**Шамаев Николай Вячеславович**
*Ученик 11 класса*
*общеобразовательной школы №131,*
*г. Харьков, Украина.*

# Интересные теоремы теории чисел и их использование в криптографии

В статье рассмотрены некоторые теоремы теории чисел, относящиеся к двум разделам: «простые числа» и «наибольший общий делитель». Часть теорем, приведённых в статье, имеют необычайный интерес, ведь их доказательства и формулировки нигде не встречались (по крайней мере, автору). Приведён пример использования доказанных теорем в криптографии.

## 1. Теоремы о простых числах

*Числами-близнецами* назовём такие простые числа, которые отличаются на 2.

Какие же свойства имеют эти числа? Основные из них иллюстрируют теорема 1 и следствия из неё.

**Теорема 1.** Пусть даны два числа-близнеца $p$ и $p + 2$ ($p > 3$). Тогда $(p+1) \vdots 6$.

Для доказательства этой теоремы докажем сначала следующую лемму.

**Лемма.** Числа-близнецы дают остатки 1 и 2 при делении на 3. Причём

$p \equiv 2 \pmod 3$ и $p + 2 \equiv 1 \pmod 3$.

**Доказательство леммы.** Простые числа при делении на 3 дают остатки 1 или 2. Предположим, что $p \equiv 1 \pmod 3$, тогда

$$p + 2 \equiv 3 \equiv 0 \pmod 3,$$

т. е. $p + 2$ делится нацело на 3, что невозможно, так как $p + 2$ простое. Тогда $p \equiv 2 \pmod 3$, $p + 2 \equiv 2 + 2 = 4 \equiv 1 \pmod 3$, что и требовалось доказать.


**Доказательство теоремы 1.** Рассмотрим сумму

$p + (p + 2) = 2p + 2 = 2 (p + 1)$.

Поскольку $p > 3$, оно не делится нацело на 2. Тогда $p + 1$ делится нацело на 2. Теперь согласно лемме получим:

$p + (p + 2) \equiv 2 + 1 \equiv 3 \equiv 0 \pmod 3$.

Получили, что $2(p + 1)$ делится нацело на 3. Число 2 на 3 не делится, следовательно, $p + 1$ делится нацело на 3. Но оно делится ещё и на 2. Следовательно, оно делится и на 6. Что и требовалось доказать.

Из теоремы 1 также следует, что квадраты двух чисел-близнецов дают остаток 1 при делении на 3. Действительно,

$$p \equiv 2 \pmod 3,$$
$$p^2 \equiv 2^2 = 4 \equiv 1 \pmod 3,$$
$$p + 2 \equiv 1 \pmod 3,$$
$$(p + 2)^2 \equiv 1 \pmod 3.$$

(Вообще, квадраты всех чисел, не делящихся на 3, дают остаток 1 при делении на 3.)

Ещё из теоремы 1 следует, что сумма двух соседних чисел-близнецов делится на 12, потому что $2(p + 1)$ делится на 2, а $p + 1$ делится на 6 (по теореме 1).

Приведем ещё одну теорему.

**Теорема 2.** Если $p$, $p + 2$ и $q$, $q + 2$ – соседние пары чисел-близнецов, то $q - (p + 2) \geq 4$.

**Доказательство.** Пусть

$$q - (p + 2) = q - p - 2 = z.$$

Тогда $q - p = z + 2$. Поскольку $q$ и $p$ – первые числа в парах чисел-близнецов, согласно лемме

$$q - p \equiv 2 - 2 = 0 \pmod 3.$$

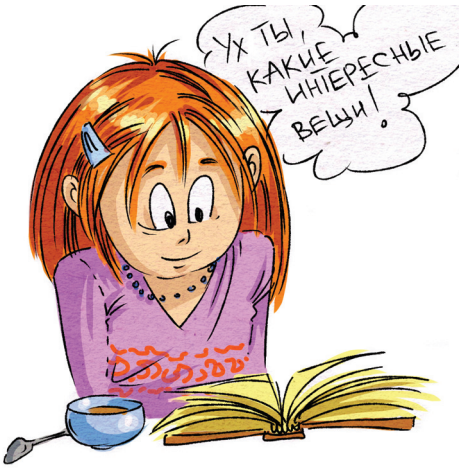
Значит, $q - p$ делится на 3:

$$q - p = (z + 2) \vdots 3.$$

Следовательно, $z \equiv 1 \pmod 3$. Поэтому или $z = 1$, или $z \geq 4$. Если $z = 1$, то одно из чисел $q$ или $p$ чётно, что невозможно. Следовательно, $z \geq 4$, что и требовалось.

