Ўзбекистон Республикаси Халқ таълими вазирлиги

Қўқон давлат педагогика институти

Физика-математика факультети

“Математика-информатика” кафедраси

У.Й.Акбаров

“Функциялар назарияси фанининг мақсад ва вазифалари. Эллиптик функциялар ва уларнинг тадбиқлари”

Қўқон – 2007

Кириш

Функция тушунчаси математиканинг асосий фундаментал тушунчаларидан бири бўлиб, улар алоҳида назария сифатида ўрганилади ва турли математик ҳамда амалий масалаларни ечишда самарали қўлланилади. Университет, педагогика институтларининг математика, математика-информатика бакалавриат йўналиши ва магистратура мутахассисликларида “Функциялар назарияси” фани ўқитилиши режалаштирилган бўлиб, Ўзбекистон Республикасининг «Таълим тўғрисида»ги Қонуни, «Кадрлар тайёрлаш миллий дастури» ва «Давлат таълим стандартлари» талабларидан функциялар назарияси фанини ўқитишнинг умумий мақсад ва вазифалари келиб чиқади.

Педагогика олий ўқув юртларида функциялар назарияси фанини ўқитишнинг асосий вазифаси - таълимнинг инсонпарварлашуви ва ижтимоийлашувига эришиш; ҳозирги замон шароитларидан келиб чиққан ҳолда ҳар бир бўлажак мутахассисни унинг меҳнат фаолияти ва кундалик ҳаёти учун зарур бўлган математик билим, кўникма ва малакани беришдан иборат.

Функциялар назариясини ўқитишнинг асосий вазифаларига яна қуйидагилар ҳам киради:

- талабаларнинг тўплам ҳақидаги билимларини кенгайтириш;
- метрик фазо ва унинг аҳамиятини ўргатиш;
- акслантиришлар ва уларнинг хоссаларни ўргатиш;
- ўлчовли тўплам ва функциялар ҳақида билим бериш;
- интеграл тушунчасини кенгайтириш;

- мантиқий мулоҳаза ва илмий-адабий нутқни ривожлантириш.

«Функциялар назарияси» фани бўйича талабалар қуйидаги билимларни эгаллаган бўлиши зарур:

- тўпламнинг қуввати, қувватларни солиштириш;
- саноқли, саноқсиз, континуум қувватли тўпламлар;
- рационал сонлар тўпламининг саноқлилиги, ҳақиқий сонлар тўпламининг саноқсизлиги;
- метрик фазо, тўла метрик фазо;
- акслантиришлар, компактда узлуксиз акслантиришларнинг асосий хоссалари;
- қисқартиб акслантириш принципи ва унинг татбиқлари;
- ўлчовли тўплам ва унинг хоссалари;
- ўлчовли функциялар ва уларнинг хоссалари;
- Лебег интеграли ва унинг хоссалари;
- Лебег ва Риман интегралари орасидаги боғланиш;
- комплекс текисликдаги соҳа, чизиқлар;
- комплекс ҳадли кетма-кетлик ва қаторлар;
- комплекс ўзгарувчили функция ва унинг геометрик талқини;
- комплекс ўзгарувчили функциянинг бир варақлилик соҳаси;
- комплекс ўзгарувчили функциянинг узлуксизлиги;
- комплекс ўзгарувчили функция ҳосиласи, Коши-Риман шартлари;
- ҳосила модули ва аргументининг геометрик маъноси;
- конформ акслантириш;
- асосий элементар функциялар ва уларнинг хоссалари;

- асосий элементар функциялар ёрдамида бажариладиган конформ акслантиришлар;
- комплекс ўзгарувчининг функциясининг интеграли;
- Коши теоремаси ва Кошининг интеграл формулалари ва уларнинг татбиқлари;
- даражали қатор, Тейлор қатори;
- аналитик функцияни Тейлор қаторига ёйиш;
- Лоран қатори;
- аналитик функцияни Лоран қаторига ёйиш;
- функциянинг ноллари ва маҳсус нуқталари;
- махсус нуқталарнинг турлари;
- чегирмалар ва чегирмалар ҳақидаги асосий теорема;
- чегирмалар назарияси ёрдамида баъзи интегралларни ҳисоблаш.

