Пример

Выберем эллиптическую кривую, задаваемую a = 1, b = 1 над полем F_{23}. Уравнение кривой примет вид:

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

Выберем точки A = (9, -7), B = (6, -4).

Вычислим значение выражения A - 3B:

3B = B + 2B;

2B = (k^2 – 2x, k(3x – k^2) – y = (-10, -7);

3B = (6, -4) + (-10, -7) = (7, 11);

A - 3B = $(9,-7)-(7,11)=(9,-7)+(7,-11)=(11,3)$.

ЛИТЕРАТУРА

1. Ш.Т. Ишмухаметов, Р.Г. Рубцова Математические основы защиты информации: Электронное учебное пособие для студентов института вычислительной математики и информационных технологий. – Казань, 2012 г. – 138 с.
2. Ю. Г. Прохоров Эллиптические кривые и криптография: учеб. для вузов – Москва: Механико-математический факультет МГУ, 2007 г. – 144 с.

УДК 519.171

Студ. В.А. Андреюк, Е.А. Баран
Науч. рук. А. А. Якименко
(кафедра высшей математики, БГТУ)

ИСТОРИЯ МАТЕМАТИЧЕСКИХ ОБОЗНАЧЕНИЙ

Слово математика пришло к нам из древнегреческого, где означало "учиться", "приобретать знания. Математика – это первая наука, которую смог освоить человек. Самой древней деятельностью был счёт. Некоторые первобытные племена подсчитывали количество предметов с помощью пальцев рук и ног, а так же палочек. Можно сказать, что 1 палочка – это первый математический символ.

С древнегреческого «символ» (греч. *symbolon* – признак, примета, пароль, эмблема) – знак, который связан с обозначаемой им предметностью так, что смысл знака и его предмет представлены только самим знаком и раскрываются лишь через его интерпретацию.

С открытием математических правил и теорем ученые придумывали новые математические обозначения, знаки. Математические знаки - это условные обозначения, предназначенные для записи математических понятий, предложений и выкладок.

1. Знаки сложения, вычитания

История математических обозначений начинается с палеолита. Этим временем датируются камни и кости с насечками, использовавшимися для счета. Наиболее известный пример – кость Ишанго. Знаменитая кость датируемая примерно 20 тысяч лет до новой эры, доказывает, что уже в то время человек выполнял достаточно сложные математические операции. Насечки на кости использовались для сложения и наносились группами, символизируя сложения чисел.

В Древнем Египте была уже намного более продвинутая система обозначений. Например, в папирус Ахмеса в качестве символа сложения используется изображение двух ног, идущих вперед по тексту, а для вычитания - двух ног, идущих назад. Древние греки обозначали сложение записью рядом, но время от времени использовали для этого символ косой черты “/’’ и полуэллиптическую кривую для вычитания.

Считается, так же, что наш знак происходит от одной из форм слова “et’’, которое по-латыни значит “и’’. Выражение **a + b** писалось на латыни так: **a et b**. Постепенно, из-за частого использования, от знака "**et**" осталось только " **t** " , которое, со временем превратилось в " + ". Первым человеком, который, возможно, использовал знак как аббревиатуру для et, был астроном Николь д’Орем в середине четырнадцатого века.

Обозначения вычитания были более запутанными, так как вместо простого знака “-” в немецких, швейцарских и голландских книгах иногда использовали символ “÷’’, которым мы сейчас обозначаем деление. В нескольких книгах семнадцатого века использованы две точки “· ·’’ или три точки “· · ·’’ для обозначения вычитания.

И даже после принятия знака не все использовали этот символ. Видман (первый использовал знаки «+», «-») сам ввел его как греческий крест (знак, который мы используем сегодня), у которого горизонтальная черта иногда немного длиннее вертикальный. Некоторые математики, такие как Рекорд, Харриот и Декарт, использовали такой же знак. Другие использовали латинский крест « † », иногда расположенный горизонтально, с перекладиной на одном конце или на другом. Наконец, некоторые использовали более декоративный вид « + ».

