BOSHLANG‘ICH ILDIZLAR. P^A VA P^{2A} MODUL BO‘YICHA BOSHLANG‘CH INDEKISLAR

Zaxriddinova Shaxlo Zaxriddin qizi
Matematika va ta’limda axborot texnologiyasi kafedra o‘qtivchisi
To‘rayeva Charos Jumanazar qizi
Shahrisabz Davlat Pedagogika instituti Pedagogika fakulteti Matematika va Informatika yo‘nalishi 2-bosqich talabasi
https://doi.org/10.5281/zenodo.15129034

Annotatsiya: Ushbu maqolada P^a va P^{2a} moduli bo‘yicha boshlang‘ich ildizlar va indekslar tushunchasi tadqiq qilinadi. Boshlang‘ich ildizlarning matematik asoslari, ularning mavjudlik shartlari va xususiyatlari ko‘rib chiqiladi. Shuningdek, P^a va P^{2a} moduli bo‘yicha indekslash usullari va ularning qo‘llanilish imkoniyatlari tahlil qilinadi. Modulli arifmetika, kriptografiya va algoritmik optimallashtirishdagi amaliy qo‘llanilishi haqida muhokama qilinadi. Maqolada boshlang‘ich ildizlarni topish va indekslarni hisoblash algoritmlari ham bayon etiladi.

Аннотация: В этой статье исследуется концепция простых корней и индексов для модулей Pa и P2a. Рассмотрены математические основы простых корней, условия их существования и свойства. Также анализируются методы индексации и возможности их применения по модулям Па и П2а. Обсуждаются практические приложения в модульной арифметике, криптографии и алгоритмической оптимизации. Также в статье описаны алгоритмы поиска начальных корней и расчета индексов.

Annotation: This article explores the concept of primary roots and indices in terms of the P^a and P^{2a} modules. The mathematical foundations of primary roots, their existence conditions and properties are considered. Also, indexing methods in terms of the P^a and P^{2a} modules and their application possibilities are analyzed. Practical applications in modular arithmetic, cryptography, and algorithmic optimization are discussed. The article also describes algorithms for finding primary roots and calculating indices.

Kalit so‘zlar: Boshlang‘ich ildiz, P^a moduli, P^{2a} moduli, indekslash, diskret logarifm, modulli arifmetika, son nazariyasi, kriptografiya..

Ключевое слово: Простой корень, модуль P^a, модуль P^{2a}, индексирование, дискретный логарифм, модульная арифметика, теория чисел, криптография.

Keywords: Prime root, P^a modulus, P^{2a} modulus, indexing, discrete logarithm, modular arithmetic, number theory, cryptography.

Kirish: Modulli arifmetika va son nazariyasida boshlang‘ich ildizlar tushunchasi muhim rol o‘ynaydi. Ayniqsa, P^a va P^{2a} kabi maxsus modullar uchun boshlang‘ich ildizlarni aniqlash va indekslash masalasi murakkab bo‘lib, uni o‘rganish turli matematik va amaliy masalalarni hal qilishga yordam beradi. Boshlang‘ich ildizlar modulli arifmetikaning asosiy elementlaridan biri bo‘lib, ular kriptografiya, kodlash nazariyasi, son nazariyasi va algoritmik hisoblashlarda keng qo‘llaniladi. Ular yordamida modulli tenglamalarni soddalashtirish, maxfiy kalitlarni generatsiya qilish va tarmoqli hisoblashlarni optimallashtirish mumkin. Mazkur maqolada P^a va P^{2a} modullari bo‘yicha boshlang‘ich ildizlar hamda ularning indekslash usullari tahlil qilinadi. Xususan, quyidagi masalalar ko‘rib chiqiladi: Boshlang‘ich ildizlarning mavjudlik

shartlari va ularni aniqlash usullari; P^a va P^{2a} moduli bo‘yicha boshlang‘ich ildizlarning soni va ularning taqsimoti; Boshlang‘ich indekslash va uni hisoblash algoritmlari; Kriptografik va amaliy qo‘llanilish imkoniyatlari. Mazkur tadqiqot natijalari modulli arifmetikaning yanada chuqur o‘rganilishiga, shuningdek, kriptografik tizimlarning rivojlanishiga hissa qo‘shishi mumkin.

