Taqqoslamali tenglamalar sistemalarini yechishning klassik usullari, Xitoy qoldiqlar teoremasi

Nasriddin Nomozovich Raximov
nasriddin.raximov@inbox.ru
Ohista Sodiqjon-qizi Soibova
Samarqand davlat pedagogika instituti

Annotatsiya: Mazkur maqolada taqqoslamali tenglamalar sistemalarini yechishning klassik usullari tahlil qilinadi. Xususan, chiziqli taqqoslamalar, ularning yechimlari, modul bo‘yicha arifmetika asoslari hamda Xitoy qoldiqlar teoremasining nazariy va amaliy jihatlari yoritiladi. Tadqiqot davomida sistemalarni yechishda qo‘llaniladigan Yevklid algoritmi, teskari elementni topish usullari hamda Xitoy teoremasining qo‘llanilishi misollar orqali ko‘rsatib beriladi. Natijalar matematik ta’limda hamda olimpiada masalalarini yechishda muhim ahamiyat kasb etadi.

Kalit so‘zlar: taqqoslama, Xitoy qoldiqlar teoremasi, Sun Tsi masalasi, kriptografiya, amaliy masalalar, modul arifmetikasi

Classical methods for solving systems of differential equations, Chinese residue theorem

Nasriddin Nomozovich Rakhimov
nasriddin.raximov@inbox.ru
Ohista Sodiqjon-kizi Saibova
Samarkand State Pedagogical Institute

Abstract: This article analyzes classical methods for solving systems of congruences. In particular, it discusses linear congruences, their solutions, the fundamentals of modular arithmetic, and both the theoretical and practical aspects of the Chinese Remainder Theorem. The study demonstrates the application of the Euclidean algorithm, methods for finding modular inverses, and the use of the Chinese Remainder Theorem through illustrative examples. The results are of significant importance in mathematical education as well as in solving Olympiad-level problems.

Keywords: congruence, Chinese Remainder Theorem, Sun Zi problem, cryptography, applied problems, modular arithmetic

KIRISH (INTRODUCTION)

Sonlar nazariyasining muhim bo‘limlaridan biri bo‘lgan modul arifmetika taqqoslamalar nazariyasining asosini tashkil etadi. Taqqoslamali tenglamalar va ularning sistemalarini yechish masalalari qadimdan matematika rivojida muhim o‘rin tutgan. Ayniqsa, qadimgi Xitoy matematiklari tomonidan ishlab chiqilgan va hozirgi kunda Xitoy qoldiqlar teoremasi nomi bilan mashhur bo‘lgan natija ko‘plab amaliy masalalarni hal qilishda qo‘llaniladi.

Mazkur ishning maqsadi - taqqoslamali tenglamalar sistemalarini yechishning klassik usullarini tizimli ravishda o‘rganish va Xitoy teoremasining nazariy asoslari hamda amaliy qo‘llanilishini tahlil qilishdan iborat.

ADABIYOTLAR TAHLILI VA METODLAR

Ushbu teorema dastlab qadimgi Xitoy matematikasi doirasida, xususan, Sun Tzi tomonidan III asrda yozilgan “Sun Tzi Suan Jing” asarida keltirilgan masalalardan birida shakllangan bo‘lib, keyinchalik Hindiston va Yevropa matematika maktablari tomonidan ilmiy asosda rivojlantirildi va umumlashtirildi. Bugungi kunda Xitoy qoldiqlar teoremasi nafaqat nazariy matematikaning, balki kriptografiya, kodlash nazariyasi va hisoblash texnikasi kabi amaliy sohalarning ham muhim vositalaridan biri hisoblanadi.

Xitoy Qoldiq Teoremasi turli modular bo‘yicha berilgan tenglamalar sistemasini bitta modul bo‘yicha yagona yechimga keltirish imkonini beradi.

1-teorema. Chiziqli taqqoslamalardan iborat quyidagi sistema berilgan bo‘lsin:

$$a_1 x \equiv b_1 (\mathrm{mod}\, m_1)$$
$$a_2 x \equiv b_2 (\mathrm{mod}\, m_2)$$
$$\dots\dots\dots\dots\dots\dots\dots (1)$$
$$a_k x \equiv b_k (\mathrm{mod}\, m_k)$$

bu yerda a_i, b_i, m_i lar berilgan butun sonlardir. Agar m_i lar o‘zaro tub (juft-juftiga tub) bo‘lsa, u holda sistema yechimga ega; aniqrog‘i, $M = m_1 \cdot m_2 \cdot \dots \cdot m_k$ modul bo‘yicha chegirmalar sinfining elementlari berilgan barcha taqqoslamalarni qanoatlantiradi. Ushbu tasdiq *Xitoy qoldiqlar teoremasi* deb ataladi.

