C_4
C_6	C_6	C_7	C_8	C_9	C_0	C_1	C_2	C_3	C_4	C_5
C_7	C_7	C_8	C_9	C_0	C_1	C_2	C_3	C_4	C_5	C_6
C_8	C_8	C_9	C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7
C_9	C_9	C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8

$*$	C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9
C_0	C_0	C_0	C_0	C_0	C_0	C_0	C_0	C_0	C_0	C_0
C_1	C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9
C_2	C_0	C_2	C_4	C_6	C_8	C_0	C_2	C_4	C_6	C_8
C_3	C_0	C_3	C_6	C_9	C_2	C_5	C_8	C_1	C_4	C_7
C_4	C_0	C_4	C_8	C_2	C_6	C_0	C_4	C_8	C_2	C_6
C_5	C_0	C_5	C_0	C_5	C_0	C_5	C_0	C_5	C_0	C_5
C_6	C_0	C_6	C_2	C_8	C_4	C_0	C_6	C_2	C_8	C_4
C_7	C_0	C_7	C_4	$C_{1`}$	C_8	C_5	C_2	C_9	C_6	C_3
C_8	C_0	C_8	C_6	C_4	C_2	C_0	C_8	C_6	C_4	C_2
C_9	C_0	C_9	C_8	C_7	C_6	C_5	C_4	C_3	C_2	C_1

$\langle\frac{z}{10\,z};\ +;\cdot\rangle$ ning halqa bo`lishi uchun additiv Abel gruppasi, multipikativ yarim gruppa va distributuvlik sharti $(C_i + C_s)C_j = C_iC_j + C_sC_j$ bajarilishi kerak.

Endi shu shartlarning bajarilishini tekshiramiz.

I. Additiv Abel gruppasi: a) $\forall C_i, C_{e,}C_s \in \frac{Z}{10Z}$ elementlar uchun $(C_i + C_e) + C_s = C_i + (C_e + C_s)$ - assotsiativlik sharti bajarilishi kerak. Bu yerda $C_i = (10q + i), C_e = (10q + e),\ C_s = (10q + s)$ bo`lgani uchun $(C_i + C_e) + C_s = C_{i+e} + C_s = C_{i+e+s}$ (yoki $C_{i+e-m+s-m} = C_{i+e+s-m}$). Shuningdek, $C_i + (C_e + C_s) = C_i + C_{e+s} = C_{i+e+s}$ (yoki $C_{i+e+s-2m}$ ). Bu tengliklarning o`ng tomonlari teng, demak chap tamonlari ham teng bo`lishi kerak. Bundan assotsiativlik shartining bajarilishi kelib chiqadi.

b) $\forall C_i \in \frac{Z}{10Z}$ uchun $\exists\ C_0 \in \frac{Z}{10Z}$ bo`lib, $C_i + C_0 = C_0 + C_i = C_i$ bajariladi, ya`ni qaralayotgan to`plamda nol element mavjud.

c) $\forall C_i \in \frac{Z}{10Z}$ uchun $\exists\ C_{10-i} \in \frac{Z}{10Z}$ bo`lib, $C_i + C_{10-i} = C_{10-i} = C_{10} = C_0$ bajariladi, ya`ni qaralayotgan to`plamda $\forall\ C_i$ ga qarama-qarshi element C_{10-i} mavjud.

d) $\forall C_i \in \frac{Z}{10Z}$ uchun $C_i + C_j = C_j + C_i = C_{i+j}$ (yoki C_{i+j-m}) bajariladi.

Shunday qilib qaralayotgan to`plam qo`shishga nisbatan additiv Abel gruppasi bo`lar ekan.

II. $< \frac{Z}{10Z};\cdot>$ ning multiplikativ yarim gruppa bo`lishini tekshiramiz:

$\forall\ C_i, C_j, C_e\ \in \frac{Z}{10Z}$ uchun $C_i(C_j \cdot C_e) = (C_i \cdot C_j)C_e$ ning bajarilishini ko`rsatish yetarli tenglikning chap tomoni $C_i(C_j \cdot C_e) = C_i \cdot C_{je} = C_{ije} = C_r$, bunda $ije =$

$10q + r$. O’ng tomoni $(C_i \cdot C_j)C_e = C_{ij} \cdot C_e = C_{ije} = C_r$. Bulardan isbotlanishi kerak bo`lgan tenglik kelib chiqadi.

III. Distributivlik sharti $\forall C_i, C_j, C_e \in \frac{Z}{mZ}$ lar uchun $(C_i + C_j)C_e = C_iC_e + C_jC_e$ tenglikning bajarilishini tekshiramiz. Bu tenglik chap tomoni (soddalik uchun $i + j + l < m$ deb qaraymiz; $i + j + l > m$ holi ham shunga o`xshash qaraladi). $(C_i + C_j)C_e = C_{i+j} \cdot C_e = C_{(i+j)e}$. O`ng tomoni $C_i \cdot C_e + C_jC_e = C_{ie} + C_{je} = C_{ij+je} = C_{(i+j)e}$ demak, bu tenglikning chap tomonlari teng, o`ng tamonlari ham teng bo`lishi kerak. Bundan ega isbotlanish talab etilgan tenglik kelib chiqadi. Shunday qilib $\langle\frac{Z}{10Z};\ +;*\rangle$ sistema halqa bo`lar ekan.

202. m moduli bo`yicha chegirmalarning to`la sistemasida m ta chegirma bo`lib, ular shu modul bo`yicha o`zaro taqqoslanmaydigan bo`lishi kerak. Bizga 5 ta son $20, -4, 22, 18, -1$, berilgan. Demak, m =5 deb olib, berilgan sonlarning 5 moduli bo`yicha o`zaro taqqoslanuvchi emas ekanligini ko`rsatamiz. Buning uchun berilgan sonlarni manfiy bo`lmagan eng kichik chermalar ko`rinishiga keltirib olamiz. U holda $0, 1, 2, 3, 4$ larga ega bo`lamiz. Bular $m = 5$ moduli bo`yicha o`zaro taqqoslanmaydi. $J{:}\, m = 5$.