1. Boshlang‘ich ildiz tushunchasi Boshlang‘ich ildiz tushunchasi modulli arifmetikaning muhim qismi bo‘lib, son nazariyasida keng qo‘llaniladi. Berilgan m moduli bo‘yicha g soni boshlang‘ich ildiz deyiladi, agar uning barcha darajalari orqali φ(m) ta turli qoldiqlar hosil qilinsa. Bu shart quyidagi shaklda ifodalanadi: g^k hech qachon 1 ga kongruent bo‘lmasligi kerak, agar $k < \varphi(m)$ bo‘lsa. $g^{(\varphi(m))} \equiv 1 \pmod m$ sharti bajarilishi kerak. Bu yerda φ(m) — Euler funksiyasi, ya’ni m ga nisbatan o‘zaro tub bo‘lgan sonlar sonini bildiradi. Boshlang‘ich ildizlar modulli arifmetikaning asosiy elementlaridan biri bo‘lib, ular quyidagi xossalarga ega: Agar m tub son bo‘lsa, u holda boshlang‘ich ildiz har doim mavjud. Agar $m = p^a$ shaklida bo‘lsa, boshlang‘ich ildizlar soni $\varphi(\varphi(p^a))$ ga teng bo‘ladi. Agar $m = p^{2a}$ bo‘lsa, boshlang‘ich ildizlarni topish yanada murakkab bo‘lib, maxsus algoritmlar talab etiladi.

2. **P^a moduli bo‘yicha boshlang‘ich ildizlar .** P^a moduli uchun boshlang‘ich ildizlarning mavjudligi Agar p tub son bo‘lsa, unda $P^a = p^a$ moduli bo‘yicha boshlang‘ich ildiz mavjudligi quyidagicha belgilanadi: Agar p = 2 bo‘lsa, boshlang‘ich ildizlar a ≥ 2 bo‘lganda mavjud. Agar p toq tub son bo‘lsa, har qanday a ≥ 1 uchun boshlang‘ich ildizlar mavjud bo‘ladi. P^a moduli bo‘yicha boshlang‘ich ildizlar soni Boshlang‘ich ildizlar soni $\varphi(\varphi(p^a))$ orqali aniqlanadi: $\varphi(\varphi(p^a)) = \varphi(p^{(a-1)\ (p-1)}) = p^{\ (a-2)\ (p-1)\ \varphi(p-1)}$. Bu natija boshlang‘ich ildizlarni topish uchun ishlatiladi va kriptografik tizimlarda ahamiyatlidir. P^a m oduli bo‘yicha indekslash Agar g boshlang‘ich ildiz bo‘lsa, har qanday x sonini quyidagi ko‘rinishda ifodalash mumkin: $x \equiv g^k \pmod{p^a}$, bu yerda k — indeks yoki diskret logarifm deb ataladi. Indekslar yordamida modulli hisoblashlarni soddalashtirish mumkin: Ko‘paytirish va bo‘lish amallarini qo‘shishga aylantirish. Kriptografik tizimlarda shifrlash va maxfiy kalit yaratishda ishlatish.

3. P^a moduli bo‘yicha boshlang‘ich ildizlar. P^a moduli bo‘yicha boshlang‘ich ildiz tushunchasi Agar p tub son va a musbat butun son bo‘lsa, unda $P^a = p^a$ moduli bo‘yicha boshlang‘ich ildizlar mavjudligi va ularning sonini aniqlash muhim masala hisoblanadi. g soni p^a moduli bo‘yicha boshlang‘ich ildiz deyiladi, agar uning barcha darajalari orqali $\varphi(p^a)$ ta turli qoldiqlar hosil qilsa. Bu shart quyidagi shaklda yoziladi: $g^{\varphi(p^a)} = 1(\ pmodp^a)$ bu yerda $\varphi(p^a) = p^a - p^{a-1}$ — Euler funksiyasi.