Isbot (matematik induksiya bilan). Dastlab, ikkita taqqoslamadan quyidagi iborat sistemani ko‘rib chiqaylik:

$$a_1 x \equiv b_1 (\mathrm{mod}\, m_1)$$
$$a_2 x \equiv b_2 (\mathrm{mod}\, m_2)\ (2)$$

Birinchi taqqoslama, farazga ko‘ra, yechimga ega. Demak, birinchi taqqoslamani qanoatlantiruvchi $x \equiv c_1 (\mathrm{mod} m_1)$ mavjud. Bu yechimni $x = c_1 + tm_1$ (bu yerda $t \in \mathbb{Z}$) ko‘rinishida olib, ikkinchi taqqoslamaga qo‘yamiz.

Bu yechimni $x = c_1 + tm_1$ (bu yerda $t \in \mathbb{Z}$) ko‘rinishida olib, ikkinchi taqqoslamaga qo‘yamiz.

$$a_2 (c_1 + m_1 t) \equiv \mathrm{b}_2 (\mathrm{mod}\, m_2)$$

$$(a_2m_1)t \equiv (b_2 - a_2c_1)(\text{mod } m_2)$$

m_1 va m_2 o‘zaro tub sonlar bo‘lgani uchun, EKUB$(a_2m_1, m_2) = EKUB(a_2, m_2)$ bo‘ladi. Teorema shartlariga ko‘ra, ikkinchi taqqoslama ham yechimga ega, shuning uchun $EKUB(a_2, m_2) \mid b_2$. Bundan esa $EKUB(a_2m_1, m_2) \mid b_2$ kelib chiqadi, bu

$$(a_2m_1)t \equiv (b_2 - a_2c_1)(\text{mod } m_2)$$

taqqoslamasining yechimga ega bo‘lish shartidir. Demak, ikkinchi taqqoslamani qanoatlantiruvchi $t \equiv c_2(\text{mod } m_2)$ mavjud. U holda x ni quyidagicha qayta yozishimiz mumkin:

$$x = c_1 + m_1(c_2 + m_2u) = (c_1 + m_1c_2) + (m_1m_2)u, u \in \mathbb{Z}$$

Bu esa $x \equiv e_1(\text{mod } m_1m_2)$ ko‘rinishidagi yechimni beradi, bu yerda

$$e_1 = c_1 + m_1c_2.$$

Shunday qilib, ikkita taqqoslama uchun yechim mavjud va u modul m_1m_2 bo‘yicha aniqlanadi. Induksiya qadamini davom ettirib, n ta taqqoslama uchun ham yechim mavjudligini isbotlash mumkin.

Endi faraz qilaylik, bu tasdiq $k = \nu$ uchun o‘rinli bo‘lsin. Modullari $m_1, m_2, \dots, m_{\nu+1}$ o‘zaro tub bo‘lgan $\nu + 1$ ta yechimga ega chiziqli taqqoslamalar sistemasini qaraymiz. Dastlabki ν ta taqqoslamadan iborat sistema, induksiya faraziga ko‘ra, yechimga ega. Shuning uchun dastlabki ν ta taqqoslamani qanoatlantiruvchi

$$x \equiv e_\nu(\text{mod } m_1m_2 \dots m_\nu)$$

mavjud.

Endi bu chegirmalar sinfining biror elementi oxirgi taqqoslamani ham qanoatlantirish-qanoatlantirmasligini aniqlashimiz kerak. Buning uchun quyidagi ikkita taqqoslamadan iborat sistemani yechamiz:

$$\begin{cases} x \equiv e_\nu(\text{mod } m_1m_2 \dots m_\nu) \\ a_{\nu+1}x \equiv b_{\nu+1}(\text{mod } m_{\nu+1}) \end{cases}$$

EKUB$(m_{\nu+1}, m_1, \dots, m_\nu) = 1$ bo‘lgani uchun, bu ikki taqqoslamadan iborat sistema yechimga ega bo‘ladi (isbotning birinchi qadamiga o‘xshash).