2.Знак равенства

Знак равенства в математике и других точных науках пишут между двумя идентичными по своему размеру выражениями. Первым употребил знак равенства Диофант. Равенство он обозначил буквой i (от греческого isos – равный). В атичной и средневековой математике равенство обозначалось словесно, например, est egale, или использовали аббревиатуру “ае’’ от латинского aequalis - “равны’’. На других языках также использовали первые буквы слова “равный’’, но это не было общепринятым. Знак равенства "=" ввел в 1557 году уэльский врач и математик Роберт Рекорд. Математическим символом для обозначения равенства служил в некоторых случаях символ II. Рекорд ввел символ “=’’ с двумя одинаковыми горизонтальными параллельными отрезками, гораздо более длинными, чем те, что используются сегодня. Некоторое время распространению символа Рекорда мешало то обстоятельство, что такой же символ использовался для обозначения параллельности прямых; в конце концов было решено символ параллельности сделать вертикальным. Распространение знак получил только после работ Лейбница на рубеже XVII—XVIII веков, то есть более чем через 100 лет после смерти впервые использовавшего его для этого Роберт Рекорд. На его могильной плите нет слов – просто вырезан знак «равно».

Родственные символы для обозначения приблизительного равенства "≈" и тождества "≡" являются совсем молодыми - первый введен в 1885 году Гюнтером, второй - в 1857 году Риманом.

3. Знаки умножения и деления

Знак умножения ввёл в 1631 году Уильям Отред (Англия) в виде косого крестика. До него использовали букву М. Позднее Лейбниц заменил крестик на точку (конец XVII века), чтобы не путать его с буквой x; до него такая символика встречалась у Региомонтана (XV век) и английского учёного Томаса Хэрриота.

Для обозначения действия деления Отред предпочитал косую черту. Двоеточием деление стал обозначать Лейбниц. До них часто использовали также букву D. Начиная с Фибоначчи, используется также черта дроби, употреблявшаяся ещё в арабских сочинениях. Деление в виде обелюс ("÷") ввел швейцарский математик Иоганн Ран.

4. Знак процента.

Символ процента появляется в середине XVII века сразу в нескольких источниках, его происхождение неясно. Есть гипотеза, что он возник от ошибки наборщика, который сокращение cto (cento, сотая доля) набрал как 0/0. Более вероятно, что это скорописный коммерческий значок, возникший лет на 100 раньше**.**

5.Знак бесконечности

Нынешний символ бесконечности "∞" ввел и придумал Джон Уоллис в 1655 году. До сих пор так и не известно, почему он остановил свой выбор именно на этом знаке. Одна из наиболее авторитетных гипотез связывает происхождение этого символа с латинской буквой «М», которую римляне использовали для обозначения числа 1000. Символ бесконечности назван "lemniscus" (лат. лента) математиком Бернулли приблизительно сорок лет спустя.

Другая версия говорит о том, что рисунок «восьмерки» передает главное свойство понятия «бесконечность»: движение **без конца**. По линиям числа 8 можно совершать, как по велотреку, бесконечное движение. Для того, чтобы не путать введенный знак с числом 8, математики решили располагать его горизонтально. Получилось . Такое обозначение стало стандартным для всей математики, не только алгебры. Почему бесконечность не обозначают нулем? Ответ очевиден: цифру 0 как не поворачивай — она не изменится. Поэтому выбор и пал именно на 8.

Другой вариант - змей, пожирающий свой хвост, который за полторы тысячи лет до нашей эры в Египте символизировал различные процессы, не имеющие начала и конца.

6. Знак корня квадратного

Знак корня впервые употребил немецкий математик Кристоф Рудольф, в 1525 году. Происходит этот символ от стилизованной первой буквы слова radix (корень). Черта над подкоренным выражением вначале отсутствовала; её позже ввёл Декарт для иной цели (вместо скобок), и эта черта вскоре слилась со знаком корня.

7.Скобки

Круглые скобки появились в 1556 году у Тартальи (для подкоренного выражения) и позднее у Жирара. Одновременно Бомбелли использовал в качестве начальной скобки уголок в виде буквы L, а в качестве конечной — его же в перевёрнутом виде (1550); такая запись стала прародителем квадратных скобок. Фигурные скобки предложил Виет (1593). Всё же большинство математиков тогда предпочитали вместо скобок надчёркивать выделяемое выражение. В общее употребление скобки ввёл Лейбниц.

8. Знаки угла и перпендикулярности

Символы «угол» и «перпендикулярно» придумал в 1634 году французский математик Пьер Эригон. Символ перпендикулярности у него был перевёрнут, напоминая букву Т. Современную форму Символ угла придал ему Уильям Отред.