P^a moduli bo‘yicha boshlang‘ich ildizlarning mavjudlik shartlari. 1. P tub son bo‘lganda boshlang‘ich ildizlarning mavjudligi p^a moduli bo‘yicha boshlang‘ich ildizlar mavjudligi quyidagi holatlar bilan bog‘liq: Agar p = 2 bo‘lsa, faqat a ≥ 2 bo‘lganda boshlang‘ich ildizlar mavjud. p = 2, a = 1 holatida esa mavjud emas. Agar p toq tub son bo‘lsa, har qanday a ≥ 1 uchun boshlang‘ich ildizlar mavjud bo‘ladi. Bu natijani isbotlash uchun boshlang‘ich ildizlar soni va modulli ko‘paytirish guruhlari xossalarini ko‘rib chiqish lozim. Euler funksiyasi orqali boshlang‘ich ildizlar mavjudligi Agar g soni p moduli bo‘yicha boshlang‘ich ildiz bo‘lsa, u holda ba’zi hollarda p^a moduli bo‘yicha ham boshlang‘ich ildiz bo‘lishi mumkin. Buni tekshirish uchun quyidagi shart bajarilishi kerak: $g^{\varphi(p^a)} = 1(\ pmodp^a)$. P^a moduli bo‘yicha boshlang‘ich ildizlar soni p^a moduli bo‘yicha boshlang‘ich ildizlarning umumiy soni quyidagi formula orqali aniqlanadi. $\varphi(\varphi(p^a)) = \varphi\ (p^{a-1}(P-1))$ Bu ifodani ochsak: $\varphi\ (p^{a-1}(P-1)) = p^{(a-2)}$

(p-1) φ(p-1) Bu natija boshlang‘ich ildizlar sonini hisoblashda ishlatiladi va kriptografik tizimlarda muhim rol o‘ynaydi. P^a moduli bo‘yicha boshlang‘ich ildizlarni topish algoritmlari Boshlang‘ich ildizlarni topishning turli xil usullari mavjud. Quyida eng samarali algoritmlar keltirilgan: 1. Brute-force usuli (oddiy tekshirish) Agar g boshlang‘ich ildiz bo‘lsa, u holda quyidagi shart bajarilishi lozim: $g^{(\varphi(p^a))} \equiv 1 \pmod{p^a}$ g ^{k} hech qachon 1 ga kongruent bo‘lmasligi kerak, agar $k < \varphi(p^a)$ bo‘lsa. Bu usul kichik qiymatlar uchun samarali bo‘lsa-da, katta qiymatlar uchun juda sekin ishlaydi. Euler teoremasi orqali tekshirish Agar g boshlang‘ich ildiz bo‘lsa, u holda: $g^{\varphi(p^a)} = 1(\text{pmod} p^a)$ 3. Pohlig-Hellman algoritmi Bu algoritm diskret logarifmni faktorizatsiya orqali tez hisoblashga asoslangan bo‘lib, katta qiymatlar uchun juda samarali hisoblanadi. Algoritm quyidagi bosqichlardan iborat.