203. Berilgan $20, 31, -8, -5, 25, 14, 8, -1, 13$ va 6 sonlarning soni 10 bo`lib, ularni eng kichik musbat chegirmalar ko`rinishida yozsak: $0, 1, 2, 5, 5, 4, 8, 9, 3, 6$ hosil bo’ladi. Bunda -5 va 25 lar $m = 10$ moduli boyicha o`zaro taqqoslanuvchi, ya`ni ular bitta sinifga tegishli. Shuning uchun ham berilgan sonlar $m = 10$ moduli bo`yicha chegirmalarning to`la sistemasini tashkil etmaydi.

204. Istalgan m ta ketma-ket kelgan $x + b$, $x = 0, 1, 2, \dots, m - 1$ sonlarni qaraymiz. Bu yerda $(m, 1) = 1$ va 1-teoremani ($a = 1$ deb) qo`llasak $x + b, x = 0, 1, 2, \dots, m - 1$ sonlarni $m$ moduli bo`yicha chegirmalarning to`la sistemasini hosil qiladi degan xulosaga kelamiz.

205. Berilgan sonlarning soni m ta bo`lib, ular $m$ moduli bo`yicha o`zaro taqqoslanmaydi. Agar $-\frac{m-i}{2} \equiv \frac{m-j}{2}(mod m)$ desak $(1 \le i, j < m$

$-\frac{m-i}{2} - \frac{m-j}{2} \equiv 0(mod m) \Rightarrow \frac{-2m+j+i}{2} \equiv 0(mod m)$ yoki $\frac{j+i}{2} \equiv 0(mod m) \Rightarrow j \equiv -i(mod) \Rightarrow j = -i + mt$. U holda $\frac{-m+i}{2} \equiv \frac{m+i-mt}{2}(mod) \Rightarrow \frac{i}{2} \equiv \frac{i}{2}(mod m)$, ya`ni $-\frac{m-i}{2}$ va $\frac{m-j}{2}$ chegirmalar bitta sinfdan olingan. Demak, $-\frac{m-i}{2} \not\equiv \frac{m-j}{2}(mod m)$ va berilgan sonlar $m$ moduli bo`yicha chegirmalarining to`la sistemasini tashkil etadi.

206. $(10, 3) = 1$ bo`lgani uchun 1- teoremaga ko`ra agar x o`zgaruvchi $m = 10$ moduli bo`yicha chegirmalarning to`la sistemasini qabul qilsa, $3x - 1$ ham shu sistemani qabul qiladi, ya`ni

x	0	1	2	3	4	5	6	7	8	9
$3x-1$	9	2	5	8	1	4	7	0	3	6

Bu yerda $3x-1$ning qiymatlarini 10 moduli bo`yicha manfiy bo`lmagan eng kichik chegirma ko`rinishida yozdik.

207. 4 modul chegirmalarning to'la sistemasida 4 ta 4 moduli bo'yicha o'zaro taqqoslanmaydigan chegirma bo'lishi kerak. Bizga ma'lumki, agar (a,m)=1 bo'lib x o'zgaruvchi m moduli bo'yicha chegirmalarning keltirilgan sistemasini qabul qilsa, $ax+b$ ham shu sistemami qabul qiladi. Bizning misolimizda $a=5$, $b=0$, $m=4$ va $(5,4)$=1. Shuning uchun ham x ga x=0, 1, 2, 3 qiymatlar bersak $5x$= 0, 5, 10,15 lar hosil bo'ladi. Bularni manfiy bo'lmagan eng kichik chegirmalar ko'rinishida yozib olsak, 0, 1, 2, 3 izlanayotgan sistema hosil bo'ladi.

208. $ax_i+b\ (i=1,2,\dots,m)$ ko`rinishidagi sonlar $m$ moduli bo`yicha chegirmalarning to`la sistemasini tashkil qilsa, ularning soni $m$ ta bo`lib m moduli bo`yicha o`zaro taqqoslanmasligi kerak.

U holda $x_i(i=1,2,\dots,m)$ lar qiymatlari ham m ta bo`lib, ular ham $m$ moduli bo`yicha o`zaro taqqoslanmaydigan bo`ladilar. Haqiqatan ham, agar $x_l\equiv x_r(modm)$ desak, $(a,m)=1$ sonini tanlab olib taqqoslamaning ikkala tamonini a ga ko`paytiramiz, u holda $ax_l\equiv ax_r(modm)$ bo`ladi. Bu taqqoslamaga $b\equiv b(modm)$ ayniy taqqoslamani hadlab qo`shsak, $ax_l+b\equiv ax_r+b(modm)$ hosil bo`ladi. Masalaning shartiga ko`ra bunday bo`lishi mumkin emas. Bu qarama-qarshilik $x_l\equiv x_r(modm)$ deganimizdan kelib chiqdi va demak, $x_l\not\equiv x_r(modm)$. Shuning uchun ham qaralayotgan sonlar $x_i(i=1,2,\dots,m)m$ moduli bo`yicha chegirmalarning to`la sistemasini tashkil etadi.

209. $f(x_i)=a_nx_i^n+a_{n-1}x_i^{n-1}+\dots+a_1x_i+a_0,(i=1,2,\dots,m)$,

$(a_i,m)=1$ ko`rinishidagi sonlar $m$ moduli bo`yicha chegirmalarning to`la sistemasini tashkil qilsa, demak ularning soni $m$ ta va $f(x_i)\not\equiv f(x_j)$(mod$m$) bajariladi. Bu holda $x_i(i=1,2,\dots,m)$ larning soni ham $m$ ta bo`ladi va ular $m$moduli bo`yicha o`zaro taqqoslanmaydigan bo`ladi. Haqiqatan ham, agar $x_s\equiv x_k(modm)$ desak, $x_s^2\equiv x_k^2(modm)$, … ,$x_s^{n-1}\equiv x_k^{n-1}(modm),x_s^n\equiv x_k^n(modm),a_0\equiv a_0(modm)$ lar bajariladi. Bu taqqoslamalarning ikkala tomonini mos ravishda $a_1,a_2,\dots,a_{n-1},a_n$ larga ko`paytirib keyin qo`shsak, $f(x_s)\equiv f(x_k)(modm)$ ga ega bo`lamiz. Lekin masalaning shartiga ko`ra $f(x_s)\not\equiv f(x_k)(modm)$. Bu qarama-qarshilik $x_i(i=1,2,\dots,m)$ lar ichida o`zaro taqqoslanuvchilar yo`q ekanligini bildiradi va demak, ular $m$ moduli bo`yicha chegirmalarning to`la sistemasini tashkil qiladi. Aksincha, tasdiq ham shunga o'xshash isbotlanadi.

