UDC 512.12

О ФУНДАМЕНТАЛЬНОЙ ТЕОРЕМЕ АРИФМЕТИКИ. НЕКОТОРЫЕ ПРИМЕРЫ ГЕНЕРАЦИИ ПРОСТЫХ ЧИСЕЛ.

Автор: Тарасов Д.С.
Костанайский государственный педагогический Университет им. У. Султангазина, г. Костанай

Научный руководитель: Алимбаев А.А.
Костанайский государственный педагогический Университет им. У. Султангазина, г. Костанай

Аннотация: В данной работе мы пытаемся искусственно применить аналоги фундаментальной теоремы арифметики на классе вычетов по конечному модулю и с помощью этого построить попытки нахождения простых чисел и найти связь с факторизацией простых чисел. В качестве отправного пункта мы рассмотрим основную теорему арифметики. Актуальность работы обуславливается тем, что фундаментальная теорема арифметики и её следствия широко используются и применяются в различных разделах математики.

Ключевые слова: Фундаментальная теорема арифметики, простые числа, множитель, умножение .

Annotation: In this paper, we try to artificially apply analogs of the fundamental theorem of arithmetic to the class of residues in a finite module and use this to construct attempts to find Prime numbers and find a connection with the factorization of Prime numbers. As a starting point, we will consider the basic theorem of arithmetic. The relevance of the work is due to the fact that the fundamental theorem of arithmetic and its consequences are widely used and applied in various branches of mathematics.

Keywords: Fundamental theorem of arithmetic, prime numbers, multiplier, multiplication .

Аннотация: Бұл жұмыста біз соңғы модуль бойынша шегерімдер класында арифметиканың негізгі теоремасының аналогтарын қолдана отырып, қарапайым сандарды табу және қарапайым сандарды факторизациялаумен байланыс табуға тырысамыз. Бастапқы пункт ретінде біз арифметиканың негізгі теоремасын қарастырамыз. Жұмыстың өзектілігі арифметиканың негізгі теоремасы мен оның салдары математиканың әр түрлі бөлімдерінде қолданылатынымен негізделеді.

Түйін сөздер: арифметиканың фундаменталды теорема, қарапайым сандар ,көбейткіш көптеген.

Фундаментальная теорема арифметики

Определение 1. Целое число p называется простым,если $p \neq 0$ и единственными делителями являются $\pm 1, \pm p$.

Следствие 1.Если p простое и $p/a_1 a_2 \dots a_n$,то p делится по крайней мере одно из a_r.

Теорема 1. Каждое целое число n, кроме 0, ±1 является произведением простых чисел. Эта простое разложение единственно в следующем смысле:

если $n = p_1 p_2 \dots p_r$ и $n = q_1 q_2 \dots q_s$

С p_r, q_s простыми числами, то $r = s$, то есть количество множителей одинаковое ,и после упорядочивания и повторной маркировки $q's$,

$p_1 = \pm q_1$, $p_2 = \pm q_2$, $p_3 = \pm q_3, \dots, p_r = \pm q_r$

Доказательство: Каждое целое число n,кроме $0, \pm 1$ имеет по крайней мере одно простое разложение. Предположим, что n имеет два простых разложения $p_1(p_2 p_3 \dots p_r) = q_1 q_2 \dots q_s$,

Так что $p_1|q_1q_2 \dots q_3$ по следствию 1, p_1 может делиться на один из q_f .Мы можем предположить что $p_1|q_1$.Поскольку p_1 и q_1 являются простыми,мы должны получить $p_1 = \pm q_1$,отсюда следует $\pm q_1p_2p_3 \dots p_r = q_1q_2q_3 \dots q_s$,

Деление обеих сторон на q_1 показывает что $p_2(\pm p_3p_4 \dots p_r) = q_2q_3q_4 \dots q_s$,