На этом простые свойства чисел-близнецов заканчиваются. Дальше только объяснение того, что множество таких чисел бесконечно и использование математического анализа. Но в это мы углубляться не будем.

Далее рассмотрим интересное свойство четырёхзначных чисел.




**Теорема 3.** Пусть четырёхзначное число $n$ не делится нацело ни на одно простое число от 2 до 97. Тогда $n$ простое.

На первый взгляд может показаться, что доказательство этого факта очевидно и сам факт очевиден. Но это не так. Приведём строгое и красивое доказательство этой теоремы для объяснения природы таких чисел.

**Доказательство.** Рассмотрим, каким образом четырёхзначное число может быть представлено в виде произведения двух чисел (по разрядности чисел в десятичной записи). Результаты приведены в таблице.

| № | Разрядность чисел, которые в произведении дают 4-значное число | |
|---|---|---|
| **1** | 1 | 3 |
| **2** | 2 | 3 |
| **3** | 2 | 2 |
| **4** | 1 | 4 |

Возникает вопрос: почему именно так? Почему четырёхзначные числа не могут, например, быть образованы двухзначным и четырёхзначным числами? Потому что если мы возьмём наименьшее двухзначное число 10 и наименьшее четырёхзначное число 1000, то при умножении получим ре-

зультат 10 000 – число, которое не является четырёхзначным. Отброс остальных случаев, не попавших в таблицу, происходит аналогично.

Приступим теперь к основной части доказательства теоремы. Если четырёхзначное число образовано так, как указано в вариантах 1 и 4 таблицы, то соответствующего однозначного числа, которое, очевидно, больше 1 и не делится ни на одно простое число из набора 2, ..., 97, не существует. Аналогично не существует двухзначного числа, не делящегося ни на одно простое число от 2 до 97, из вариантов 2 и 3 таблицы. Так что однозначным числом в варианте 4 является 1. То есть наше число является простым. Что и требовалось доказать.

## 2. Теоремы о наибольшем общем делителе

Поскольку наибольший общий делитель является, наверное, одним из самых интересных объектов, изучаемых в теории чисел, приведем несколько общеизвестных, но занимательных теорем. Начнем с интересного факта, связанного с наибольшим общим делителем.

**Теорема 4.** Пусть НОД $(a,b) = d$. Тогда НОД $\left(\frac{a}{d},\frac{b}{d}\right) = 1$.

**Доказательство.** Предположим, что

$$\left(\frac{a}{d},\frac{b}{d}\right) = m > 1.$$

Тогда

$$\frac{a}{d} \vdots m, \quad \frac{b}{d} \vdots m.$$

Следовательно,

$$a \vdots dm, \; b \vdots dm.$$

Но наибольшее число, на которое делятся $a$ и $b$, равно $d$. Поскольку $m > 1$, получаем противоречие, следовательно НОД $\left(\frac{a}{d},\frac{b}{d}\right) = 1$.

А теперь важная теорема. Она обязательно должна пригодиться!

**Теорема 5.** Пусть $a, b, c \in \mathbb{N}$, при этом $a^2 = bc$ и НОД $(b,c) = 1$. Тогда $b$ и $c$ – полные квадраты.

Доказательство теоремы, как и все доказательства в этой статье, достаточно интересное и не требует дополнительных знаний от читателя.

**Доказательство.** Понятно, что необходимо рассматривать, каким образом может быть образован квадрат. Рассмотрим на конкретном примере: $6^2 = 36 = 9{\cdot}4 = 3{\cdot}3{\cdot}2{\cdot}2$. Видим, что число образовано парами одинаковых множителей. На этом и будет построено доказательство теоремы. Кстати, 9 и 4 – полные квадраты. Поскольку НОД $(b,c) = 1$, числа взаимно просты и не имеют общих множителей. Поэтому в произведении этих чисел не будет образовано пар одинаковых множителей, то есть образовать число $a^2$ можно только произведением полных квадратов, что и требовалось доказать.

В следующей теореме будет использован алгоритм теоремы 4. Лишний раз убеждаемся в её необходимости. (О верной очерёдности теорем судить только вам.)

**Теорема 6.** Пусть $au + bv = 1$. Тогда НОД $(a,b) = 1$.

**Доказательство.** Нам нужно доказать, что НОД $(a,b) = 1$, другими словами, что числа взаимно просты и не имеют общих множителей. Предположим противное – что у них есть общие множители (хотя бы один, например $p_1^{\alpha_1}$).