210. m moduli bo`yicha chegirmalar keltirilgan sistemasida $\varphi(m)$ta chegirma bo`lib, ularning har biri m moduli bilano`zaro tub bo`lishi kerak. Masalada $m = 6$, $\varphi(6) = \varphi(2) \cdot \varphi(3) = (2-1)(3-1) = 2$. $x \leq 6$ va $(x;\ 6) = 1$ shartlarni qanoatlantiruvchi sonlarni yozib olish kifoya: $1, 5$; $-5, 5$; $-5, -1$; $7, 11$; $13, 17$.

211. Qulaylik uchun berilgan chegirmalarni eng kichik musbat chegirmalar ko`rinishida yozib olamiz. U holda $7, 1, 11, 3, 5$ va $\varphi(12) = \varphi(2^2 \cdot 3) = \varphi(2^2) \cdot \varphi(3) = (2^2 - 2)(3-1) = 4$ bo`lgani uchun 12 modulli bo`yicha chegirmalarning keltirilgan sistemasida 4ta chegirma bo`lish kerak va ularning har biri 12 bilan o`zaro tub bo`lishi kerak. Bizda 5 ta chegirma bor, lekin$(3, 12) = 3$. Shuning uchun ham berilgan sonlar sistemasi 12 moduli bo`yicha chegirmalarning keltirilgan sistemasini tashkil etmaydi.

212. p modul bo`yicha chegirmalarning to`la sistemasi sifatida $1, 2, 3, \ldots$, $p-1$, p larni olish mumkun. Bularning ichidan p bilan o`zaro tublarini ajratib olsak: $1, 2, 3, \ldots, p-1$ chegirmalarning keltirilgan sistemasi hosil bo`ladi. Bu sistemadagi chegirmalar soni $p-1$ ta.

213. Berilgan chegirmalar soni $\varphi(p) = p - 1$ ta va ularning ham biri p bilan o`zaro tub, ya`ni $\left(\frac{p-i}{2};\ p\right) = 1$, bunda $p > 2$ tub son, $i = 2k + 1$ toq son $\frac{p-i}{2} < p$ va demak $\frac{p-i}{2}$ soni p tub soniga bo`linmaydi. Qaralayotgan chegirmalarning $p$ moduli bo`yicha har xil sinflarga tegishli ekanligi 212-masalada isbotlangan edi. Demak qaralayotgan sonlar sistemasi $p > 2$ moduli bo`yicha chegirmalarning keltirilgan sistemasini tashkil etadi.

214. Qaralayotgan sistemada $\varphi(7) = 7 - 1 = 6$ ta son bor. Ularning har biri 7 bilan o`zaro tub, chunki $(5;\ 7) = 1$. Ular turli sinflarga tegishli, chunki $5^i \equiv 5^j (\mathrm{mod} 7)$ $(0 < j \leq i \leq 6)$ dan $5^{i-j} \equiv 1 (\mathrm{mod} 7)$, bundan $i = j$ kelib chiqadi. Demak, chegirmalarning keltirilgan sistemasining ta`rifiga asosan berilgan sonlar sistemasi 7 modul bo`yicha chegirmalarning keltirilgan sistemasini tashkil etadi.

215. $ax_i, (i = 1,2, \ldots \varphi(m))$ sonlarni m moduli bo'yicha chegirmalarning keltirilgan sistemasini tashkil etsa, ularning soni $\varphi(m)$ ta bo'lib $(ax_i; m) = 1$ va $ax_1 \not\equiv ax_s\ (modm)$ bo'lishi kerak. Bundan $(a; m) = 1$ va$(x_i; m) = 1$ kelib chiqadi. Bizda $x_i\ (i = 1,2, \ldots \varphi(m))$ larning soni $\varphi(m)$ ta va $(x_i; m) = 1$ $x_s \not\equiv x_k\ (modm)$ ekanligini ko'rsatamiz. Faraz etaylik, $x_s \equiv x_k\ (modm)$ bo'lsin, u holda bu taqqoslamaning ikkala tomoni $a, (a, m) = 1$ soni ko'paytiramiz. U holda $ax_s \equiv ax_k\ (modm)$ taqqoslamaga ega bo'lamiz. Masalaning sharti bo'yicha $ax_s \not\equiv ax_k (modm)$. Bu qarama–qarshilik $x_s \equiv x_k\ (modm)$ bo'lsin degan farazimizdan kelib chiqdi. Demak, $x_s \not\equiv x_k\ (modm)$ ekan. Shunday qilib, agar $ax_i\ (i = 1,2, \ldots \varphi(m))$ sonlari m modul bo'yicha chegirmalarning keltirilgan sistemasini tashkil qilsa, x_i $(i = 1,2, \dots \varphi(m))$ sonlari ham m moduli bo'yicha chegirmalarning keltirilgan sistemasini tashkil qilar ekan.

216. x o'zgaruvchining qiymatlari $x_1, x_2, \dots, x_{\varphi(m)}$ (bunda $(x_i, m) = 1$ va $x_i \not\equiv x_j(modm)$) lar m modul bo'yicha chegirmalar-ning keltirilgan sistemasini tashkil etgani uchun bu qiymatlarni $ax + b$ ga qo'yib $\varphi(m)$ ta $ax_1 + b$, $ax_2 + b$, ... , $ax_{\varphi(m)} + b$ songa ega bo'lamiz.