Талабалар бу фан бўйича қуйидаги кўникмалар ҳосил қилиши лозим:

- тўпламлар орасида ўзаро бир қийматли акслантириш ўрната олиш:
- тўпламнинг қувватини аниқлаш;
- Кантор-Бернштейн теоремаси ёрдамида тўпламларнинг қувватини аниқлаш;
- метрик фазога доир мисоллар ечиш;
- акслантиришларга доир мисоллар ечиш;
- қисқартиб акслантириш принципини татбиқ қила олиш;
- баъзи тўпламларнинг ўлчовини аниқлаш;
- ўлчовли функцияларга доир мисол ва масалалар ечиш;

- баъзи функцияларнинг Лебег интегралини ҳисоблаш;
- комплекс ҳадли кетма-кетлик ва қаторларни яқинлашишга текшириш;
- комплекс ўзгарувчили функциянинг ҳақиқий ва мавҳум қисмларини ажрата олиш;
- комплекс ўзгарувчининг функциясини узлуксизга текшириш;
- комплекс ўзгарувчининг функцияси ҳосиласини ҳисоблаш;
- комплекс ўзгарувчили функцияни аналитикликка текшириш;
- асосий элементар функцияларга доир мисоллар ечиш;
- асосий элементар функциялар ёрдамида бажариладиган конформ акслантиришларни тавсифлаш;
- комплекс ўзгарувчили функциянинг интегралини ҳисоблаш;
- Кошининг интеграл формуласини интегралларни ҳисоблашга татбиқ қилиш;
- даражали қаторнинг яқинлашиш радиуси ва соҳасини топиш;
- аналитик функцияни Тейлор қаторига ёйиш;
- Лоран қаторини яқинлашишга текшириш;
- аналитик функцияни Лоран қаторига ёйиш;
- функциянинг ноллари ва маҳсус нуқталарини топиш;
- махсус нуқталарнинг турларини аниқлаш;
- чегирмаларни ҳисоблаш;
- чегирмалар назарияси ёрдамида баъзи интегралларни ҳисоблаш.

«Функциялар назарияси» фани бошқа фанлар узвий алоқада. Бу фан «Алгебра ва сонлар назарияси» фанидаги тўпламлар назарияси, комплекс сонлар майдони, ҳақиқий сонлар майдони,

акслантиришларга асосланади. Бу фанни ўрганишда «Дифференциал тенгламалар» фанидаги дифференциал тенглама ечимининг мавжудлиги ва ягоналиги ҳақидаги теорема, геометриядаги геометрик фигураларнинг катталиклари (узунлик, юза, ҳажм) умумлаштирилади, илмий асосланади, «Математик таҳлил» фанидаги ошкармас функциянинг мавжудлиги ва узлуксизлиги ҳақидаги теорема исботланади, «Сонли усуллар», «Математик дастурлаш», «Эҳтимоллар назарияси ва математик статистика» фанларни ўрганишга замин яратади.

Функциялар назарияси алоҳида йўналиш бўлиб, унинг бошқа ўзига хос йўналишлари, қирраларини ҳам ўрганиш мумкин. Масалан, аналитик функцияларни, даврий функцияларни, махсус функцияларни алоҳида ўрганса бўлади. Шулардан бири эллиптик функциялар назариясидир. Шундан келиб чиққан ҳолда ушбу малака ошириш битирув ишида эллиптик функциялар, уларни келиб чиқиши, тадбиқлари, хусусий ҳоллари ҳақида маълумотлар бериш мақсад қилиб олинган.

Эллиптик функцияларга доир маълумотларни [1-4,7-9] адабиётлардан, Интернет саҳифаларидан олиш мумкин.

Эллиптик функциялар алгебраик чизиқлар тушунчаси билан ҳам боғлиқдир.

