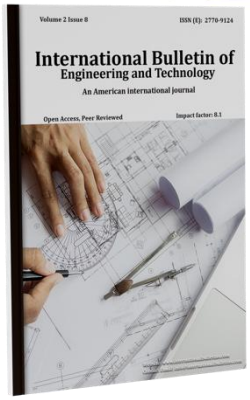

ZAMONAVIY FAN VA TEXNOLOGIYADA XITOY QOLDIQ TEOREMASI.

Boyg ‘uziyeva Shukrona
Amirqulova O‘g‘iloy
Asadullayeva Soniya
Shahrisabz davlat pedogogika instituti pedagogika fakulteti matematika yo‘nalishi 2-kurs talabari
Turayev Ziyavutdin
Ilmiy rahbar:
https://doi.org/10.5281/zenodo.17830378

Anotatsiya: Ushbu maqolada Xitoy qoldiq teoremasining nazariy asoslari,matematik mohiyati va amaliy qo‘llanish yoritiladi. Teoremaning fundamental g‘oyasi bir nechta o‘zaro tub modullar bo‘yicha berilgan qoldiqlar orqali noma’lum sonni tiklash imkoniyati tushuntiriladi. Maqolada teoremaning qo‘llanish sharti bo‘lgan o‘zaro tub modullar tushunchasi izohlanadi, ularning tizimdagi roliga alohida e’tibor qaratiladi. Bundan tashqari, maqolada teoremaning zamonaviy fan va texnologiyadagi ahamiyati keng yoritiladi. Xususan, kriptografiya, parallel hisoblash, parallel hisoblash va kompyuter arxitekturasi kabi yo‘nalishlarda teoremaning qo‘llanilishi yoritilib, katta sonlar bilan ishlashdagi optimizatsiya imkoniyatlari ko‘rsatib beriladi.

Kalit so‘zlar: Xitoy qoldiqlar teoremasi,O‘zaro tub sonlar,Sonlar nazariyas, Qoldiqlar , texnologiya, kriptografiya, modul, kongruensiyalar.

Abstract: This article discusses the theoretical foundations, mathematical essence and practical application of the Chinese remainder theorem. The fundamental idea of the theorem is the possibility of recovering an unknown number from the given remainders for several coprime modules. The article explains the concept of coprime modules, which is a condition for the application of the theorem, and pays special attention to their role in the system. In addition, the article broadly covers the importance of the theorem in modern science and technology. In particular, the application of the theorem in areas such as cryptography, parallel computing, parallel computing and computer architecture is highlighted, and optimization opportunities in working with large numbers are shown.

Keywords: Chinese remainder theorem, Coprime numbers, Number theory, Residues, technology, cryptography, module, congruences,

Аннотация: В данной статье рассматриваются теоретические основы, математическая сущность и практическое применение китайской теоремы об остатках. Основная идея теоремы заключается в возможности восстановления неизвестного числа по заданным остаткам для нескольких взаимно простых модулей. В статье объясняется понятие взаимно простых модулей, являющееся условием применения теоремы, и особое внимание уделяется их роли в системе. Кроме того, в статье широко освещается значение теоремы в современной науке и технике. В частности, освещаются её применение в таких областях, как криптография, параллельные вычисления, параллельные вычисления и архитектура компьютеров, а также показаны возможности оптимизации при работе с большими числамn

Ключевые слова: китайская теорема об остатках, взаимно простые числа, теория чисел, вычеты, технология, криптография, модуль, сравнения.

Xitoy qoldiq teoremasi sonlar nazariyasining eng muhim teoremalaridan biri bo‘lib, turli modul bo‘yicha berilgan kongruensiyalar sistemasining yechimi mavjudligini va uning yagona ekanligini isbotlaydi. Teorema dastlab milodiy III asrda Xitoy matematigi Sun Zi tomonidan bayon qilingan, keyinchalik esa Yevropa matematiklari L.Eyler,K.Gauss va boshqalar tomonidan umumlashtirilgan.Ushbu teoremaga asoslangan metodlar bugungi kunda kriptografik protokollar (RSA algoritmi), parallel hisoblash tizimlari, qator kodlash usullari, katta sonlarni modul bo‘yicha ajratish orqali tezkor hisoblash kabi jarayonlarda markaziy o‘rin tutadi.