NATIJALAR VA MUHOKAMA

Xitoy qoldiqlar teoremasi (2) ko‘rinishidagi taqqoslamalar sistemasining modullari o‘zaro tub bo‘lmagan hol haqida hech narsa demaydi. Bunday holda, sistema yechimga ega bo‘lmasligi mumkin, garchi har bir taqqoslama alohida yechimga ega bo‘lsa ham. Ammo sistema yechimga ega bo‘lishi ham mumkin.

Chiziqli taqqoslamalar sistemasi yechimini qurish. Dastlab, (2) sistemasining yechimini qurishning qo‘llaniladigan usulini keltiramiz. Quyidagi ko‘rinishdagi u (2) sistemasining yechimi bo‘lishini ko‘rsatamiz.

2-teorema. Chiziqli taqqoslamalarning (2) yechimga ega sistemasini qaraylik. U holda

$$u = \sum_{i=1}^{k} \frac{m}{m_i} c_i r^{(i)} = \frac{m}{m_1} c_1 r^{(1)} + \cdots + \frac{m}{m_k} c_k r^{(k)} \quad (3)$$

berilgan sistemaning umumiy yechimi bo‘ladi.

Bu yerda: $r^{(i)}$ – bu $a_i x \equiv b_i (\mathrm{mod} m_i)$ taqqoslamasining yechimi,

c_i – $\frac{m}{m_i} y \equiv 1 (\mathrm{mod} m_i)$ taqqoslamasining yechimi, $m = m_1 m_2 \ldots m_k$;

$i = 1, \ldots, k$ va $EKUB\left(\frac{m}{m_i}, m_i\right) = 1$.

Qadimgi Xitoy matematigi Sun Tzi (milodiy IV asr) ga tegishli bo‘lgan matematik risolada quyidagi masalani uchratish mumkin: *“Bir qancha narsalarning noma’lum soni berilgan. Agar ular uchlab sanalsa, ikkitasi ortib qoladi, agar beshlab sanalsa, uchtasi ortib qoladi, agar yettilab sanalsa, ikkitasi ortib qoladi. Bu narsalarning sonini aniqlang”.*

Bu mashhur masala Xitoy qoldiqlar teoremasining klassik misoli bo‘lib, u quyidagi taqqoslamalar sistemasiga ekvivalent:

$$\begin{cases} x \equiv 2 (mod\ 3) \\ x \equiv 3 (mod\ 5) \\ x \equiv 2 (mod\ 7) \end{cases}$$

Demak, $a_1 = 2, a_2 = 3, a_3 = 2$ va $m_1 = 3, m_2 = 5, m_3 = 7$

Yechim. 1) $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k \rightarrow M = 3 \cdot 5 \cdot 7 = 105$

2) $M_i = \frac{M}{m_i}$ dan foydalanib M_1, M_2 va M_3 larni topamiz

$$M_1 = \frac{105}{3} = 35, M_2 = \frac{105}{5} = 21, M_3 = \frac{105}{7} = 15$$

3) Teskari elementlar: $M_i \cdot y_i \equiv 1 (mod\ m_i)$

$$35 \cdot y_1 = 1 (mod\ 3) \rightarrow y_1 = 2$$
$$21 \cdot y_2 = 1 (mod\ 5) \rightarrow\ y_2 = 1$$
$$15 \cdot y_3 = 1 (mod\ 7) \rightarrow y \rightarrow y_3 = 1$$

4) (2) ga qo‘yib hisoblaymiz:

$$x = \sum_{i=1}^{3} a_i \cdot M_i \cdot y_i (mod\ M) = (2 \cdot 35 \cdot 2) + (3 \cdot 21 \cdot 1) + (2 \cdot 15 \cdot 1) = 233$$

$$x \equiv 233 (mod\ 105)$$

Demak, $x = 23 + 105k$ ko‘rinishidagi barcha sonlar sistemani qanoatlantiradi.

Masala. 7 ga bo‘lganda 3 qoldiq, 11 ga bo‘lganda 5 qoldiq va 13 ga bo‘lganda 2 qoldiq qoladigan 1000 dan kichik bo'lgan eng katta natural sonning raqamlar yig‘indisini toping.