Алгебраик чизиқлардан

$W2=a0z4+ a1z3+ a2z2+ a3z+ a4$ ёки $W2= a0z3+ a1z2+ a2z+ a3$ кўринишдаги чизиқлар эллиптик чизиқлар дейилади. Эллиптик чизиқларни (z,w) жуфтлик ҳақиқий сонлар бўладиган ҳоли ҳозирги кунда криптология масалаларида қўлланилади[5,6].

Икки даврли мероморф функциялар ва эллиптик функцияларни қуриш

1. Асосий тушунчалар, таърифлар ва мулоҳазалар.

Таъриф. Агар f(z) функция *a* нуқтада аналитик бўлса, у холда *a* нуқта f(z) функциянинг тўғри нуқтаси дейилади.

Таъриф. Берилган f(z) функциянинг тўғри бўлмаган нуқтаси махсус нуқта дейилади.

Таъриф. Агар f(z) функция *a* нуқтанинг бирор $0\langle|z-a|\langle R$ атрофида аналитик бўлиб, *a* нуқтанинг ўзида аналитик бўлмаса, у ҳолда *a* нуқта f(z) функциянинг ажралган махсус нуқтаси дейилади.

Ажралган махсус нуқталар уч типга, яъни қутулиб бўладиган махсус нуқталар, қутблар ва муҳим махсус нуқталарга бўлинади.

Таъриф. Агар А) $\lim\limits_{z\to a} f(z)=A$ бўлиб А аниқ чекли сон бўлса, у ҳолда *a* нуқта f(z) функциянинг қутулиб бўладиган махсус нуқтаси,

Б) $\lim\limits_{z\to a} f(z)=\infty$ бўлса, у ҳолда *a* нуқта f(z) функциянинг қутби,

В) $\lim\limits_{z\to a} f(z)$ мавжуд бўлмаса, а нуқта f(z) нинг муҳим махсус нуқтаси дейилади.

Таъриф. Чекли текисликда қутблардан бошқа махсус нуқталарга эга бўлмаган бир қийматли аналитик функцияни мероморф(ёки каср) функция дейилади.

Мероморф функцияга қуйидагича таъриф бериш ҳам мумкин.

Таъриф. Агар нолдан фарқли f(z) функция ихтиёрий чекли *a* нуқтанинг атрофида

$f(z)=C_0(z-a)^n + C_1(z-a)^{n+1} +\dots$ (бу ерда n–бутун сон, $C_0\neq 0$) ёйилмага эга бўлса, f(z) функция мероморф функция дейилади.

Агар f(z) функция барча z комплекс сонларда аниқланган бўлиб, ихтиёрий z ва бирор ω сон учун f(z+ω)= f(z) тенглик бажарилса, ω сон f(z) функциянинг даври дейилади. ω=0 сони ихтиёрий функция учун давр бўлади. Шунинг учун, даврий функция деганда, камида битта нолдан фарқли даврга эга бўлган функцияни тушунамиз.

Даврий функциялар элементар функциялар ичида ҳам, мероморф ва бутун функциялар ичида ҳам учрайди. Масалан, sinz, cosz функциялар 2π даврга, tgz, ctgz функциялар π даврга, e^z функция эса $2\pi i$ даврга эгадир. Ихтиёрий $\omega\neq 0$ даврга эга бўлган функцияни ҳар доим қуриш мумкин. Масалан, $f(z)=e^{\frac{2\pi i}{\omega}z}$ функция ω даврга эга. Энди ушбу даврий функциялардан умумийроқ бўлган даврий функциялардан бири эллиптик функция тушунчасини кўрамиз.

2. Эллиптик функциялар ва асосий хоссалари.

Таъриф. C комплекс соҳада аниқланган f(z) мероморф функция берилган бўлиб, у $\tau=\omega'/\omega$ нисбат мавҳум сон бўладиган иккита 2ω ва $2\omega'$ даврга эга бўлган даврий функция бўлса, f(z) эллиптик функция дейилади.

