Әдебиеттер:
1. Горский Е.А. Использование электронных средств обучения при изучении тригонометрических функций // Вестник Псковского государственного университета. Серия: Естественные и физико-математические науки. – 2015. - №7. – С. 68-74.
2. Жафяров А.Ж. Методология и технология повышения компетентности учителей, студентов и учащихся по тригонометрии. - Новосибирск: НГПУ, 2011. - 235 с.
3. Мамонтова Т.С., Мусякаева Е.И. Приемы запоминания значений тригонометрических функций // Научно-методический электронный журнал «Концепт». – 2018. – № V8. – С. 51–56.
4.Краевский, В. В. (2002) Методология педагогики: прошлое и настоящее // Педагогика.
5.Гальперин П. Я. (1976) ; теория планомерного формирования умственных действий и понятий,новые методы обучения и воспитания военнослужащих
6.Андреев, В. И. (1998) Педагогика творческо го саморазвития: Инновационный курс. Кн. 2. Казань.
7. Беспалько, В. П. (1995) Педагогика и прогрес сивные технологии обучения. М.
8.Попов, Н. И., Марасанов, А. Н. (2000) Тригонометрия : учеб. пособие. ЙошкарОла : Мар. гос. унт.
9. Азаров, А. И. и др. (1998) Тригонометрия. Тождества, уравнения, неравенства, системы : учеб. пособие. Минск : Полымя.
10. Литвиненко, В. Н., Мордкович, А. Г. (2005) Задачникпрактикум по математике. Алгебра. Тригонометрия : для поступающих в вузы. М. : ОНИКС 21 век.
11.Шаталов, В. Ф. (1993) Методические рекомен дации для работы сопорными сигналами по тригонометрии. М.

ӘОЖ 372.851

ЭЛЛИПТИКАЛЫҚ ҚИСЫҚТАРДЫ МЕҢГЕРУДІҢ МАҢЫЗДЫЛЫҒЫ .

Қошқар Бағлан Жұпарбекұлы, Данебеков Магжан Жандосулы
Механика-математика факультетінің магистранты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан қ.
№ 42 орта мектебінің мұғалімі, Нұр-Сұлтан қ.
Ғылыми жетекші Д. Қозыбаев

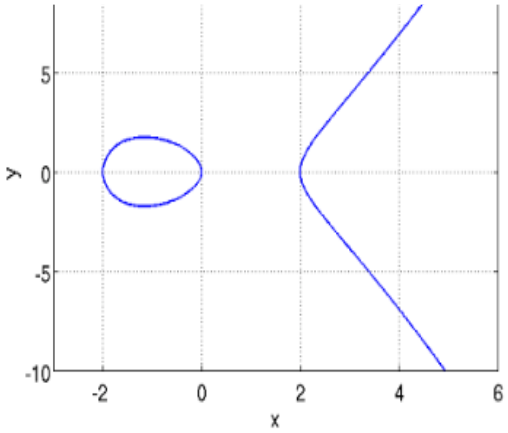
Ақпараттық технологиялардың дамуына байланысты көптеген қолданбалы ғылымдар дамып жатыр. Соның ішінде математика ғылымының қолданбалы саласын қарастыруға болады. Технология дамыған сайын оның қауіпсіздігі бірінші орында тұрғаны белгілі. Жаңартылған білім бағдарламасына сәйкес оқушылар мектеп қабырғасында жоғары математика элементтерін меңгеруі тиіс. Біз де бұл мақалада мектеп оқушыларына эллиптикалық қисықтар туралы алғашқы ақпаратты берудің маңыздылығына тоқталамыз.

Эллиптикалық қисықтар теориясы қазіргі уақытта көптеген салаларда қолданылуда. Соның ішінде, жоғарыда айтып кеткеніміздей, ақпараттық қауіпсіздікті қамтамасыз етуде жиі қолданылады. Сонымен қатар еліміздегі қолданылатын электронды қолдаңба – ақырлы өрістегі эллиптикалық қисықтың нүртелер жиыны ережесіне негізделген.