9. Знак параллельноси

Символ «параллельности» известен с античных времён. Сначала символ был похож на нынешний знак равенства, но с появлением последнего, во избежание путаницы, символ был повёрнут вертикально.

10. Число пи

Общепринятое обозначение числа, равного отношению длины окружности к ее диаметру (3,1415926535...), впервые образовал Уильям Джонс в 1706 году, взяв первую букву греческих слов окружность и периметр, то есть длина окружности. Это сокращение понравилось Эйлеру, труды которого закрепили обозначение окончательно.

11. Синус и косинус

Sinus с латинского - пазуха, впадина. Далеко в тригонометрии продвинулись индийские математики в районе 5 века. Самого слова "тригонометрия" не было. То, что мы сейчас называем синусом, примерно соответствует тому, что индусы называли ардха-джия, в переводе - полутетива (т.е. полухорда). Для краткости называли просто - джия (тетива). Когда арабы переводили работы индусов с санскрита, они не стали переводить "тетиву" на арабский, а просто транскрибировали слово арабскими буквами. Получилась джиба. Но так как в слоговой арабской письменности краткие гласные не обозначаются, то реально остается дж-б, что похоже на другое арабское слово - джайб (впадина, пазуха). Когда Герард Кремонский в 12 веке переводил арабов на латынь, он перевел это слово как sinus, что по-латыни также означает пазуху, углубление.

Косинус появился автоматически, т.к. индусы называли его коти-джия, или сокращено ко-джия. Коти - изогнутый конец лука на санскрите. Современные краткие обозначения и введены Уильямом Отредом и закреплены в трудах Эйлера.

Обозначения тангенса/котангенса имеют намного более позднее происхождение (английское слово tangent происходит от латинского tangere - касаться). И даже до сих пор нет унифицированного обозначения - в одних странах чаще используется обозначение tan, в других – tg.

Математическая наука необходима для цивилизованного общества. Математика содержится во всех науках. Благодаря математическим открытиям прошлого, ученые создают новые технологии. Сохранившиеся открытия дают возможность решать сложные математически задачи. Благодаря математике Архимед, Платон, Ньютон открыли физические законы. Но математический язык не теряется среди физических формул. Наоборот, эти формулы нельзя написать без знания математики. Благодаря истории сохраняются знания и факты для будущих поколений. Дальнейшее изучение математики необходимо для новых открытий.

ЛИТЕРАТУРА

1. Википедия – свободная энциклопедия [Электронный ресурс].– Режим доступа: https://wikipedia.org.– Дата обращения: 11.04.2017

2. NewConsepts [Электронный ресурс].– Режим доступа: http://newconcepts.club.– Дата обращения: 12.04.2017

История математических обозначений [Электронный ресурс].– Режим доступа: http://dic.academic.ru.– Дата обращения: 13.04.2017

УДК 378.6:519.83

Студ. Д.И.Синюк
Науч. рук. доц. О.Н.Пыжкова
(кафедра высшей математики, БГТУ)

ОБ ОПЫТЕ РЕАЛИЗАЦИИ ИГРЫ ГАРВАРД В БГТУ

Математическая теория игр берёт своё начало из неоклассической экономики. Впервые математические аспекты и приложения теории были изложены в классической книге 1944 года Джона фон Неймана и Оскара Моргенштерна «Теория игр и экономическое поведение». Этот труд был сразу же провозглашен одним из величайших научных открытий века. Авторы предложили систематический подход к пониманию того, как ведут себя игроки в ситуациях, когда результат каждого зависит от действия всех остальных. В этой книге предпринята попытка построения системы аксиом теории игр, игр двух лиц с нулевой суммой, игр n лиц с нулевой суммой [1].

Теория игр получила окончательное признание в 1994 году, когда Джон Нэш, Джон Харшань и Рейнхард Зелтен получили Нобелевскую премию в области экономики за «новаторский анализ равновесия в теории игр с противоположными интересами».

Просматривая в интернете видео обзор лекции по теме «Теория игр» Алексея Владимировича Савватеева я увидел одну некооперативную игру «Гарвард», которая меня заинтересовала. Условие данной игры, следующее: пусть мы имеем множество игроков $\mathrm{N}=(x_1,x_2,x_3,...,x_n)$, каждый из которых должен выбрать одно целое число из промежутка $[1...100]$, таким образом, чтобы выбранное игроком число было как можно ближе к половине среднего арифметического из всех чисел названными игроками. Пусть среднее