Шундай қилиб, эллиптик функциялар икки даврли функция бўлиб, даврларининг нисбати мавҳум сондир, яъни эллиптик функция учун

$$f(z+2\omega)=f(z) \text{ ва } f(z+2\omega')=f(z)$$

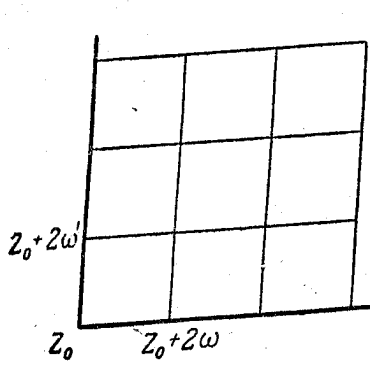
тенгликлар бажарилади. Бу тенгликлардан ихтиёрий m ва n бутун сонлар учун

$$f(z+2m\omega+2n\omega')=f(z)$$

тенгликни бажарилиши келиб чиқади. 2ω ва $2\omega'$ эллиптик функциянинг фундаментал даврлари дейилади.

Текисликда z_0 нуқта олиб, $z=z_0+2m\omega+2n\omega'$ формула орқали m ва n ни ўзгартириб, текисликда ётувчи параллелограмнинг учларида ётувчи нуқталарни топамиз. Ҳосил бўладиган паралеллограм учлари тўпламини P_{mn} деб белгилаймиз.

P_{mn} параллелограмлар даврлар паралеллограми дейилади.



Эллиптик функциялар қуйидаги хоссаларга эга:

1. f(z)=const функция эллиптик функция бўлади.
2. Эллиптик функциянинг ҳосиласи яна эллиптик функция бўлади.
3. Ўзгармас сондан фарқли эллиптик функциялар даврлар паралеллограмида камида битта қутбга эга бўлади.
4. Агар бир хил даврли иккита эллиптик функция даврлар паралеллограмида бош қисмлари бир хил бўлган қутбга эга бўлса, у ҳолда улар ўзгармас сонга фарқ қилади.
5. Агар бир хил даврли иккита эллиптик функция даврлар паралеллограмида бир хил каррали нолларга ва қутбларга эга бўлса, у ҳолда улар ўзгармас кўпайтувчига фарқ қилади.

6. Эллиптик функцияларни даврлар паралеллограмида ётувчи барча қутбларига нисбатан қолдиқларининг йиғиндиси нолга тенг.
7. Эллиптик функциялар даврлар паралеллограмида ихтиёрий қийматини бир хил сон марта қабул қилади.

Таъриф. Агар эллиптик функция даврлар паралеллограмида ихтиёрий қийматини s марта қабул қилса, у ҳолда эллиптик функцияни тартиби s га тенг дейилади.

Теорема. Эллиптик функцияни даврлар паралеллограмида ётувчи барча ноллари йиғиндиси билан барча қутблари йиғиндиси айирмаси эллиптик функциянинг бирор даврига тенг бўлади, яъни

$\sum_{k=1}^{s}\alpha_k - \sum_{k=1}^{s}\beta_k = 2\mu\omega + 2\nu\omega'$ бу ерда $\alpha_к$–ноллар, $\beta_к$–қутблар.

Қуйида эътибор бериш лозим бўлган иккита ҳолатни келтирамиз.

1) Агар 2ω ва 2ω′ даврларга эга бўлган f(z) эллиптик функция

f(z)= – f(K–z) (бу ерда K–бирор ўзгармас сон) муносабатни қаноатлантирса,

K/2, K/2+ω, K/2+ω′, K/2+ ω+ω′

сонлар f(z) функцияни ноллари ёки қутблари бўлади.

2) Агар 2ω ва 2ω′ даврларга эга бўлган f(z) эллиптик функция

f(z)= f(K–z) (бу ерда K–бирор ўзгармас сон) муносабатни қаноатлантирса,

K/2, K/2+ω, K/2+ω′, K/2+ ω+ω′

сонлар $f'(z)$ функцияни ноллари ёки қутблари бўлади.