1. $\varphi(p^a)$ ni faktorizatsiya qilish. 2. g $^{(\varphi(p^a)}$ / qi) ni har bir qi tub ko‘paytuvchilarga bo‘lish. 3. Hosil bo‘lgan qiymatlarni birlashtirish va boshlang‘ich ildizni aniqlash. Bu usul katta modullar uchun qo‘llaniladi va kriptografik tizimlarda ishlatiladi . P^a moduli bo‘yicha indekslash Agar g boshlang‘ich ildiz bo‘lsa, har qanday x sonini quyidagi ko‘rinishda ifodalash mumkin: $x = g^k(\text{pmod} p^a)$ bu yerda k— indeks yoki diskret logarifm deb ataladi. Indeks yordamida modulli hisoblashlarni soddalashtirish mumkin: Ko‘paytirish va bo‘lish amallarini qo‘shishga aylantirish. Kriptografik tizimlarda shifrlash va maxfiy kalit yaratishda ishlatish. P^a moduli bo‘yicha boshlang‘ich ildizlarning amaliy qo‘llanilishi Boshlang‘ich ildizlar turli sohalarda qo‘llaniladi: Kriptografiya – Diffie-Hellman kalit almashinuvi, ElGamal shifrlash algoritmi. Blokcheyn texnologiyalari – Bitcoin va Ethereum kabi kriptovalyutalarda modulli arifmetika asosida ishlovchi protokollar. Kodlash va tarmoqli hisoblash – shaxsiy identifikatsiya va autentifikatsiya tizimlari. Modulli hisoblash algoritmlari – katta sonlar ustida samarali hisob-kitoblar uchun.

Boshlang‘ich ildizlarni topish algoritmlari. Boshlang‘ich ildizlarni topish modulli arifmetika, kriptografiya va kodlash nazariyasi uchun muhim ahamiyatga ega. Boshlang‘ich ildizlar modulli ko‘paytirish guruhining generator elementlari bo‘lib, ular yordamida har qanday qoldiq sinfini hosil qilish mumkin.

1. Boshlang‘ich ildizni topish muammosi Berilgan m moduli bo‘yicha g soni boshlang‘ich ildiz bo‘lishi uchun quyidagi shart bajarilishi lozim: $g^{\varphi(m)} = 1(\text{pmod} p^a)$ bu yerda $\varphi(m)$ — Euler funksiyasi. Bundan tashqari, har qanday $k < \varphi(m)$ uchun: $g^k \neq 1 \pmod m$ Ya’ni, faqat $\varphi(m)$ darajada 1 hosil qilishi kerak. Agar g ushbu shartni bajarsa, u holda m moduli bo‘yicha boshlang‘ich ildiz bo‘ladi. 2. Boshlang‘ich ildizlarni topish algoritmlari Boshlang‘ich ildizlarni topishning bir necha usullari mavjud. Quyida eng samarali algoritmlar ko‘rib chiqiladi. Oddiy tekshirish (Brute-force usuli) Eng oddiy usul g ning barcha mumkin bo‘lgan qiymatlarini tekshirishdan iborat. Algoritm quyidagi bosqichlardan iborat: 1. g ning barcha mumkin bo‘lgan qiymatlarini tanlash ($1 < g < m$). 2. g ning $\varphi(m)$ darajasini hisoblash: $g^{\varphi(m)} = 1 \pmod m$. Agar g natijasi 1 ga erta yetib kelsa, keyingi g sonini sinab ko‘ramiz. Kamchiligi: Katta sonlar uchun sekin ishlaydi. Hisoblash murakkabligi: $O(\varphi(m))$. 2.2. Euler teoremasi asosida tekshirish Boshlang‘ich ildizlarni tezroq topish uchun Euler teoremasidan foydalanish mumkin. Algoritm 1. $\varphi(m)$ ni hisoblash. 2. $\varphi(m)$ ni tub ko‘paytuvchilarga ajratish: $\varphi(m) = p_1^{e1} p_2^{e2} \ldots . p_k^{ek}$ $\varphi(m)^{pi} \neq 1 \pmod m$)

Afzalliklari: Oddiy tekshirishga qaraganda tezroq ishlaydi. 2.3. Diskret logarifm usuli (Indeks usuli) Agar g boshlang‘ich ildiz bo‘lsa, har qanday x quyidagicha ifodalanadi: $x \equiv g^k$

