НЕКОТОРЫЕ ТЕОРЕМЫ ТЕОРИИ ЧИСЕЛ И ПРИМЕНЕНИЕ ИХ В ЭЛЕМЕНТАРНЫХ ЗАДАЧАХ КРИПТОГРАФИИ

Николай Шамаев, г. Харьков, Харьковская народная республика

В данной статье будут рассмотрены достаточно интересные теоремы теории чисел, а вернее, посвященные числам-близнецам и интересному свойству четырехзначных чисел, которое может значительно помочь в криптографии. Статья рассчитана на широкий круг читателей: как и для тех, кто только начал интересоваться математикой, так и более титулованным научным сотрудникам. Теоремы, приведенные в статье имеют необычайный интерес, ведь их доказательство и формулировка нигде не встречались (если, конечно же, читателю известны источники доказательства или формулировки, или есть свои доказательства — я с радостью приму их во внимание).
Теперь приступим к формулировкам и доказательствам теорем (конечно же, с наличием авторского комментария).

1.1. Числа-близнецы.

Числами-близнецами назовем такие простые числа, которые отличаются на 2. Какие же свойства имеют эти числа? Основные из них иллюстрируют теорема и следствия к ней.

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

Доказательство теоремы 1.
Докажем сначала лемму.
Лемма 1. Числа-близнецы дают остатки 1 и 2 при делении на 3. Причем $p \equiv 2 \pmod 3$ и $(p+2) \equiv 1 \pmod 3$.
Доказательство леммы. Простые числа при делении на три 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.
Но $(p+2)$ — простое, то есть это невозможно. Тогда $p \equiv 2 \pmod 3$, $(p+2) \equiv 2+2 = 4 \equiv 1 \pmod 3$, что и требовалось доказать.
Продолжим доказательство теоремы.
Теперь, рассмотрим сумму $p+p+2 = 2p+2 = 2(p+1)$. Поскольку $p > 3$, то p — не делится нацело на 2. Есть $p+1$ делится нацело на 2. Теперь, согласно лемме 1, получим: $p+p+2 = 2p+2 = 2(p+1)$

$\equiv 2 + 1 = 3 \equiv 0 \pmod 3$. Получили, что $2(p+1)$ делится нацело на 3. 2 на 3 не делится, следовательно $p + 1$ делится нацело на 3. Но оно делится еще и на 2. Следовательно, оно делится и на 6. Что и требовалось доказать. Еще 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 (из теоремы). Попросту, на этом простые свойства чисел-близнецов заканчиваются. Дальше только — объяснение их бесконечности существования и использования математического анализа. Но до этого уровня мы углубляться не будем.