W= f(z) эллиптик функцияни иккинчи тартибли деб қараб,

$z = \int \frac{dw}{\sqrt{R(w)}}$ (бу ерда R(W) – W га нисбатан 4-тартибли полином)

формулага эга бўлиш мумкин. Ушбу интеграл биринчи тартибли эллиптик интеграл дейилади. Бундан келиб чиққан ҳолда, иккинчи тартибли эллиптик функцияга қуйидагича таъриф бериш мумкин.

Таъриф. $z = \int \frac{dw}{\sqrt{R(w)}}$ кўринишдаги биринчи тартибли эллиптик интегралга тескари функция сифатида аниқланадиган W= f(z) функция иккинчи тартибли эллиптик функция дейилади, бу ерда R(W) – W га нисбатан 4-тартибли полином.

3. Якоби эллиптик функциялари ва асосий хоссалари.

Иккинчи тартибли эллиптик функциялардан бири Якоби эллиптик функциясидир. Якоби эллиптик функциясининг ўзига хос тарихий ва амалий аҳамияти(математик маятник тенгламаси орқали) мавжуд. Бундан ташқари тригонометрик функциялар билан узвий боғлиқли, ўхшашлиги, белгилашларда яқинлик борлиги яққол кўринади. Бу функцияларни тахминан 1830 йилларда Якоби киритган. Якобининг эллиптик функциялари 12 та, уларнинг 3 таси асосий ҳисобланади.

Ушбу $z = \int_0^w \frac{dw}{\sqrt{(1-w^2)(1-k^2w^2)}}$ (1) эллиптик интегралга тескари бўлган функция W=sn(z,k) ёки W=sn(z) ёки W=*sn*z деб белгиланади ва Якобининг sn эллиптик функцияси дейилади. k сони бу функциянинг модули дейилади.

sn функция даври 2ω ва 2iω′ бўлган мероморф функциядир, яъни sn(z+2ω)= sn(z) ва sn(z+2iω′)= sn(z). Бундан ташқари sn(–z)= –sn(z), sn(0)=0. Бу хоссалар sn(z) функция билан оддий

тригонометрик sinz функция орасида айрим ўхшашлик борлигини кўрсатади. (1) да к=0 бўлганда z=arcsin(w) ҳосил бўлади, демак sn(z,0) оддий синусга айланади.

Якобининг кейинги иккита асосий эллиптик функцияси қуйидагича аниқланади:

cn(z,k) = $cnz = \sqrt{1-sn^2 z}$, dn(z,k) = $dnz = \sqrt{1-k^2 sn^2 z}$.

к=0 да cn(z,0) = cosz, dn(z,0) = 1 бўлади.

cn функция даври 2ω ва ω+2iω′ бўлган функциядир. dn функция эса даври ω ва 4iω′ бўлган функциядир.

sn функцияни ифодаловчи (1) формуладан

$$\frac{dw}{dz} = \sqrt{(1-w^2)(1-k^2 w^2)}$$

формулага эга бўламиз. Бундан W=sn(z) эканлигини ҳисобга олсак,

$$\frac{dsnz}{dz} = cnz \cdot dnz$$

ҳосил бўлади. Булардан ташқари қуйидаги муносабатлар ҳам ўринли.

$$\mathrm{cn}^2 + \mathrm{sn}^2 = 1,$$

$$\mathrm{dn}^2 + k^2\mathrm{sn}^2 = 1.$$

$$\frac{dcnz}{dz} = -snz \cdot dnz$$

$$\frac{ddnz}{dz} = -k^2 snz \cdot cnz$$

Якоби функциялари учун қуйидаги қўшиш формулалари ҳам ўринлидир

$$\mathrm{cn}(x+y) = \frac{\mathrm{cn}(x)\,\mathrm{cn}(y) - \mathrm{sn}(x)\,\mathrm{sn}(y)\,\mathrm{dn}(x)\,\mathrm{dn}(y)}{1 - k^2\,\mathrm{sn}^2(x)\,\mathrm{sn}^2(y)},$$