(mod m) bu yerda k — indeks (diskret logarifm). Agar boshlang‘ich ildiz oldindan ma’lum bo‘lsa, barcha indekslar oldindan hisoblab chiqilib, yangi g lar osongina topilishi mumkin. Afzalliklari: Ko‘paytirish va bo‘lish amallarini qo‘shish operatsiyasiga aylantiradi. Tez hisoblash imkonini beradi. Pohlig-Hellman algoritmi Pohlig-Hellman algoritmi diskret logarifmni tub sonlarga ajratib hisoblash printsipiga asoslangan. φ(m) faktorizatsiya qilingan bo‘lsa, u holda bu usul juda tez ishlaydi.

Algoritm 1. φ(m) ni faktorizatsiya qilish: \ $\varphi(m) = p_1^{e1} p_2^{e2} \ldots . p_k^{ek}$

3. Xitoy qoldiqlar teoremasi yordamida natijalarni birlashtirish.

Afzalliklari: Katta modullar uchun ishlaydi. Kriptografik tizimlarda qo‘llaniladi. Kamchiligi: φ(m) ni faktorizatsiya qilish qiyin bo‘lsa, bu usul sekin ishlaydi. Shank’s Baby-Step Giant-Step algoritmi Bu algoritm diskret logarifmni tez hisoblashga mo‘ljallangan. Algoritm

1. $m = \lceil \sqrt{\varphi(m)} \rceil$ qilib olinadi.
2. g ning barcha $g^j \pmod m$ qiymatlari oldindan hisoblanadi (baby-step).
3. $g^{(-m)}$ ning y $g^{(-mi)} \pmod m$ qiymatlari hisoblanadi (giant-step).
4. Indeks j + mi ni topish uchun mos keladigan qiymat qidiriladi. Hisoblash murakkabligi $O(\sqrt{\varphi(m)})$.

Afzalliklari: Diskret logarifmni tezroq hisoblaydi. Katta modullar uchun yaxshi ishlaydi. Pollard rho algoritmi Pollard rho — bu diskret logarifmni hisoblash uchun tasodifiy yurish printsipiga asoslangan probabilistik algoritm. Algoritm1. Tasodifiy funktsiya f(x) aniqlanadi. 2. $X_1 = g^r \pmod m$ va $X_2 = g^s \pmod m$ kabi juftliklar hosil qilinadi. 3. Agar $X_1 = X_2$ bo‘lsa, logarifm topildi. Afzalliklari: Katta sonlar uchun samarali. Amaliy kriptografiyada ishlatiladi. Kamchiligi: Hech qanday aniqlik kafolati yo‘q, natija tasodifiy yurishga bog‘liq. 3. Amaliy qo‘llanilishi Boshlang‘ich ildizlarni topish algoritmlari turli sohalarda ishlatiladi:Kriptografiya – Diffie-Hellman kalit almashinuvi, RSA, ElGamal shifrlash algoritmlari. Blokcheyn texnologiyalari – kriptovalyutalarda tranzaksiya shifrlash. Kodlash nazariyasi – maxfiy kalitlar yaratish. Son nazariyasi – modulli hisob-kitoblar.

Xulosa. Ushbu maqolada P^a va P^{2a} moduli bo‘yicha boshlang‘ich ildizlar va boshlang‘ich indekslar tushunchalari atroflicha o‘rganildi. Boshlang‘ich ildizlar modulli arifmetikaning muhim elementi bo‘lib, ular ko‘plab matematik, kriptografik va kodlash sohalarida ishlatiladi. 1. P^a va P^{2a} moduli bo‘yicha boshlang‘ich ildizlarning ahamiyati P^a va P^{2a} modullar bo‘yicha boshlang‘ich ildizlarni topish oddiy tub modullar holatiga qaraganda murakkabroq masala hisoblanadi. Ular modulli guruhlarning tuzilishini aniqlash va kriptografik protokollarni qurishda muhim rol o‘ynaydi. Euler funksiyasi va diskret logarifm nazariyasi orqali ushbu ildizlarning mavjudligi va xossalari chuqur tadqiq qilinadi.