Так что $p_2|q_2q_3 \dots q_s$ по следствию 1 p_2 должен разделить один из q_f.Как и прежде мы можем предположить что $p_2|q_2$,отсюда следует $p_2 = \pm q_2$ и $\pm q_2p_3p_4 \dots p_r = q_2q_3q_4 \dots q_s$

Деление обеих сторон на q_2 показывает что $p_3(\pm p_4 \dots p_r) = q_3q_4 \dots q_s$,

Мы продолжаем в том же духе, многократно используя следствие 1 и устраняя по одному простому с каждой стороны на каждом шаге. Если $r = s$ то этот процесс приводит нас к желаемому выводу : $p_1 = \pm q_1$, $p_2 = \pm q_2$,…, $p_r = \pm q_s$ Итак, чтобы завершить доказательство теоремы, мы должны показать что $r = s$. Доказательство того что $r = s$ можно доказать противоречием: мы предположим что r не равно s (что означает что $r > s$ или $r < s$), и покажем что это предположение приводит к противоречию.

Во первых предположим что $r > s$.То после с шагов предыдущего процесса все $q's$ будут устранены и уравнение будет таким $\pm p_{s+1}p_{s+2} \dots p_r = 1$

Это уравнение говорит что $p_r|1$.Поскольку единственным делителем единицы является ± 1,мы имеем $p_r = \pm 1$.Однако, поскольку p_r является простым числом,мы знаем что $p_r \neq \pm 1$,по определению «простое».Мы пришли к противоречию ($p_r = \pm 1$ *и* $p_r \neq \pm 1$).Поэтому $r > s$ не может произойти. Аналогичный аргумент показывает, что предположение $r < s$ также приводит к сокращению и отсюда следует не может произойти. Значит $r = s$ это единственная возможность и теорема доказана.

Следствие 2.Каждое целое число $n > 1$ может быть записано в виде $n = p_1p_2p_3 \dots p_r$ только одним способом, где p_f положительные простые числа,такие что $p_1 \leq p_2 \leq p_3 \leq \cdots \leq p_r$

В теории легко определить, является ли положительное целое число n простым.Нужно просто разделить n на каждое целое число между 1 и n, чтобы увидеть, имеет ли n множитель, отличный от 1 и n. На самом деле,вам нужно только проверить простые делители, потому что любой множитель n(кроме 1) делится по крайней мере на одно простое число.

Пример 1:Докажите, что каждое целое число $n > 1$ может быть записано в форме $p_1^{r_1}p_2^{r_2} \dots p_t^{r_t}$ с p_t отличными положительными простыми числами и каждое $r_i > 0$

Доказательство: Согласно теореме 1 ,каждое целое число, кроме $0, \mp 1$,может быть записано как произведение простых чисел, и представление является уникальным вплоть до порядка и знаков простых чисел. Поскольку в нашем случае $n > 1$ положительно и мы хотим использовать положительные простые числа, представление будет уникально вплоть до порядка. Так запишем $n = q_1q_2 \dots q_s$, где каждое $q_i > 0$ является простым. Пусть $p_1p_2 \dots p_r$ различные простые числа в списке. Собирая вместе каждое p_i , «давая» r_i копии p_i, то есть $p_i^{r_i}$.

■

Аналоги фундаментальной теоремы на классе вычетов по конечному модулю

В своей работе мы хотим найти аналог фундаментальной теоремы арифметики в конечном множестве Z_n.

Пусть -произвольное целое положительное число. Рассмотрим множество Z_n всех классов чисел, сравнимых между собой по модулю n. Конечное множество Z_n тесно связано с бесконечным множеством Z . Поэтому естественно спросить, можно ли

определить умножение в Z_n и сделать там какую-нибудь разумную арифметику. Чтобы определить умножение в Z_n необходимо взять 2 класса в Z_n и перевести их в другой класс с помощью произведения. Умножение классов сравнимых между собой чисел определяется по представителям : $[a][b] = [ab]$. Это умножение , очевидно , коммутативно и ассоциативно.