$$\operatorname{sn}(x+y) = \frac{\operatorname{sn}(x)\,\operatorname{cn}(y)\,\operatorname{dn}(y) + \operatorname{sn}(y)\,\operatorname{cn}(x)\,\operatorname{dn}(x)}{1 - k^2\,\operatorname{sn}^2(x)\,\operatorname{sn}^2(y)},$$

$$\operatorname{dn}(x+y) = \frac{\operatorname{dn}(x)\,\operatorname{dn}(y) - k^2\,\operatorname{sn}(x)\,\operatorname{sn}(y)\,\operatorname{cn}(x)\,\operatorname{cn}(y)}{1 - k^2\,\operatorname{sn}^2(x)\,\operatorname{sn}^2(y)}.$$

sn, cn ва dn функцияларда ҳарфларни ўрнини алмаштириб, бу функцияларга тескари функцияларга эга бўламиз, яъни

$$\operatorname{ns}(u) = 1/\operatorname{sn}(u)$$

$$\operatorname{nc}(u) = 1/\operatorname{cn}(u)$$

$$\operatorname{nd}(u) = 1/\operatorname{dn}(u)$$

sn, cn ва dn функцияларни нисбатлари орқали қуйидаги функциялар аниқланади:

$$\operatorname{sc}(u) = \operatorname{sn}(u)/\operatorname{cn}(\mathrm{u})$$

$$\operatorname{sd}(u) = \operatorname{sn}(u)/\operatorname{dn}(\mathrm{u})$$

$$\operatorname{dc}(u) = \operatorname{dn}(u)/\operatorname{cn}(\mathrm{u})$$

$$\operatorname{ds}(u) = \operatorname{dn}(u)/\operatorname{sn}(\mathrm{u})$$

$$\operatorname{cs}(u) = \operatorname{cn}(u)/\operatorname{sn}(\mathrm{u})$$

$$\operatorname{cd}(u) = \operatorname{cn}(u)/\operatorname{dn}(\mathrm{u})$$

Киритилган функцияларни квадратлари учун қуйидаги формулалар ҳам ўринли бўлади:

$$-m_1\,\operatorname{nd}^2(u) + m_1 = -mm_1\,\operatorname{sd}^2(u) = m\,\operatorname{cd}^2(u) - m$$

$$m_1\,\operatorname{sc}^2(u) + m_1 = m_1\,\operatorname{nc}^2(u) = \operatorname{dc}^2(u) - m$$

$$\operatorname{cs}^2(u) + m_1 = \operatorname{ds}^2(u) = \operatorname{ns}^2(u) - m$$

бу ерда $m + m_1 = 1$ ва $m = k_2$.

Якоби эллиптик функияларини чизиқли бўлмаган оддий дифференциал тенгламаларни ечими билан боғлиқлиги

Юқорида кўрдикки, Якобининг эллиптик функцияларини ҳосиласи қуйидагича эди:

$$\frac{\mathrm{d}}{\mathrm{d}z}\,\mathrm{sn}\,(z;k) = \mathrm{cn}\,(z;k)\,\mathrm{dn}\,(z;k),$$

$$\frac{\mathrm{d}}{\mathrm{d}z}\,\mathrm{cn}\,(z;k) = -\mathrm{sn}\,(z;k)\,\mathrm{dn}\,(z;k),$$

$$\frac{\mathrm{d}}{\mathrm{d}z}\,\mathrm{dn}\,(z;k) = -k^2\mathrm{sn}\,(z;k)\,\mathrm{cn}\,(z;k).$$

Кўрсатиш мумкинки, берилган k (0 < k < 1)ларда Якобининг эллиптик функциялари мос равишда қуйидаги оддий дифференциал тенгламаларни ечимлари бўлади:

$\mathrm{sn}\,(x;k)$ функция

$$\frac{\mathrm{d}^2y}{\mathrm{d}x^2} + (1+k^2)y - 2k^2y^3 = 0,$$ ва

$$\left(\frac{\mathrm{d}y}{\mathrm{d}x}\right)^2 = (1-y^2)(1-k^2y^2)$$

тенгламаларни ечимидан иборат бўлади;