Yechim. Taqqoslamalar sistemasini yozib olamiz:

$$\begin{cases} x \equiv 3(\mathrm{mod}7) \\ x \equiv 5(\mathrm{mod}11) \\ x \equiv 2(\mathrm{mod}13) \end{cases}$$

$(7,11) = 1,\ (7,13) = 1, (11,13) = 1 \rightarrow$ Barcha modullar o‘zaro tub, demak, Xitoy qoldiq teoremasini to‘g‘ridan-to‘g‘ri qo‘llash mumkin.

Asosiy ko‘paytmani hisoblash: $N = 7 \cdot 11 \cdot 13 = 1001$

Har bir tenglama uchun N_i va y_i ni topish

Birinchi tenglama ($n_1 = 7$):

$$143 \cdot y_1 \equiv 1(mod7)$$

$$143 \div 7 = 20 \cdot 7 = 140, \text{qoldiq } 3$$

Demak, $3 \cdot y_1 \equiv 1(mod7)$

$$3 \cdot 5 = 15 \equiv 1(mod7) \rightarrow y_1 = 5$$

Ikkinchi tenglama **($n_2 = 11$):**

$$N_2 = \frac{1001}{11} = 91$$

$$91 \cdot y_2 \equiv 1(mod11)$$

$$3 \cdot y_2 \equiv 1(mod11)$$

$$3 \cdot 4 = 12 \equiv 1(mod11) \rightarrow y_2 = 4$$

Uchinchi tenglama ($n_3 = 13$):

$$N_3 = \frac{1001}{13} = 77$$

$$77 \cdot y_3 \equiv 1(mod13)$$

$$77 \div 13 = 5 \cdot 13 = 65, \text{qoldiq } 12$$

$$12 \cdot y_3 \equiv 1(mod13)$$

$$y_3 = 12$$

Yechimni qurish: $x = a_1 N_1 y_1 + a_2 N_2 y_2 + a_3 N_3 y_3$

$$x = 3 \cdot 143 \cdot 5 + 5 \cdot 91 \cdot 4 + 2 \cdot 77 \cdot 12$$

$x = 2145 + 1820 + 1848 = 5813$. **Javob:** 5813

XULOSA

Xitoy qoldiqlar teoremasi bugungi raqamli texnologiyalar uchun ham muhim ahamiyat kasb etadi. Ayniqsa, zamonaviy kriptografiyada, xususan RSA shifrlash algoritmida katta sonlar bilan ishlash talab etilgani sababli, hisoblash jarayonlarini ikki yoki undan ortiq modul bo‘yicha alohida bajarish orqali tezlikni sezilarli darajada oshirish mumkin. Olingan natijalar esa aynan Xitoy qoldiqlar teoremasi vositasida yagona ko‘rinishga keltiriladi. Bunday yondashuv hisoblash xarajatlarini kamaytirish bilan birga, algoritmlarning umumiy samaradorligini ham oshiradi.

Foydalanilgan adabiyotlar

1. Chen E. The Chinese Remainder Theorem. – 2015. – 4 p.

2. Radcliffe M. Math 127: Chinese Remainder Theorem. – Carnegie Mellon University, 2019. – 6 p.

3. Silverman J.H. A Friendly Introduction to Number Theory. Fourth Edition. – Brown University, 2013. – 432 p.

4. Raximov N., Ro'ziyev M. Taqqoslama va uning tatbiqi // “Science and Education” Scientific Journal. – 2022. – Volume 3, Issue 5. – B. 101-107.

5. Maxmudov F. Xitoy qoldiqlar teoremasi va uning masalalarda qo‘llanilishi // RESEARCH AND EDUCATION. – 2023. – Volume 2, Issue 8. – B. 40-45. – ISSN: 2181-3191. – SJIF: 5.789.

6. Raximov, N. and Ro’Ziyev, M., 2022. Taqqoslama va uning tatbiqi. Science and Education, 3(5), pp.106-112.

7. Raximov N. Tub va murakkab sonlar hamda ularga oid masalalarni yechish metodlari //Science and Education. – 2025. – Т. 6. – №. 8. – С. 6-11.

8. Raximov, N. (2023). Sonning butun va kasr qismi qatnashgan tenglamalarni yechish yuzasidan ba’zi metodik tavsiyalar. Science and Education, 4(12), 29-34.

9. Raximov, N., and B. Mamasidikov. "Methods of solving equations related to whole and fractional part of a number." Eurasian Research Bulletin 14 (2022): 190-192.