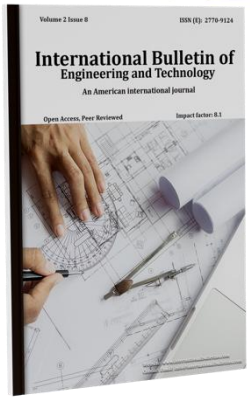

XITOY TEOREMASI.

Berdieva Sevara
Ulasheva Anvara
Otaqulova Zarina
Shahrisabz davlat pedogogika instituti talabari
Turayev Ziyavutdin
Ilmiy rahbar
https://doi.org/10.5281/zenodo.17800181

Annotatsiya.

Ushbu maqolada Xitoy qoldiqlar teoremasining matematik asoslari, tarixiy shakllanish jarayoni, modul tenglamalarining yagona yechim bilan ta'minlanish mexanizmlari va teoremaning isboti ilmiy jihatdan yoritiladi. Shuningdek, teoremaning kriptografiya, axborot xavfsizligi, kodlash nazariyasi, kompyuter arxitekturasi va sonlar nazariyasidagi amaliy qo'llanilishlari batafsil tahlil qilinadi. Teorema yordamida murakkab arifmetik amallarni soddalashtirish, ularga tezkor algoritmik yechim topish imkoniyatlari ochib beriladi.

Kalit so'zlar:

Xitoy qoldiqlar teoremasi, modul arifmetikasi, kriptografiya, RSA algoritmi, qoldiq kodlash tizimi.

Abstract.

This article provides a comprehensive scientific analysis of the Chinese Remainder Theorem, its mathematical foundations, and historical development. The mechanisms ensuring unique solutions to systems of modular congruences and the theorem's formal proof are explained in detail. Furthermore, practical applications in cryptography, information security, coding theory, computer architecture, and number theory are thoroughly examined. The theorem's role in simplifying complex arithmetic operations and enabling efficient computational algorithms is also emphasized.

Keywords:

Chinese Remainder Theorem, modular arithmetic, cryptography, RSA algorithm, residue number system.

Аннотация.

В данной статье приводится всесторонний научный анализ теоремы китайских остатков, раскрываются её математические основы и историческое формирование. Подробно рассматриваются механизмы обеспечения единственности решений систем модульных сравнений и строгие доказательства теоремы. Также анализируются её практические применения в криптографии, информационной безопасности, теории кодирования, компьютерной архитектуре и теории чисел. Особое внимание уделено роли теоремы в упрощении сложных арифметических операций и разработке эффективных вычислительных алгоритмов.

Ключевые слова:

Теорема китайских остатков, модульная арифметика, криптография, алгоритм RSA, система остатков.

Matematikada modul arifmetikasi qadim davrlardan buyon turli masalalarni soddalashtirish, tizimli yechimlarni topish va murakkab tenglamalar sistemalarini

yengillashtirishda muhim o‘rin tutib keladi. Ayniqsa, Xitoy qoldiqlar teoremasi modul tenglamalarining mos yozuvlar tizimini bir yagona yechimga birlashtirishning eng samarali usuli sifatida alohida ahamiyatga ega. Teorema dastlab miloddan avvalgi III asrlarda Xitoy matematiklari tomonidan aytib o‘tilgan bo‘lsa-da, uning mukammal matematik shakli XIX asr matematiklarining tadqiqotlari bilan chuqurlashtirilgan.

XQT modul arifmetikasining asosiy natijalaridan biri bo‘lib, bugungi kunda kriptografiya, kompyuter fanlari, kodlash nazariyasi va sonlar nazariyasida eng ko‘p qo‘llaniladigan teoremalar qatoriga kiradi.

Asosiy qism.

Xitoy qoldiqlar teoremasining tarixiy shakllanishi.

XQT qadimgi Xitoy matematik manbalaridan biri bo‘lgan “Sunzi Suanjing” asarida uchraydi. Unda quyidagi shakldagi masala keltiriladi:

“Bir sonni 3 ga bo‘lganda 2 qoldiq qoladi, 5 ga bo‘lganda 3 qoldiq, 7 ga bo‘lganda 2 qoldiq qoladi. Bu son qanday?”

Bu masala hozirgi modul tenglamalar sistemasiga mos keladi:

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

Sunzi bu tenglama uchun umumiy yechim mavjudligini ko‘rsatgan. Keyinchalik teorema Yevropa matematiklari tomonidan qayta tiklanib, umumlashtirilgan.

Xitoy qoldiqlar teoremasining asosiy formulasi quyidagicha ifodalanadi:

Agar quyidagi ko‘rinishdagi tenglamalar sistemi berilgan bo‘lsa:

Natijada x ning yagona yechimi (mod M bo‘yicha) hosil bo‘ladi.

Xitoy qoldiqlar teoremasi – Asosiy formula.

Agar quyidagi kongruensiyalar tizimi berilgan bo‘lsa:

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$x \equiv a_k \pmod{m_k}$

bu yerda barcha $m_1, m_2, ..., m_k$ o‘zaro nisbatan tub bo‘lsa, unda tizimning yagona yechimi quyidagi formula orqali aniqlanadi:

$x \equiv \Sigma\ (a_i \cdot M_i \cdot y_i) \pmod M$

Bu yerda:

— $M = m_1 \cdot m_2 \cdot ... \cdot m_k$ (umumiy modul),

— $M_i = M / m_i$,

— y_i — M_i ning m_i bo‘yicha teskari elementi, ya’ni $M_i \cdot y_i \equiv 1 \pmod{m_i}$.