$\mathrm{cn}\,(x;k)$ функция

$$\frac{\mathrm{d}^2y}{\mathrm{d}x^2} + (1-2k^2)y + 2k^2y^3 = 0,$$ ва

$$\left(\frac{\mathrm{d}y}{\mathrm{d}x}\right)^2 = (1-y^2)(1-k^2+k^2y^2)$$

тенгламаларни ечимидан иборат бўлади;

$\mathrm{dn}\,(x;k)$ функция

$$\frac{\mathrm{d}^2y}{\mathrm{d}x^2} - (2-k^2)y + 2y^3 = 0,$$ ва

$$\left(\frac{\mathrm{d}y}{\mathrm{d}x}\right)^2 = (y^2-1)(1-k^2-y^2)$$

тенгламаларни ечимидан иборат бўлади.

Якобининг эллиптик функциялари тета-функция ёки Вейерштрасс функцияси орқали ҳам ифодаланиши мумкин. Эллиптик функциялар назариясида $\tau=\omega'/\omega$ катталик ва унга боғлиқ бўлган катталиклар муҳим рол ўйнайди. Ушбу катталикларни ўрганиш эллиптик функциялар назариясини кенгайишига, янги эллиптик функцияларни келтириб чиқарилишига, турли кўринишдаги математик масалаларни қўйилишига ва ушбу масалаларни ечилишига сабаб бўлган.

Эллиптик функцияларни алгебраик чизиқлар тушунчаси билан боғлиқлиги ва тадбиқлари.

Эллиптик функциялар алгебраик чизиқлар тушунчаси билан ҳам боғлиқдир.

$G(z,w)=0$ (2) тенгламани қаноатланирувчи текисликдаги барча (z,w) комплекс сонлар тўплами алгебраик чизиқ дейилади, бу ерда $G(z,w)$ ўз аргументларига нисбатан кўпҳаддир . Бу ердаги алгебраик чизиқ тушунчаси (x,y) ҳақиқий сонлар жуфти учун берилган алгебраик чизиқ тушунчасига ўхшаш ҳолда берилган.

(2) тенгламани ечимларини

$z=\varphi(u)$, $w=\psi(u)$ кўринишдаги бир қийматли аналитик функциялар шаклда ифодалаш алгебраик чизиқларни униформизациялаш дейилади.

Алгебраик чизиқлардан

$W2=a0z4+ a1z3+ a2z2+ a3z+ a4$ ёки $W2= a0z3+ a1z2+ a2z+ a3$ кўринишдаги чизиқлар эллиптик чизиқлар дейилади. Эллиптик чизиқларни (z,w) жуфтлик ҳақиқий сонлар бўладиган ҳоли

ҳозирги кунда криптология масалаларида қўлланилмоқда Қуйида шу ҳақида қисқача тўҳталиб ўтамиз

Қуйидаги

$$y^2 = x^3 + ax + b$$

тенгламани қаноатлантирувчи барча (*x,y*) текислик нуқталарининг геометрик ўрни эллиптик эгри чизиқни ташкил этади.

Кўплаб маълум бўлган криптосистемаларда

$$y^2 = x^3 + ax + b \bmod p, \quad (1)$$

бу ерда p- туб сон, кўринишдаги эллиптик тенглама асос қилиб олинади.