Endi ularning har xil sinflarga tegishli ekanligini va m modul bilan o'zaro tub ekanligini ko'rsatamiz. Agar $ax_i + b \equiv ax_j + b(modm)$ desak, bu taqqoslamalarning xossalariga ko'ra $ax_i \equiv ax_j(modm)$ ga teng kuchli. Buning ikkala tomonini $a, (a, m) = 1$ soniga qisqartirsak, $x_i \equiv x_j(modm)$ ga ega bo'lamiz. Bu esa $x_i \not\equiv x_j(modm)$shartga ziddir. Demak, qaralayotgan sonlar m moduli bo'yicha har xil sinflarga tegishli ekan. $(ax_i + b,\ m) = d > 1$ desak, $ax_i + b \equiv 0(modd)$ va $m \equiv 0(modd)$ ga ega bo'lamiz. $b = m \cdot b_1$ va $m \equiv d \cdot m_1$ bo'lgani uchun $b = d \cdot (m_1 \cdot b_1)$ bo'ladi, ya'ni b soni d ga bo'linadi. U holda $ax_i + b \equiv 0(modd)$ dan $ax_i \equiv 0(modd)$ ni hosil qilamiz. $(a, m) = 1$ dan $(a, d) = 1$ ekanligi kelib chiqadi. Shuning uchun $ax_i \equiv 0(modd)$ dan $x_i \equiv 0(modd)$ bajarilishi kerak degan xulosa kelib chiqadi. Bunday bo'lishi mumkin emas, chunki $(x_i, m) = 1$ va demak, $(x_i, d) = 1$. Bu yerdan $\varphi(m)$ta $ax_1 + b,\ ax_2 + b$, ... , $ax_{\varphi(m)} + b$ larning har xil sinflarga tegishli ekanligi kelib chiqadi.

217. $(a; m) = d$ shart $\left(\frac{a}{d}; \frac{m}{d}\right) = 1$ ga teng kuchli. Shuning uchun ham a ning o'rniga $\frac{a}{d}$ va m ning o'rniga $\frac{m}{d}$ ni olib 1- teoremani qo'llaymiz. U holda 1-teoremadan – agar x o$'$zgaruvchi $\frac{m}{d}$ moduli bo'yicha chegirmalarning to'la sistemasini qabul qilsa, $\frac{a}{d}x + b$ ham $\frac{m}{d}$ moduli bo'yicha chegirmalarning to'la sistemasini qabul qiladi degan tasdiq kelib chiqadi.

218. $(a; m) = d$ shartdan $\left(\frac{a}{d}; \frac{m}{d}\right) = 1$ shart kelib chiqadi. Shuning uchun ham a ni $\frac{a}{d}$ bilan, m ni $\frac{m}{d}$ bilan almashtirib, 2 – teoremani qo'llaymiz. U holda 2-teoremadan – "agar x o'zgaruvchi $\frac{m}{d}$ moduli bo'yicha chegirmalarning keltirilgan sistemasini qabul qilsa, u holda ax ham $\frac{m}{d}$ moduli bo'yicha chegirmalarning keltirlgan sistemasini qabul qiladi" – degan tasdiqqa ega bo'lamiz.

219. m=9 moduli bo'yicha chegirmalarning to'la sistemasida 9 ta son bo'lib ular o'zaro taqqoslanmaydigan bo'lishi kerak. Shuning uchun ham:

$1, 2, 3, 4, 5, 6, 7, 8, 9-$lar m=9 moduli boyicha musbat eng kichik chegirmalarning to'la sistemasi;

$0, 1, 2, 3, 4, 5, 6, 7, 8-$ lar m=9 moduli boyicha manfiy bo'lmagan eng kichik chegirmalarning to'la sistemasi;

$0, \pm 1, \pm 2, \pm 3, \pm 4-$ lar m=9 moduli bo`yicha absolyut qiymati jihatidan eng kichik chegirmalarning to'la sistemasi bo'ldi.

Endi m=9 moduli bo'yicha chegirmalarning keltirilgan sistemalarini 3 xil (musbat, manfiy bo'lmagan, absolyut qyimati jihatidan eng kichik chegirmalar) ko'rinishda yozish uchun to'la sistemalardagi chegirmalarning m bilan o'zaro tublarini ajratib olish kifoya, ya'ni ularning har birida φ(9)=6 ta chegirma bo'ladi. Shuning uchun ham:

$1, 2, 4, 5, 7, 8$ $-$ lar m=9 moduli boyicha musbat eng kichik chegirmalarning keltirilgan sistemasi;

$1, 2, 4, 5, 7, 8 -$ lar m=9 moduli boyicha manfiy bo'lmagan eng kichik chegirmalarning keltirilgan sistemasi;

$\pm 1, \pm 2, \pm 4-$ lar m=9 moduli boyicha absolyut qiymati jihatidan eng kichik chegirmalarning keltirilgan sistemasi bo'ladi.

Shuni ham ta'kidlash kerakki, bu misolda m=9 moduli boyicha musbat eng kichik chegirmalarning va manfiy bo'lmagan eng kichik chegirmalarning keltirilgan sistemalari bir xil bo'lar ekan.

III.3-§.

220. a) $(a, 7) = 1$ bo'lganligi uchun Ferma teoremasiga ko'ra $a^6 \equiv 1(mod 7)$ bajariladi. Bundan $a^{12} \equiv 1(mod 7)$, ya'ni $(a^{12} - 1) \vdots 7$.

b) $(a, 65) = 1$ dan $(a; 5 \cdot 13) = (a; 5) = (a; 13) = 1$ kelib chiqadi. Demak, Ferma teoremasiga asosan $a^{12} \equiv 1(mod 13)$ va $a^4 \equiv 1(mod 5)$. Oxirgi taqqoslamaning ikkala tomonini kubga ko'tarsak $a^{12} \equiv 1(mod 5)$ hosil bo'ladi. $a^{12} \equiv 1(mod 5)$ va $a^{12} \equiv 1(mod 13)$, hamda $(5; 13) = 1$ dan $a^{12} \equiv 1(mod 65)$ kelib chiqadi. $(b; 65) = 1$ bo'lganligi uchun yuqoridagidek mulohaza yuritib, $b^{12} \equiv 1(mod 65)$ ni hosil qilamiz. $a^{12} \equiv 1(mod 65)$ va $b^{12} \equiv 1(mod 65)$ taqqoslamalardan $a^{12} - b^{12} \equiv 0(mod 65)$ ga ega bo'lamiz. Bu esa $a^{12} - b^{12} \vdots$ 65 ga teng kuchli.

221. Kanonik yoyilmasiga 2 va 5 sonlari kirmaydigan natural sonni $x$desak $(x, 10) = 1$ va $\varphi(10) = 4$ bo'lgani uchun Eyler teoremasiga ko'ra $x^4 \equiv 1(mod 10)$. Shuning uchun ham $x^{12} \equiv (x^4)^3 \equiv 1(mod 10)$. Demak, kanonik yoyilmasiga 2 va 5 sonlari kirmaydigan natural sonning $12 -$darajasining birlik raqami 1ga teng ekan.