Xitoy qoldiq teoremasining matematik mohiyati

Xitoy qoldiq teoremasi sonlar nazariyasidagi eng muhim natijalardan biri bo‘lib, o‘zaro tub bo‘lgan modullar bo‘yicha berilgan kongruensiyalar tizimini yagona yechim yordamida tiklashga imkon beradi. Matematik ifodada u quyidagi shaklda yoziladi:

Dastlab Xitoy qoldiqlar teoremasini keltiramiz:

1-Teorema (Xitoy Qoldiqlar Teoremasi [1]). $m_1, m_2, ..., m_k$ juft-jufti bilan o‘zaro tub va 1 dan farqli natural sonlar bo‘lsin. U holda har biri 0 dan farqli ixtiyoriy $a_1, a_2, ..., a_k$ butun sonlar uchun

$x \equiv a_1, (\text{mod } m_1,)$

$x \equiv a_2, (\text{mod } m_2,)$

… … … … … … … …

$x \equiv a_k, (\text{mod } m_k,)$

Taqqoslamalar sistemasini qanoatlantiruvchi x natural son mavjud. Taqqoslamalar sistemasining har qanday ikkita yechimini $m=m_1 m_2 ... m_k$ ga bo‘lganda bir xil qoldiq qoladi.

Isboti: 1-qadam. Yagona yechim borligini ko‘rsatish

Demak, yechim mavjud.

Faraz qilaylik x va y shu tizimning ikkita yechimi bo‘lsin. Demak:

$x \equiv y (\text{mod } m_1), x \equiv y (\text{mod } m_2), ……., x \equiv y (\text{mod } m_k)$

Bu shuni bildiradiki:

$m_i|(x-y)$ (har bir i uchun)

Demak:

$m_1, m_2, ..., m_k|(x-y)$

Modullar o‘zaro tub bo‘lgani uchun ularning ko‘paytmasi ham bo‘ladi:

$m_1 \cdot m_2 \cdots\cdots m_k = M \cdot (x-y)$

Demak:

$x \equiv y(\text{mod } M)$

Yagona yechim mod M **da mavjudligi isbotlandi.**

2-qadam. Yechim mavjudligini ko‘rsatish

Yechimni qurib olamiz.

Belgilar:

$M=m_1 m_2 \cdots m_n,\ M_i \frac{M}{m_1}$

M barcha modullar ko‘paytmasi, faqat m_i bundan chiqarib tashlangan.

Muhim fakt:

Avvalo shartga ko‘ra EKUB$(m_i \frac{m}{m_1}) = 1$, i = 1,2, … , n o‘rinli.

Chunki m_i boshqa barcha modullardan o‘zaro tub.

Shuning uchun Bézout lemmasiga ko‘ra **har bir i uchun** butun son y_i topiladi:

$M_i y_i \equiv 1 \pmod{m_i}$

Bu y_i-M_i ning m_i modul bo‘yicha teskari elementi.

***3*-qadam. Umumiy yechim formulasi**

Yechim quyidagicha quriladi:

$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots\cdots + a_n M_n y_n$

2 . O‘zaro tub modullar tushunchasi va tizimdagi roli.

XQTning amal qilishi uchun modullar **mutlaqo o‘zaro tub** bo‘lishi zarur. Aks holda, kongruensiyalar orasida mos kelmaslik holati yuzaga kelishi va yechim mavjud bo‘lmasligi mumkin.

Masalan:

$x \equiv (2 \bmod 4)$

$x \equiv (3 \bmod 6)$

bu yerda 4 va 6 o‘zaro tub emas, shuning uchun tizim mos kelmaydi va yechim yo‘q.

O‘zaro tub modullar:

- yig‘indida konflikt yuzaga kelishiga yo‘l qo‘ymaydi,
- yechimning **yagonaligini** kafolatlaydi,
- yirik modulli masalalarni kichik bo‘laklarga ajratishga imkon beradi.