Эллиптикалық қисық – Вейерштрасс теңдеуімен сипатталатын нүктелер жиыны [1]: $y^2 = x^3 + ax + b.$

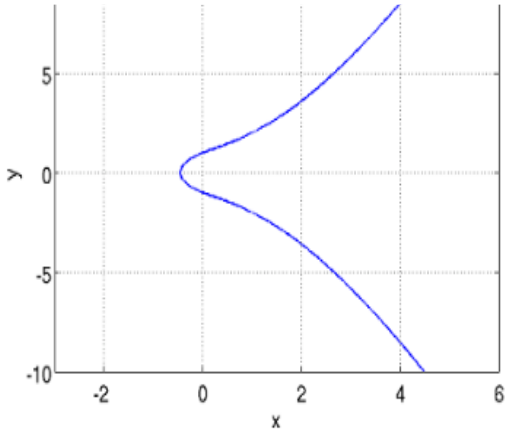
Ескере кететін жағдай, біз эллиптикалық қисықтардың дербес жағдайларын ғана қарастырып отырмыз. Енді эллиптикалық қисықтардың түрлерін қарастыра кетейік:

$y^2 = x^3 - 4x + 0$



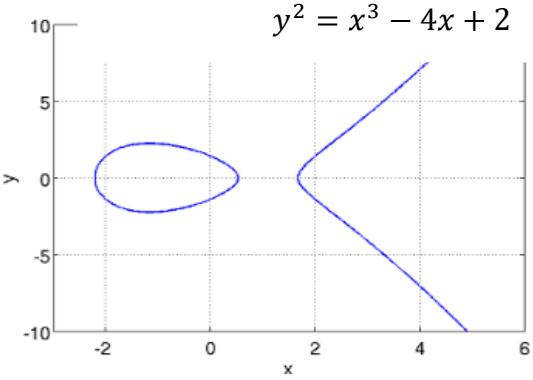
1 - сурет

$y^2 = x^3 + 2x + 1$



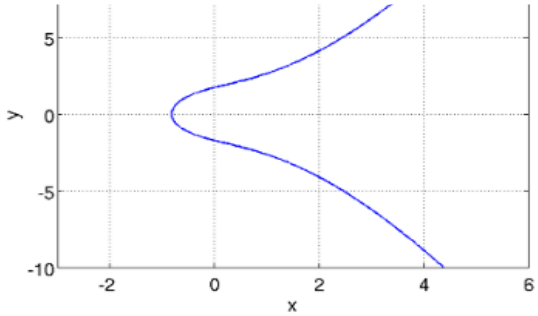
2 - сурет

$y^2 = x^3 - 4x + 2$

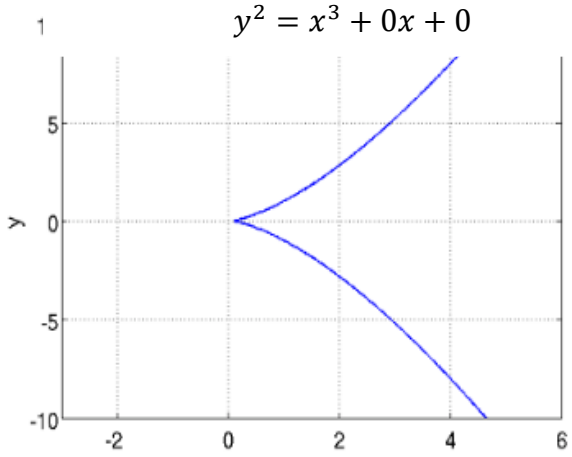


3 - сурет

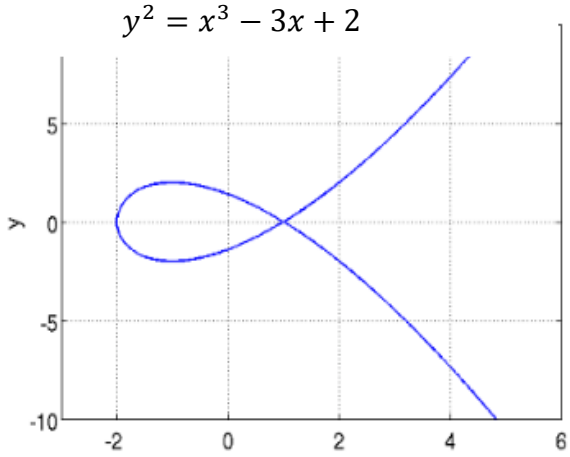
$y^2 = x^3 + 3x + 3$



4 - сурет



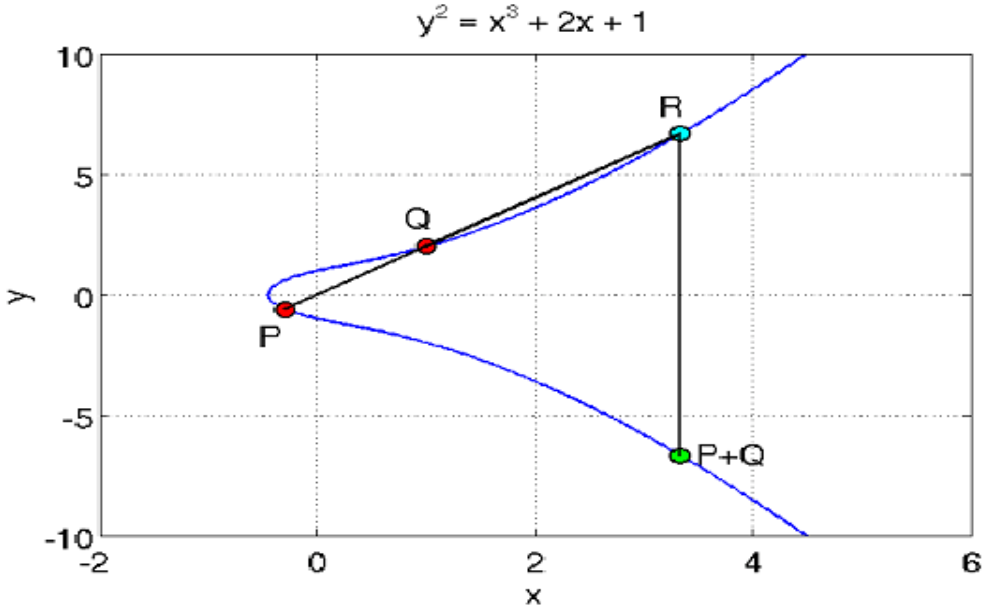
5 - сурет



6 - сурет

Жоғарыда көрсетілген эллиптикалық қисықтардың алғашқы төртеуі тегіс (гладкие) эллиптикалық қисықтар, соңғы екеуі **сингулярлы** эллиптикалық қисықтар деп аталады. Сингулиярлы емес эллиптикалық қисықтар үшін $4a^3 + 27b^2 \neq 0$ осы шарт орындалады.

Эллиптикалық криптографиядағы арифметикалық амалдар эллиптикалық қисық нүктелеріне орындалады. Осы амалдарға тоқтала кетейік. Басым көпшілігі **қосу** амалына қатысты. Екі нүктені қосудық қарапайым түрін қарастыра кетейік:



7 - сурет

7-суретте көрсетілгендей, P және Q нүктелерін қосу үшін , екі нүкте арқылы түзу жүргізу керек, түзу міндетті түрде қисықтың қандай да бір R нүктесімен қиылысады. Горизонталь оське қатысты R нүктесін көрсетіп , P + Q нүктесін аламыз.