222. $a \not\equiv 0(modp)$ bo'lgani uchun $(a; p) = 1$ deb yozish mumkin. U holda, Ferma teoremasiga ko'ra $a^{p-1} \equiv 1(modp)$ bajariladi. Bundan $a^{p-1} - 1 \equiv 0(modp)$. Bu taqqoslamaning chap tomoniga p ni qo'shsak, (taqqoslamaning istalgan tomoniga yoki ikkala tomoniga modulga karrali bo'lgan sonni qo'shish va ayirish mumkin) $a^{p-1}+p-1\equiv 0(modp)$ hosil bo'ladi. Bundan $(a^{p-1}+p-1)\vdots p$, ya'ni $a^{p-1}+p-1$ soni murakkab son.

223. Ferma teoremasiga asosan $2^{11-1}\equiv 1(mod11)$, $2^{30}\equiv 1(mod31)$ yoki $2^{11}\equiv 2(mod11)$, $2^{31}\equiv 2(mod31)$. Birinchi taqqoslamadan $(2^{11})^{31}\equiv 2^{31}(mod11)\equiv 2\cdot(2^6)^5(mod11)\equiv 2\cdot(-2)^5(mod11)\equiv 2\cdot(-32)(mod11)\equiv 2(mod11)$. Shunga o'xshash $(2^{31})^{11}\equiv 2^{11}(mod31)\equiv 2\cdot(2^5)^2(mod31)\equiv 2(mod11)$. Shunday qilib, $2^{11\cdot 31}\equiv 2(mod11)$ va $2^{31\cdot 11}\equiv 2(mod31)$ hamda $(11;31)=1$ bo'lgani uchun $2^{11\cdot 31}\equiv 2(mod11\cdot 31)$.

224. Ferma teoremasiga ko'ra $2^{12}\equiv 1(mod\ 13)$. Shuning uchun $2^{24}\equiv 1(mod\ 13)$. Bundan tashqari $2^6\equiv 64\equiv -1(mod\ 13)$ ekanligidan $2^{30}\equiv -1\equiv 12(mod\ 13)$ bo'ladi. Demak, izlangan qoldiq 12 ga teng.

225. $3^{16}\equiv 1(mod17)$ bo'lganligi uchun $3^{59}\equiv 3^{11}\cdot(3^{16})^3\equiv 3^{11}(mod17)\equiv (3^3)^3\cdot 3^2(mod17)\equiv 10^3\cdot 9(mod17)\equiv 1000\cdot 9(mod17)\equiv 14\cdot 9(mod17)\equiv 126(mod17)\equiv 7(mod17)$. Demak 3^{59} ni 17 ga bo'lsak, 7 qoldiq qoladi.

226. Ferma teoremasiga asosan $a^{p-1}\equiv 1(modp)$, $(a;p)=1$. Bu taqqoslamaning ikkala tomonini n-darajaga ko'taramiz. U holda $a^{n(p-1)}\equiv 1(modp)$ hosil bo'ladi. Bundan va $a\equiv a(modp)$ dan $a^{n(p-1)+1}\equiv a(modp)$ kelib chiqadi. Keyingi taqqoslama $a\vdots p$ bo'lsa ham o'rinli. Shunday qilib ixtiyoriy a butun, n-natural va p tub sonlar uchun $a^{n(p-1)+1}\equiv a(modp)$ taqqoslama o'rinli.

227. 317 ni 15 ga bo'lgandagi qoldiq 2 ga teng bo'lgani uchun, ya'ni $317\equiv 2(mod15)$ ekanligidan $317^{259}\equiv 2^{259}(mod\ 15)$ bo'lishini topamiz. Eyler teoremasiga ko'ra $2^{\varphi(15)}\equiv 1(mod15)$va $\varphi(15)=\varphi(3\cdot 5)=\varphi(3)\cdot\varphi(5)=2\cdot 4=8$ bo'lgani uchun $2^8\equiv 1(mod15)$. $259=32\cdot 8+3$ ekanligidan $2^{259}=(2^8)^{32}\cdot 2^3\equiv 8(mod15)$≡8(mod15) bo'ladi. Demak 317^{259} sonini 15 ga bo'lgandagi qoldiq 8 ga teng ekan.

228. Bu yerda$(3,11)=1$. Shuning uchun ham Eyler teoremasiga ko'ra $3^{\varphi(11)}\equiv 1(mod11).\varphi(11)=11-1=10$ bo'lganligi sababli $3^{10}\equiv 1(mod11)$ bo'ladi. Bundan

$$3^{80}=(3^{10})^8\equiv 1^8\equiv 1(mod11). \quad (1)$$

Shunga o'xshash $(7,11)=1$ va Eyler teoremasiga ko'ra $7^{\varphi(11)}\equiv 1(mod11)$ bo'lganligi sababli $7^{10}\equiv 1(mod11)$ bo'ladi. Bundan

$$7^{80}=(7^{10})^8\equiv 1^8\equiv 1(mod11). \quad (2)$$

(1) va (2) taqqoslamalarni hadlab qo'shib

$$3^{80}+7^{80}\equiv 2(mod11)$$

ni hosil qilamiz. Demak, $3^{80}+7^{80}$sonini 11 ga bo'lgandagi qoldiq 2 ga teng ekan.

229. Avvalo 3^{100} ni 7 ga bo'lgandagi qoldiqni topamiz. $(3;7)=1$ bo'lganligi uchun Ferma teoremasidan $3^6\equiv 1(mod\ 7)$ kelib chiqadi. Shuning uchun ham

$$3^{100} \equiv (3^6)^{16} \cdot 3^4 (mod\ 7) \equiv 3^4 (mod\ 7) \equiv 4 (mod\ 7). \qquad (1)$$

Endi 4^{100} ni 7 ga bo'lgandagi qoldiqni aniqlaymiz. Bu yerda $(4;7) = 1$ va $4^6 \equiv 1(mod\ 7)$. Shuning uchun

$$4^{100} \equiv (4^6)^{16} \cdot 4^4 (mod7) \equiv 4^2 \cdot 4^2 (mod7) \equiv 9 \cdot 9 (mod7) \equiv 4(mod7) \quad (2)$$

(1) va (2) taqqoslamalardan $4^{100} + 3^{100} \equiv 1(mod7)$ hosil bo'ladi.