Пусть

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\pi^{\alpha_\pi}$$

и $b = p_1^{\alpha_1} \varsigma_2^{\beta_2} \ldots \varsigma_\kappa^{\beta_\kappa}$.

Тогда

$$au + bv = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\pi^{\alpha_\pi} \cdot u +$$

$$+ p_1^{\alpha_1} \varsigma_2^{\beta_2} \ldots \varsigma_\kappa^{\beta_\kappa} \cdot v =$$

$$= p_1^{\alpha_1} \left( p_2^{\alpha_2} \ldots p_\pi^{\alpha_\pi} \cdot u + \varsigma_2^{\beta_2} \ldots \varsigma_\kappa^{\beta_\kappa} \cdot v \right) = 1.$$

Значит, или $p_1^{\alpha_1} = 1$, или

$$p_2^{\alpha_2} \ldots p_\pi^{\alpha_\pi} \cdot u + \varsigma_2^{\beta_2} \ldots \varsigma_\kappa^{\beta_\kappa} \cdot v = 1 < au + bv,$$

что невозможно. Полученное противоречие доказывает теорему.

Теперь должен обязательно возникнуть вопрос: «И что же с этим всем делать? Есть ли какое-то применение в реальной жизни?» Оказывается, есть.

## 3. Применения

Рассмотрим такую задачу.

**Задача 1.** Есть канал связи между племенами А и Б. Двум программистам племен А и Б необходимо установить между собой контакт (враг наступает!), но этот же самый враг канал связи закодировал. Шпионы узнали, что шифром является четырёхзначное простое число (причём любое). Вывести алгоритм для написания программы, которая будет подтверждать или опровергать предположения шпиона по поводу шифра, причём её работа должна быть начата в кратчайший срок. Племена не обладают суперкомпьютерами и им необходимо наладить контакт. Программисты племён А и Б знают только простые однозначные и двухзначные числа.

**Решение.** Ясно, что желаемого результата можно достичь простым перебором четырёхзначных простых чисел, они всем известны (погуглите), но это один из длительно работающих алгоритмов, то есть нам это не подходит. Но племена-то далёкие и знают только двухзначные и однозначные простые числа. В этом и состоит проблема. Простому человеку, например, попавшему на олимпиаду, эту задачу будет решать трудно. Но у нас есть теорема 3! Она и составляет решение задачи.


Всего простых двухзначных и однозначных чисел 25. Поэтому, очевидно, что программа с другим алгоритмом будет работать значительно дольше. Итак, алгоритм будет таков.

Шпион передал шифр, программа проверяет его делимость на 25 первых простых чисел. Если число не делится нацело на простое число в каждом из случаев, программа должна выдавать 1, если делится – 0. Тогда в каждом из 25 вариантов программа выдаст либо 1, либо 0. Просуммировав результаты, получаем, что для того чтобы число, переданное шпионами, было простым, сумма должна оказаться 25. Если

так окажется, программа выдаст `true`, если нет – `false`. То есть программисты могут раскодировать канал связи, используя только свои возможности.

Рассмотрим ещё одну задачу, она будет маленьким продолжением первой.

**Задача 2.** Пусть шифр состоит не из одного числа, а из двух чисел-близнецов (задача 1). Вывести алгоритм, который по двум данным числам покажет, являются ли они искомым шифром.

**Решение.** Построим алгоритм, похожий на алгоритм задачи 1. Ясно, что нам нужно выяснить, на сколько отличаются два данных нам числа (поскольку программисты не могут производить арифметические операции не на компьютере). Тогда программа считает два числа, вычисляет их разность. Если она равна 2, то алгоритм продолжается, если нет – выведет `false`. Далее программа проверит таким образом, как в задаче 1, два числа и получит результат: `true` или `false`.

Понятно, что возникает вопрос о написании не только алгоритма, но и самой программы на каком-то из языков программирования. Это мы оставляем читателю.

Я очень надеюсь, что теоремы, приведённые в статье, вам помогут в дальнейшей работе при изучении математики, программирования и криптографии.

## Юмор Юмор Юмор Юмор Юмор Юмор

### Вот так ответ!

Один из газетных магнатов как-то запросил у астрономов срочный ответ на вопрос: «Есть ли жизнь на Марсе?» и оплатил их телеграмму в тысячу слов. Ответ состоял всего из двух слов: «Nobody knows» (никто не знает), повторённых 500 раз.

### Вывод лектора

Если бы не было такого явления, как магнетизм, то, например, у мореплавателей не было бы компаса, и тогда Колумб вряд ли открыл бы Америку. Хотя, пожалуй, лучше бы он её не открывал.