Пример 1: Построить таблицу умножения в Z_5 .

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	4	1	4	2
4	0	4	3	2	1

Поскольку мы работаем в Z_5 и читатель возможно еще не знаком с правилами умножения в таких числовых множествах , мы разберем некоторые из произведений:

$2 \cdot 3 = 1$ в Z_5, в обычном известном нам множестве Z целых чисел мы получили бы $2 \cdot 3 = 6$.В этом случае в Z_5 мы действительно получаем 1, что можно проверить по алгоритму деления , где $6 = 5 \cdot 1 + 1$

$4 \cdot 3 = 2$ в Z_5 ,если сделать проверку, то получаем $12 = 5 \cdot 2 + 2$, когда в множестве Z целых чисел мы получили бы $4 \cdot 3 = 12$

Теперь найдем «простые» числа в Z_5 для этого выпишем представление каждого числа , кроме 0 и 1, из таблицы в виде произведения других чисел:

$2 = 3 \cdot 4$

$3 = 2 \cdot 4$

$4 = 2 \cdot 2 = 3 \cdot 3$

Можно предположить что из выписанных чисел, «простыми» в Z_5 будут являться числа 2 и 3 , так как только эти два числа можно записать в единственном разложении , и ни одно из них не будет присутствовать в собственной записи разложении числа.

Чтобы проверить эту нашу гипотезу , построим таблицу умножения в Z_8 и найдем «простые» числа.

Пример 2. Построить таблицу умножения в Z_8.

	0	1	2	3	4	5	6	7

	0	0	0	0	0	0	0	0
0	0	1	2	3	4	5	6	7
	0	2	4	6	0	2	4	6
1	0	3	6	1	4	7	2	5
	0	4	0	4	0	4	0	4
2	0	5	2	7	4	1	6	3
	0	6	4	2	0	6	4	2
3	0	7	6	5	4	3	2	1
4								
5								
6								
7								

Выпишем разложение каждого числа , кроме 0 и 1, из данной таблицы:

$$2 = 2 \cdot 5 = 3 \cdot 6 = 6 \cdot 7$$

$$3 = 5 \cdot 7$$

$$4 = 2 \cdot 6 = 3 \cdot 4 = 4 \cdot 7$$

$$5 = 3 \cdot 7$$

$$6 = 2 \cdot 3 = 5 \cdot 6$$

$$7 = 3 \cdot 5$$

Из чего мы можем сделать вывод что на множестве Z_8 , так называемыми «простыми» числами будут 3,5,7 . Исходя из этого мы можем предположить аналог фундаментальной теоремы арифметики в конечном Z_n.

Теорема 2. Каждое целое число x , кроме 0, ±1 будет являться простым числом в конечном Z_n , если это число можно представить в виде произведения «простых» чисел.

Попытки генерации простых чисел

С древних времен простые числа привлекают большое внимание математиков. Закон , по которому простые числа следуют один за другим еще не найден. Простые числа в математике имеют очень большую значимость, и играют очень важную роль. С помощью умножения простых чисел можно получить все остальные числа. Но с этими числами существует проблема , которая до сих пор остается нерешенной , все простые числа невозможно сосчитать. « Самого большого простого числа не существует » - именно эти слова сказал один из умнейших математиков древности Евклид.Трудно сказать, когда впервые люди начали задумываться о простых числах, ученые предполагают , что это могло происходить более двух веков назад. Греческие , египетские , арабские математики внесли огромный вклад в изучение простых чисел . Именно поиск простых чисел является одной из самых парадоксальных проблем математики . Эту проблему пытаются решить уже несколько тысячелетий , но она остается нерешенной до наших дней. Появление простых чисел не подчинено какому-либо закону : они появляются в ряду натуральных чисел в случайном порядке и не смотря на все попытки вычислить хоть какую-нибудь закономерность , ученым так и не удалось её найти. Такие великие математики как Пьер Ферма , Марен Мерсенн , Леонард Эйлер , Рене Декарт и множество других математиков трудились над поиском максимально больших чисел.