Demak, $4^{100} + 3^{100}$ ni 7 ga bo'lsak 1 qoldiq qoladi.

Izoh. $4^{100} + 3^{100} \equiv 3^{100} + (-3)^{100}(mod7) \equiv 2 \cdot 3^{100}(mod7)$ dan foydalanib ham shu natijani olish mumkin.

230. $197 = 35 \cdot 5 + 22$ bo'lganligi uchun $197^{157} \equiv (35 \cdot 5 + 22)^{157} \equiv 22^{157}(mod35)$. Bu yerda $(22;35) = 1$ va Eyler teoremasiga asosan $22^{\varphi(35)} \equiv 1(mod35)$ yoki $22^{24} \equiv 1(mod35)$. Bundan $22^{157} \equiv (22^{24})^6 \cdot 22^{13}(mod35)$ $\equiv 22^{13}(mod35) \equiv (22^2)^6 \cdot 22^1(mod35) \equiv (-6)^6 \cdot 22(mod35) \equiv ((-6)^2)^3 \cdot 22(mod35) \equiv 22(mod35)$. Shunday qilib 197^{157} ni 35 ga bo'lgandagi qoldiq 22 chiqar ekan.

231. $2^{72} \equiv 1(mod73)$ va $2^{36} \equiv 1(mod37)$. Bulardan

$2^{73} \equiv 2(mod73)$ va $2^{37} \equiv 2(mod37)$. Bu yerdagi birinchi taqqoslamaga asosan $(2^{73})^{37} \equiv 2^{37}(mod73) \equiv (2^6)^6 \cdot 2(mod73) \equiv (-9)^6 \cdot 2(mod73) \equiv ((-9)^2)^3 \cdot 2(mod73) \equiv 8^3 \cdot 2(mod73) \equiv 1024(mod73) \equiv 2(mod73)$, ya'ni

$$(2^{73})^{37} \equiv 2(mod73). \qquad (3)$$

Endi $2^{73} \equiv 2(mod37)$ taqqoslamadan $(2^{37})^{73} \equiv 2^{73}(mod37) \equiv (2^{36})^2 \cdot 2(mod37)) \equiv 2(mod37)$, ya'ni

$$(2^{37})^{73} \equiv 2(mod73). \qquad (4)$$

(3) va (4) taqqoslamalardan $(2^{37})^{73} \equiv 2(mod37 \cdot 73)$ yoki bundan $2^{n-1} \equiv 1(modn)$, bu yerda $n = 37 \cdot 73$.

232. $1^{30} \equiv 1(mod11), 2^{30} \equiv (2^{10})^3 \equiv 1(mod11), \ \ldots\ , \ 10^{30} \equiv 1(mod11)$. Bu yerda $i = 1,2,3,\ldots.10$ bo'lsa, $i^{10} \equiv 1(mod11)$ ekanligidan foydalandik. Bundan $1^{30} + 2^{30} + \cdots + 10^{30} \equiv 10(mod11) \equiv -1(mod11)$ kelib chiqadi.

233. a) $x^7 \equiv x(mod42)$ dan $x^7 \equiv x(mod2 \cdot 3 \cdot 7)$. Demak, biz $x^7 \equiv x(mod7)$, $x^7 \equiv x(mod3)$ va $x^7 \equiv x(mod2)$ taqqoslamalarning ixtiyoriy x butun soni uchun o'rinli ekanligini ko'rsatishimiz kerak. Birinchi taqqoslama Ferma teoremasidan bevosita kelib chiqadi. 2- va 3- larni bevosita chegirmalarning to'la sistemasini tekshirib ko'rish bilan ishonch hosil qilamiz. 2 moduli bo'yicha chegirmalarning to'la sistemasi 0 va 1 dan iborat va bularning ikkalasi ham $x^7 \equiv x(mod2)$ taqqoslamani qanoatlantiradi. 3 moduli bo'yicha chegirmalarning to'la sistemasi $0,1,2$ dan iborat va bularning uchalasi ham $x^7 \equiv x(mod3)$ taqqoslamani qanoatlantiradi.

b) $x^{13} \equiv x(mod2730)$ dan $x^{13} \equiv x(mod\ 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13)$. Bu yerdan $x^{13} \equiv x(mod13)$, (Ferma teoremasiga ko'ra); $x^{13} \equiv x(mod2)$ (0,1 ni qo'yib tekshirsak); $x^3 \equiv x(mod3)$ dan $x^{13} \equiv (x^3)^4 \cdot x \equiv x^5 \equiv x^3 \cdot x^2(mod3) \equiv x^3(mod3) \equiv$

$x(mod3)$. $x^{13} \equiv x(mod5)$ va $x^{13} \equiv x(mod7)$ lar ham shunga o'xshash isbotlanadi. Endi hosil bo'lgan $x^{13} \equiv x(mod2)$, $x^{13} \equiv x(mod3)$, $x^{13} \equiv x(mod5)$, $x^{13} \equiv x(mod7)$ va $x^{13} \equiv x(mod13)$ taqqoslamalarning ixtiyoriy x butun son uchun o'rinli ekanligidan $x^{13} \equiv x(mod\ 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13)$ ning, yoki bundan $x^{13} \equiv x(mod2730)$ ning o'rinli ekanligi kelib chiqadi.

234. p va q lar $(p;q) = 1$ shartni qanoatlantiruvchi tub sonlar bo'lgani uchun $p^{q-1} \equiv 1(modq)$ va $q^{p-1} \equiv 1(modp)$. Bu taqqoslamalarni tenglik qilib yozsak, $p^{q-1} - 1 = qt,\ q^{p-1} - 1 = pl, t, l\epsilon\ Z$. Bulardan

$(p^{q-1} - 1)(q^{p-1} - 1) = pqtl$ yoki $p^{q-1} \cdot q^{p-1} - p^{q-1} - q^{p-1} + 1 = pqtl$.
Endi taqqoslama qilib yozsak, $q^{p-1} + p^{q-1} - p^{q-1} \cdot q^{p-1} - 1 \equiv 0(modpq)$.
Bundan $q^{p+1} + p^{q+1} \equiv 1(modpq)$ kelib chiqadi.