2. Boshlang‘ich indekslar va ularning roli Boshlang‘ich indeks tushunchasi modulli ko‘paytirish guruhlarining tuzilishini o‘rganish uchun muhim ahamiyatga ega. Ular orqali raqamli autentifikatsiya tizimlari, kriptografik kalit almashinuvi va shifrlash algoritmlari samaradorligini oshirish mumkin. P^a va P^{2a} modullar bo‘yicha boshlang‘ich indekslarni hisoblash oddiy modullar bilan ishlashga qaraganda murakkabroq bo‘lib, bu Pohlig-Hellman, Shank’s BSGS va Pollard rho kabi algoritmlarning qo‘llanilishini talab eta.

3. Amaliy qo‘llanilishi Kriptografiya: Diffie-Hellman kalit almashinuvi, RSA va ElGamal algoritmlari. Son nazariyasi: Modulli arifmetika va algebraik tuzilmalar tadqiqotlari. Kodlash nazariyasi: Ma’lumotlarni shifrlash va autentifikatsiya tizimlari.

4. Tadqiqot natijalari va istiqbollari P^a va P^{2a} moduli bo‘yicha boshlang‘ich ildizlarni topish usullari aniqlandi va ularning samaradorligi tahlil qilindi. Kelajakda ushbu sohada kvant hisoblash, post-kvant kriptografiya va optimallashtirilgan algoritmlar asosida yanada samarali usullar ishlab chiqilishi kutilmoqda. Yangi algoritmlar yordamida P^a va P^{2a} moduli bo‘yicha boshlang‘ich ildizlarni hisoblash tezligi oshirilishi va kriptografik xavfsizlik yanada mustahkamlanishi mumkin. Umuman olganda, P^a va P^{2a} moduli bo‘yicha boshlang‘ich ildizlar va boshlang‘ich indekslar mavzusi matematikaning fundamental bo‘limi bo‘lib, u son nazariyasi, algebra va kriptografiya bilan chambarchas bog‘liqdir. Bu yo‘nalishda yangi ilmiy tadqiqotlar va algoritmlar ishlab chiqish dolzarb masalalardan biri bo‘lib qolmoqda.

Foydalanilgan adabiyotlar/Используемая литература/References:

1. Alimov Sh., Usmonov S. “Elementar sonlar nazariyasi” – Toshkent: Fan, 2010.
2. Mo‘minov A. “Diskret matematika va uning amaliy tatbiqlari” – Toshkent: O‘zbekiston Milliy universiteti nashriyoti, 2015.
3. Karimov U. “Algebra va sonlar nazariyasi” – Toshkent: Sharq, 2012.
4. G‘ulomov K. “Kriptografiya asoslari va uning amaliy qo‘llanilishi” – Toshkent: Iqtisod-moliya, 2018.
5. Ibragimov B. “Raqamli imzo va modulli arifmetika” – Toshkent: Innovatsiya nashriyoti, 2020.
6. Koblitz N. “Sonlar nazariyasi va kriptografiya” – O‘zbek tiliga tarjima qilingan nashr, Toshkent: 2017.
7. Hardy G., Wright E. “Sonlar nazariyasining asoslari” – O‘zbek tiliga tarjima qilingan nashr, Toshkent: Fan, 2016.
8. O‘zbekiston Respublikasi Fanlar akademiyasi “Zamonaviy matematika va uning amaliy tatbiqlari” – Ilmiy jurnal, 2021.
9. IEEE Xplore, Springer va MathSciNet elektron kutubxonalari – Modulli arifmetika va kriptografiya bo‘yicha ilmiy maqolalar.