Natijada yechim quyidagi ko‘rinishda bo‘ladi:

$x = (a_1M_1y_1 + a_2M_2y_2 + ... + a_kM_ky_k) \bmod M$.

Xitoy qoldiqlar teoremasi sonlar nazariyasining fundamental tushunchalaridan biri bo‘lib, modul arifmetikasi asosida tuzilgan bir nechta tenglamalar sistemasiga yagona yechim mavjudligini ta’minlaydi. Teoremaning mazmuniga ko‘ra, agar tenglamalarda qatnashgan modullar bir-biriga bog‘liq bo‘lmaydigan, ya’ni o‘zaro tub sonlar bo‘lsa, ular bo‘yicha berilgan qoldiqlarga mos keladigan bitta umumiy sonni topish mumkin. Mazkur natija qadimgi Xitoy matematikasida shakllangan bo‘lib, keyinchalik Yevropa matematika maktablari tomonidan ilmiy asosda kengaytirildi.

Teoremaning ahamiyati shundaki, u murakkab arifmetik jarayonlarni soddalashtiradi. Bir nechta modul bo‘yicha alohida-alohida bajarilgan hisob-kitoblar keyinchalik yagona natijaga birlashtirilishi mumkin. Bu esa katta sonlar ustida ishlashda samaradorlikni oshiradi. Teorema, ayniqsa, algoritmlarni optimallashtirishda va parallel hisoblash tizimlarida katta ustunlik beradi.

Xitoy qoldiqlar teoremasi bugungi raqamli texnologiyalarda ham muhim o‘rin tutadi. Ayniqsa, zamonaviy kriptografiya, xususan RSA kabi shifrlash algoritmlarida katta sonlar bilan ishlash zarur bo‘lgani uchun, jarayonlarni ikki yoki undan ortiq modul bo‘yicha ajratib bajarish orqali tezlik sezilarli oshiriladi. Natijalar esa aynan Xitoy qoldiqlar teoremasi yordamida yagona ko‘rinishga keltiriladi. Bu usul hisoblash xarajatlarini kamaytiradi va algoritmlarning samaradorligini oshiradi.

Shuningdek, teorema qoldiq kodlash tizimlarida ham qo‘llanadi. Bunday tizimlarda katta sonlar bir nechta kichik modul bo‘yicha saqlanadi va qayta ishlanadi. Bu esa xatolarga chidamlilikni kuchaytiradi, hisoblash vaqtini qisqartiradi va parallel hisoblash imkoniyatini yaratadi. Kompyuter arxitekturasida, ma’lumotlarni qayta tiklash jarayonlarida va axborot xavfsizligi sohalarida ushbu yondashuvning samarasi yuqori.

Umuman olganda, Xitoy qoldiqlar teoremasi turli modullar orasida uyg‘unlikni ta’minlash, murakkab masalalarni mayda qismlarga ajratib yechish va ularni yagona natijaga birlashtirish imkoniyatini beruvchi kuchli matematik vosita hisoblanadi. Uning qo‘llanish doirasi nafaqat nazariy matematika, balki amaliy informatika, kriptografiya va kompyuter texnologiyalarini ham keng qamrab oladi.

Kodlash nazariyasi va axborot xavfsizligi

XQT qoldiq kodlash tizimlari (RNS) ning asosiy tayanchi hisoblanadi. Bunday tizimlar:

yuqori tezlik,

kam xatolik,

massiv hisoblashni parallel bajarish

kabi ustunliklarga ega.

Kompyuter arxitekturasida qo‘llanilishi.

Ko‘p protsessorli tizimlarda murakkab amallarni modullar bo‘yicha bo‘lib yuborib, parallel ishlashga erishiladi. Natijalar XQT yordamida yagona qiymatga keladi.

Xulosa.

Xitoy qoldiqlar teoremasi modul arifmetikasining eng kuchli va amaliy jihatdan foydali natijalaridan biri hisoblanadi. U tarixan qadimiy bo‘lsa-da, zamonaviy matematikaning turli yo‘nalishlarida, ayniqsa, kriptografiya, kodlash nazariyasi, kompyuter arxitekturasi, sonlar nazariyasi va algoritmik tizimlarda beqiyos ahamiyat kasb etadi.

Teoremaning kuchi — murakkab masalani bir nechta sodda modul tenglamalariga ajratib, qayta birlashtirish imkoniyatidadir. Shu sababli, XQT hozirgacha eng samarali matematik asbob-uskunalardan biri sifatida qo‘llanilmoqda..

Foydalanilgan adabiyotlar:

1. Burton, D. M. Elementary Number Theory. McGraw-Hill, 2011.
2. Rosen, K. H. Discrete Mathematics and Its Applications. McGraw-Hill, 2019.
3. Lidl, R., Niederreiter, H. Introduction to Finite Fields and Their Applications. Cambridge University Press, 1994.

4. Koblitz, N. A Course in Number Theory and Cryptography. Springer, 1994.
5. Sunzi Suanjing (古典数学文献). Ancient Chinese mathematical manuscript