235. 2^{100} sonining oxirgi ikkita raqamini topish uchun uni 100 ga bo'lishdan chiqqan qoldiqni topish kifoya. Bu yerda $100 = 25 \cdot 4$ va Eyler teoremasiga ko'ra $2^{\varphi(25)} \equiv 1(mod25)$, ya'ni $2^{20} \equiv 1(mod25)$ hamda $2^{100} = 2^{98} \cdot 2^2$ bo'lgani uchun $2^{98} \equiv 2^{80} \cdot 2^{18}(mod25) \equiv 2^{18}(mod25) \equiv (2^9)^2(mod25) \equiv 144(mod25) \equiv 19(mod25)$. Buni tenglik qilib yozsak, $2^{98} = 19 + 25t$. Bu tenglikni ikkala tomonini 4 ga ko'paytirib, taqqoslama ko'rinishida yozamiz. U holda $2^{100} = 76 + 100t$ yoki $2^{100} \equiv 76(mod\ 100)$. Demak, 2^{100} ning oxirgi raqami ikkita raqam 7 va 6.

236. Berilgan sonning oxirgi raqamini topish uchun uni 10 ga bo'lishdan chiqqan qoldiqni topish kifoya. $(3{,}10) = 1$va Eyler teoremasiga ko'ra $3^{\varphi(10)} \equiv 1(mod11)$. Bunda $\varphi(10) = \varphi(2 \cdot 5) = \varphi(2) \cdot \varphi(5) = (2-1) \cdot (5-1) = 4$ bo'lganligi sababli $3^4 \equiv 1(mod10)$ bo'ladi. Shuning uchun ham $3^{100} = (3^4)^{25} \equiv 1^{25} \equiv 1(mod10)$. Demak, 3^{100} sonining oxirgi raqami 1 ga teng bo'lar ekan.

237. 243^{402} sonining oxirgi uchta raqamini topish uchun uni 1000 ga bo'lishdan chiqqan qoldiqni topish kerak bo'ladi. $243 = 3^5,\ 1000 = 10^3 = 5^3 \cdot 2^3$ bo'lgani uchun $(243; 1000) = 1$ va Eyler teoremasiga asosan $243^{\varphi(1000)} \equiv 1\ (mod1000)$ bajariladi. Bu yerda $\varphi(1000) = \varphi(2^3 \cdot 5^3) = \varphi(2^3) \cdot \varphi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = 4 \cdot 100 = 400$ bo'lgani uchun $243^{400} \equiv 1(mod1000)$. Shuning uchun ham $243^{402} \equiv 243^{400} \cdot 243^2 \equiv 243^2(mod1000)$

$\equiv 59049(mod1000) \equiv 49(mod1000)$. Demak, uchta raqami 0,4,9.

238. Shartga asosan $(n;6) = 1$. Bundan $(n;2) = 1$ va $(n;3) = 1$ bo'lgani uchun u toq son $n = 2k+1$, u holda $n^2 - 1 = (n-1)(n+1) = (2k+1-1)(2k+1+1) = 4k(k+1)$ ifoda 8 ga bo'linadi , ya'ni $n^2 - 1 = 0(mod8)$ yoki bundan

$$n^2 \equiv 1(mod8). \tag{5}$$

Ikkinchi tomondan $(n;3) = 1$ bo'lgani uchun Ferma teoremasiga asosan

$$n^2 \equiv 1(mod3). \tag{6}$$

Hamda $(8;3) = 1$ bo'lgani uchun (5) va (6) dan $n^2 \equiv 1(mod24)$ kelib chiqadi.

239. Ferma teoremasiga ko'ra : $1^{p-1} \equiv 1(modp)$, $2^{p-1} \equiv 1(modp)$, ... , $(p-1)^{p-1} \equiv 1(modp)$. Bunda p- tub son . Bu taqqoslamaning har birini $k\epsilon N$ darajaga ko'tarib keyin hadlab qo'shamiz . U holda

$$1^{k(p-1)} + 2^{k(p-1)} + \cdots + (p-1)^{k(p-1)} \equiv p-1(modp)$$

hosil bo'ladi. Bundan

$$1^{k(p-1)} + 2^{k(p-1)} + \cdots + (p-1)^{k(p-1)} + 1 \equiv 0(modp).$$

Buni qisqacha

$$\sum_{i=1}^{p-1} i^{k(p-1)} + 1 \equiv 0(modp)$$

ko'rinishda yozishimiz mumkin.

240. Ma'lumki, $a^p - a \equiv 0(modp)$. Shunga asosan $(a_1 + a_2 + \cdots + a_n)^p \equiv a_1 + a_2 + \cdots + a_n(modp)$. Bu yerda $a_1 \equiv a_1^p(modp)$, $a_2 \equiv a_2^p(modp)$,... $a_n \equiv a_n^p(modp)$ ekanligini e'tiborga olsak : $(a_1 + a_2 + \cdots + a_n)^p \equiv a_1^p + a_2^p + \cdots + a_n^p(modp)$ ga, ya'ni isbotlanishi kerak bo'lgan taqqoslama $(\sum_{i=1}^{n} a_i)^p \equiv \sum_{i=1}^{n} a_i{}^p$ (modp) ga ega bo'lamiz.

241. Eyler teoremasiga asosan $(a;m) = 1$ bo'lsa , $a^{\varphi(m)} \equiv 1(modm)$ bo'ladi. Endi faraz etaylik x soni $a^x \equiv 1(modm)$ taqqoslamaning eng kichik yechimi bo'lib, $\varphi(m) = x \cdot q + r$, $0 \le r < x$ bo'lsin, u holda $a^{\varphi(m)} \equiv (a^x)^q \cdot a^r \equiv 1 \cdot a^r(modm) \equiv 1(modm)$, ya'ni $a^r \equiv 1(modm)$. Bu esa x soni

$a^x \equiv 1(modm)$ taqqoslamaning eng kichik yechimi deganimizga zid. Demak, $r = 0$ va $\varphi(m) = x \cdot q$, ya'ni x soni $\varphi(m)$ ning bo'luvchisi.