Рассмотрим наиболее общеизвестные попытки генерации простых чисел.

1.Решето Эратосфена . Один из самых известных алгоритмов вычисления простых чисел - Решето Эратосфена(Сито Эратосфена). Алгоритм назван в честь греческого математика Эратосфена Киренского, именно его называют автором этого алгоритма.По методу Эратосфена, чтобы найти все простые числа , меньше заданного числа, нужно следовать следующему алгоритму:

1)Записать натуральные числа от 1 до P.

2)Вычеркнуть 2 и далее все числа кратные ей , затем вычеркнуть 3 и каждое третье число.

3)Продолжать этот процесс, пока возможно, выбирая каждый раз первое оставшееся не вычеркнутым число , следующее за тем , кратные которому были вычеркнуты последними.

4)Числа, которые остались и будут составлять множество простых чисел от 1 до P.

2.Пьер Ферма и его простые числа

Пьер Ферма выдвинул следующую гипотезу: все числа вида $2^n + 1$ всегда простые , где n степень двойки. Проверив свою гипотезу для $n = 1,2,4,8,16$,и был уверен , что если n не является степенью двойки , число не всегда получится простым. Именно эти числа носят название чисел Ферма, и только через 100 лет Леонард Эйлер доказал, что число $2^{32} + 1 = 4294967297$ будет делиться на 641,и не будет являться простым числом.

3.Предположение для облегчения нахождения простых чисел на определенном промежутке. Мое предположение , опирающееся на Решето Эратосфена , основывается на том , что можно все простые числа на каком либо промежутке , с помощью признаков делимости на 2 , 3 , 4 , 5 , 6 , 7 , 8 , 9 , 10 , 11 , 13 , 17 , 19 , 20 , 23 , 25 , 27 , 29 , 30 , 31 , 41 , 50 , 59 , 79 , 99 ,101.Например , можно попробовать найти все простые числа от 2500 до 2800,с помощью признаков делимости. Как итог мы получим числа: 2503 , 2521 , 2531 , 2539 , 2543 ,2549 , 2551 , 2557 , 2579 , 2591 , 2593 , 2609 , 2617 , 2621 , 2633 , 2647 , 2657 , 2659 , 2663 , 2671 , 2677 , 2683 , 2687 , 2689 , 2693 , 2699 , 2707 , 2711 , 2713 , 2719 , 2729 , 2731 , 2741 , 2749 , 2753 , 2767 , 2777 , 2789 , 2791 , 2797 .Ни одно из этих чисел нельзя представить в виде произведения каких-либо чисел , кроме как произведения самого числа на 1,также ни одно из этих чисел не удовлетворяет ни одному из признаков делимости.

Список литературы:

А. И. Кострикин , Введение в алгебру/ Издательство «Наука», 1977 – 496 с.

Л. Я. Куликов, Алгебра и теория чисел/ Москва «Высшая школа», 1979 – 559 с.

Э. Фрид , И. Пастор , П. Ревес , И. Рейман, И. Ружа , Малая математическая энциклопедия/ Издательство академии наук Венгрии, Будапешт 1976 – 693 с.

Abstract Algebra: An Introduction, Third Edition Thomas H. Huneerford . Brooks/Cole 20 Channel Center Street Boston, MA 02210 USA, 2014

ПАЙЫЗДАРҒА БАЙЛАНЫСТЫ МӘТІНДІК МӘСЕЛЕ ЕСЕПТЕРДІ ШЕШУДІ ОҚЫТУ ӘДІСТЕМЕСІ

Теңізбай Г.М.

Ө.Сұлтанғазин атындағы Қостанай мемлекеттік педагогикалық университеті, Қостанай қ.