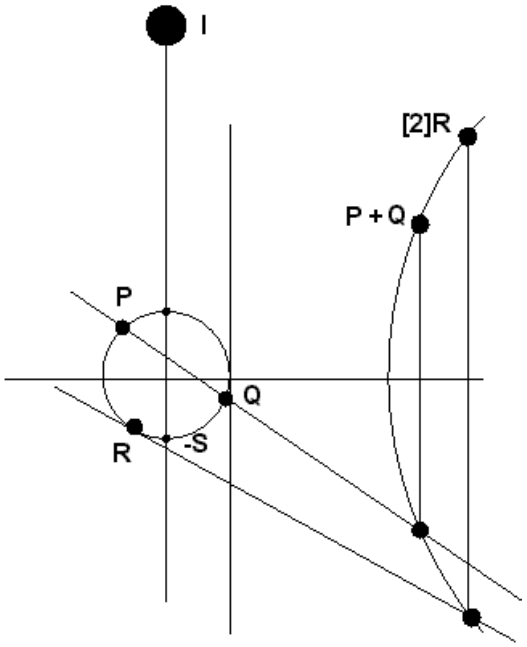
Эллиптик эгри чизиқларда дискрет логарифмлаш масаласининг моҳияти қуйдагича, эллиптик эгри чизиқда берилган $G = (x_G, y_G)$ ва $Д = (x_Д, y_Д)$ нуқталар учун $Д = \gamma G$, яъни $(x_Д; y_Д) = \gamma(x_C; y_C)$ тенгликни қаноатлантирувчи ягона γ ни топишдан иборат.

Эллиптик эгри чизиқлар ёрдамида криптографик алгоритмлар яратишнинг ўзига хос ҳусусиятлари мавжуд. Бу ерда *p* модуль бўйича қолдиқлар билан ишлаш ўрнига геометрик муносабатлардан фойдаланилади. Бунинг биринчи қулайлиги, унда дискрет логарифм муаммосига нисбатан ҳам қийинроқ бўлган геометрик ҳисоблаш усуллари мавжуд (ёки буни маъносини тушуниб олиш осон эмаслигида). Бу масалада унча катта бўлмаган туб сонларни ишлатса ҳам бўлади. Бундай холларда криптографик алгоритмлар тез ишлайди.

p туб сони очиқ ҳолда берилиб, (1) кўринишдаги тенгламада иштирок этади. Бундан ташқари (1) тенглама параметрлари қуйидаги шартни қаноатлантириши керак

$$4a^3 + 27b^2 = 0 \bmod p$$

Шундай қилиб, эллиптик чизиқлар $y^2=x^3+ax+b \bmod p$ тенгламани қаноатлантирувчи x ўқига симметрик бўлган (x,y) нуқталардан иборат. Бу чизиқ нуқталарини маълумотларни бошқариш учун тадбиқ қилишда бу нуқталар устида бажариладиган операциялар киритилган. Масалан, P, Q (R ва R) нуқталарни қўшиш расмда берилган.



Бу операция коммутативлик ва ассоциативлик ҳоссасига эга. Бу нуқталар тўплами алгебраик жиҳатдан ўрганилиб, Эл-Гамалия алгоритми ёрдамида криптология масалаларига тадбиқ этиш мумкинлигини кўрсатиб бериш мумкин.

Адабиётлар

1.Гурвиц А., Курант Р. Теория функций. М.: Наука., 1968, 619 с.

2.Маркушевич А.И. Краткий курс аналитических функций. М.: Наука., 1978, 416 с.

3.Привалов И.И. Введение в теорию функций комплексного переменного. М.: Наука., 1977, 444 с.

4. Сирожиддинов С.Х., Мақсудов Ш., Салоҳиддинов М. Комплекс ўзгарувчининг функциялари назарияси. Т.: Ўқитувчи, 1979, 368 б.

5. Д.Е.Акбаров, В.В.Ясинский. Математика в становлении науки криптологии. Киев, Политехника, 2001. -42 с.

6. Д.Е.Акбаров, Ш.Ш. Ахмадалиев, Ш.З.Нуриев. Криптология асосларида математика. Фарғона, 2002.

7. Milton Abramowitz Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables. — New York: Dover. ISBN ISBN 0-486-61272-4 See Chapter 16

8. Naum Illyich Akhiezer, Elements of the Theory of Elliptic Functions, (1970) Moscow, translated into English as AMS Translations of Mathematical Monographs Volume 79 (1990) AMS, Rhode Island ISBN 0-8218-4532-2

9.E. T. Whittaker and G. N. Watson A Course of Modern Analysis, (1940, 1996) Cambridge University Press. ISBN 0-521-58807-3

Мундарижа