242. Ferma teoremasiga asosan

$$a_i^5 \equiv a_i(mod5) \text{ va } a_i^5 \equiv a_i(mod2)\ ,\ a_i^5 \equiv a_i(mod3). \qquad (7)$$

Keyingi ikkita taqqoslamaning o'rinli ekanligini bevosita chegirmalarning to'la sistemasini qo'yib, tekshirib ko'rish mumkin. Bulardan

$$a_i^5 \equiv a_i(mod30), \qquad i = 1,2,\dots.n.$$

Bu taqqoslamalarni hadlab qo'shsak,

$$\sum_{i=1}^{n} a_i^5 \equiv \sum_{i=1}^{n} a_i(mod30),$$

ya'ni $M \equiv N(mod30)$. Bundan, agar N soni 30 bo'linsa, M ning ham 30 ga bo'linishi kelib chiqadi.

Izoh.(7) taqqoslamalar $a_i^5 \equiv a_i(mod6)$ ga teng kuchli bu taqqoslamani

$$a_i^5 - a_i \equiv a_i(a_i^4 - 1) \equiv a_i(a_i - 1)(a_i + 1)\big(a_i^2 + 1\big)(mod6)$$
$$\equiv (a_i - 1)a_i(a_i + 1)\big(a_i^2 + 1\big)(mod6).$$

Bunda $(a_i - 1)a_i(a_i + 1) \equiv 0(mod6)$ bo'lganligi uchun $a_i^5 - a_i \equiv 0(mod6)$ bajariladi.

243. Agar a soni 5 ga karrali bo'lsa, $a = 5k$ va $a^{100} \equiv (5k)^{100} \equiv 5^{100} \cdot k^{100} \equiv 0(mod125)$. Agarda $(a; 5) = 1$ bo'lsa, u holda Eyler teoremasiga asosan $a^{\varphi(125)} \equiv 1(mod125)$. Bundan $a^{\varphi(125)} \equiv a^{\varphi(5^3)} \equiv a^{5^3-5^2} \equiv a^{100} \equiv 1(mod\ 125)$. Demak, agar a butun soni 5 ga karrali bo'lsa, a^{100} ni 125 ga bo'lishdan chiqqan qoldiq 0 ga teng, aks holda qoldiq 1 ga teng bo'lar ekan.

244. Masalaning shartiga ko'ra $(a; 10) = 1$. Bu esa $(a; 2) = 1$ va $(a; 5) = 1$ larga teng kuchli. Agar $(a; 5) = 1$ bo'lsa, 24-masalaga asosan

$$a^{100} \equiv 1(mod\ 125)\ . \tag{8}$$

Ikkinchi tomondan esa Eyler teoremasiga asosan $a^{\varphi(8)} \equiv 1(mod8)$. Bundan $a^4 \equiv 1(mod8)$. Bu taqqoslamaning ikkala tomonini 25 −darajaga ko'taramiz, u holda

$$a^{100} \equiv 1(mod\ 8) \tag{9}$$

taqqoslama hosil bo'ladi. (8) va (9) dan $(8; 125) = 1$ bo'lgani uchun $a^{100} \equiv 1(mod\ 1000)$ ni hosil qilamiz. Bu oxirgi taqqoslamaning ikkala tomonini n −darajaga ko'taramiz va keyin ikkala tomonini a ga ko'paytirsak,

$$a^{100n+1} \equiv a(mod\ 1000)$$

ga ega bo'lamiz .

245. a soni 7 ga bo'linmasa, u holda $(a; 7) = 1$ bo'ladi va $a^6 \equiv 1(mod\ 7)$ bo'ladi. Bu taqqoslamani avval m −darajaga keyin eas n −darajaga ko'taramiz. U holda $a^{6m} \equiv 1(mod\ 7)$ va $a^{6n} \equiv 1(mod\ 7)$ larga ega bo'lamiz. Bularni hadlab qo'shsak, $a^{6m} + a^{6n} \equiv 2(mod\ 7)$ ni hosil qilamiz. Ya'ni agar a soni 7 ga bo'linmasa $a^{6m} + a^{6n}$ ni 7 ga bo'lsak, 2 qldiq qolar ekan. Endi $a \vdots 7$ bo'lsin. U holda $a^{6m} \vdots 7$ va $a^{6n} \vdots 7$ bajariladi. Bundan $(a^{6m} + a^{6n}) \vdots 7$, ya'ni $a^{6m} + a^{6n} = 0(mod7)$.

246. Bu yerda $p \neq 5$ chunki, agarda $p = 5$ bo'lsa, $5^{25} + 1 \equiv 0(mod25)$ bo'lishi kerak.Lekin bu yerda ikkinchi qo'shiluvchi 25 ga bo'linmaydi. Berilgan taqqoslamani quyidagicha yozib olamiz:

$$5^{p^2} + 1 = (5^{p^2} - 5) + 6 = 5\left(5^{p^2-1} - 1\right) + 6 = 5[(5^{p-1})^{p+1} - 1] + 6 \equiv 0(modp^2).$$

Ferma teoremasiga asosan $5^{p-1} - 1 \equiv 0(modp)$. Bu yerda $(5^{p-1})^{p+1} - 1$ soni $5^{p-1} - 1$ ga karrali bo'lganligi uchun $[(5^{p-1})^{p+1} - 1]$ soni p ga bo'linadi. Demak, 6 ham p ga bo'linishi kerak. Bundan $p = 2$ yoki $p = 3$. Agar $p = 2$ bo'lsa, u holda $5^{2^2} + 1 = 5^4 + 1 \equiv 626 \not\equiv 0(mod2^2)$, agarda $p = 3$ bo'lsa, u holda $5^{3^2} + 1 = 5^9 + 1 \equiv 1953126 \equiv 0(mod3^2)$. Shunday qilib izlanayotgan son $p = 3$ ekan .

247. Masalaning sharti bo'yicha p va $2p + 1$ lar tub sonlar. Shuning uchun ham Ferma teoremasiga ko'ra $(2p + 1)^2 \equiv 1(mod3)$ va $p^2 \equiv 1(mod3)$. Ikkinchi taqqoslamani 4 ga ko'paytirib $4p^2 \equiv 4(mod3)$ birinchisidan ayiramiz, u holda $4p^2 + 4p + 1 - 4p^2 \equiv 1 - 4(mod3)$ yoki $4p + 1 \equiv -3(mod3)$. Bundan $4p + 1 \equiv 0(mod3)$. Demak, $4p + 1$ soni 3 dan katta va 3 ga bo'linadi. Shuning uchun ham u murakkab son.