Енді, осы Қосу амалын формула түрінде көрсетейік:

$$P + Q = -R$$

P нүктесінің координаты (x_P, y_P) болсын, Q нүктесінің координаты сәйкесінше (x_Q, y_Q) болсын.

Есептейік: $\alpha = \frac{y_Q - y_P}{x_Q - x_P}$, сонда $P + Q$ нүктесінің координаты төмендегідей болады:

$$x_{P+Q} = \alpha^2 - x_P - x_Q$$
$$y_{P+Q} = -y_P + \alpha(x_P - x_R)$$

Біз жоғарыда қисық түрлерін қарастырдық және ең қарапайым мысал ретінде қосу амалына қатысты қысқа шолу жасап өттік. Дәл осылай көбейту амалын да қарастыруға болады. Енгізіліп отырған амалдар жаратылыстану бағытындағы жоғарғы сынып оқушыларына түсінікті болатыны сөзсіз. Өзімізге белгілі критптографияның RSA алгоритмін цифрлық қолтаңбада қолданып жүрміз. Мектепте оқушылар сандар теориясының элементтерін меңгергендіктен, RSA алгоритмін факультатив сабақтарда оқуға болады [2]. Егер кванттық компьютерлер шығатын болса, RSA алгоритмін бұзу қиындық туғызбайды. Олай болса, қолданыстағы алгоритмдерді ары қарай дамыту керек. Олай болса, алгоритмдегі жай сандардың орнына эллиптикалық қисықтарды қойсақ, жаңа алгоритм пайда болады. Әрине өзіне тән есептеудегі күрделі мәселелер де туындайды. Бұл мәселелер бойынша мектеп оқушылары факультатив сабақтарда меңгеріп, математика және информатика пәндері бойынша жоба жасауына болады деп ойлаймыз.

Енді осы эллиптикалық криптографияның артықшылықтарына тоқталайық [3]:

• Эллиптикалық криптографияда кілттердің ұзындығы «классикалық» ассиметриялық криптографиямен салыстырғанда әлдеқайда қысқа

• Эллиптикалық алгоритмнің орындалу жылдамдығы классикалықпен салыстырғанда едәуір жоғары.

• Эллиптикалық криптографияның кілттер ұзындығының қысқалығы және алгоритм жылдамдығы жоғары болғандықтан смарт карталар және есептеу ресурстары шектеулі құрылғыларда қолдануға болады.

Қорытындылай келе эллиптикалық қисықтарды мектеп қабырғасынан бастап оқушыларға таныстыра бастау керек. Сол кезден бастап оқушыларға ақпаратты қорғаудың математикалық негіздері бойынша құзіреттілікке ие бола бастайды. Болашақ мамандығын таңдаған кезде де бұл құзіреттіліктің атқаратын ролі зор. Өйткені ақпаратты сақтауда, қорғауда криптографиялық алгоритмдердің маңызы зор. Ал елімізде жеке меншік алгоритм құру үшін өз кадрларымызды дайындауымыз керек. Мектеп қабырғасынан бастап ақпаратты қорғаудың маңыздылығы мен алгоритмдерін меңгерген оқушылар болашақ еліміздің математика және IT саласының мықты маманы болуы мүмкін.

Эллиптикалық қисықтарды тереңірек меңгеру және зерттеу қазір де, болашақта да ғылымның маңызды бағыттардың бірі болып қала береді.

Қолданылған әдебиеттер:

1. Don Johnson, Alfred Menezes, Scott Vanstone — The Elliptic Curve Digital Signature Algorithm. International Journal of Information Security, volume 1, p. 36–63 (2001).
2. С.Коутинхо. Введение в теорию чисел. Алгоритм RSA. – Москва, Постмаркет. 2001.
3. А. Болотов, С. Гашков, А. Фролов, А. Часовских — Элементарное введение в эллиптическую криптографию. – Москва, Комкнига. 2006.