Bu xususiyat teoremaning matematik kuchini belgilaydi.

3. Teoremaning tarixiy shakllanishi

Xitoy qoldiq teoremasining dastlabki shakli eramizning III asrida xitoy matematigi **Sun Tse** tomonidan “Sunzi Suanjing” asarida bayon etilgan. Uning mashhur misollaridan biri quyidagicha:

"Bir sonni 3 ga bo‘lganda qoldiq 2, 5 ga bo‘lganda 3, 7 ga bo‘lganda 2 bo‘lsa, bu son nima?"

Bu savol XQTning ilk ko‘rinishidir.

Keyinchalik:

- **Yevropa matematiglari** — Gauss, Fermat, Lagrange
- Hind olimlari — Brahmagupta teoremaga o‘z hissasini qo‘shgan.

Xususan, Gauss XQTni qat’iy matematik isbot bilan shakllantirdi va modul arifmetikasining to‘liq nazariyasini yaratdi. Shu tariqa qadimiy Xitoy yondashuvi Yevropa matematikasi orqali universal matematik prinsiplarga aylandi.

4. Zamonaviy texnologiyalarda XQTning ahamiyati

Xitoy qoldiq teoremasi hozirgi kunda ko‘plab texnologik jarayonlarda asosiy matematik mexanizmlardan biri hisoblanadi.

4.1. Kriptografiya

XQT:

- RSA algoritmi,
- Shamir secret sharing,
- Modular exponentiation optimizatsiyasi

kabi kriptografik protokollarda ishlatiladi.

Masalan, RSAda katta sonlar ustida hisob-kitoblarni kichik modullar bo‘yicha bo‘lib, tezlashtirilgan shaklda amalga oshirish uchun XQT qo‘llanadi.

4.2. Parallel hisoblash

Teorema yirik arifmetik masalalarni bir nechta protsessorlarga bo‘lib yuborish imkonini beradi. Har bir modul bo‘yicha hisob mustaqil ravishda bajarilari uchun:

- hisoblash tezligi oshadi,
- xatolik ehtimoli kamayadi.

4.3. Kompyuter arxitekturasi va katta sonlar arifmetikasi

XQT:

- katta bitli sonlarni qismlarga bo‘lib ishlash,
- remainder-based memory addressing,
- signal qayta ishlash

kabi jarayonlarda qo‘llaniladi.

Bu usul orqali kompyuter arifmetikasida **modulli operatsiyalar samaradorligi bir necha baravar oshiriladi**.

Xulosa

Xitoy qoldiq teoremasi qadimiy matematikaning bebaho merosi bo‘lib, o‘zaro tub modullar orqali qoldiqlar asosida sonni tiklash imkoniyatini ta’minlaydi. Uning nazariy asoslari modul arifmetikasining eng muhim bo‘limi hisoblanadi. Teorema nafaqat matematikada, balki zamonaviy kriptografiya, parallel hisoblash, kompyuter arxitekturasi, signal qayta ishlash kabi ko‘plab sohalarda markaziy ahamiyat kasb etadi.

Foydalanilgan adabiyotlar (References):

1.Burton, D. M. (2011). Elementary Number Theory. McGraw–Hill.
2.Rosen, K. H. (2012). Elementary Number Theory and Its Applications. Pearson Education.
3.Niven, I., Zuckerman, H. S., & Montgomery, H. L. (1991). An Introduction to the Theory of Numbers. Wiley.
4.Hardy, G. H., & Wright, E. M. (2008). An Introduction to the Theory of Numbers (6th ed.). Oxford University Press.
5.LeVeque, W. J. (1990). Fundamentals of Number Theory. Dover Publications.
6.Koblitz, N. (1994). A Course in Number Theory and Cryptography (2nd ed.). Springer-Verlag.
7.Stillwell, J. (2002). Elements of Number Theory. Springer.
8.Sun, T. (Translation). (1993). The Mathematical Classic of Sun Zi (Sunzi Suanjing).
9.Ding, C., & Pei, D. (1998). Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography. World Scientific.
10.Andrews, G. E. (1971). Number Theory. Saunders College Publishing.