Теория чисел в криптографии, доказательства некоторых теорм из лекции
14 апреля 2019 г., АНО Школа 21

1. **Сколько всего простых чисел?** *Рассмотрим два различных доказательства.*

   (a) Пойдем от противного. Предположим, что простых чисел **не** бесконечно много, тогда пусть $\mathbb{P} = \{p_1, p_2, p_3, ..., p_n\}$ - все существующие простые числа. Тогда рассмотрим $\prod_1^n p$ и $\prod_1^n p + 1$. По Алгоритму Евклида НОД $(\prod_1^n p, \prod_1^n p + 1) = 1$. Это значит, что данные числа взаимно простые и у числа $\prod_1^n p + 1$ есть простые делители, отличные от простых делителей числа $\prod_1^n p$, однако по нашему предположению $\prod_1^n p$ делится на все существующие простые числа. Противоречие. $\blacksquare$

   (b) Рассмотрим следующую бесконечную сумму:

$$(*) \quad \Sigma_{n=1}^{\infty}\frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + ... + \frac{1}{n} + ...$$

   Сгруппируем ее члены следующим образом:

$$\Sigma_{n=1}^{\infty}\frac{1}{n} = (1) + (\frac{1}{2}) + (\frac{1}{3} + \frac{1}{4}) + (\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}) + ... + \frac{1}{n}...$$

   Рассмотрим вспомогательную сумму(заменим в каждой скобке дроби на наименьшую имеющуюся):

$$(1) + (\frac{1}{2}) + (\frac{1}{4} + \frac{1}{4}) + (\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}) + ...$$

   Очевидно, что сумма в каждых скобках равна $\frac{1}{2}$. Данная сумма может быть сколь угодно большой, требуется лишь взять достаточно большое n. Так как каждое слагаемое предыдущей суммы больше или равно слагаемого последней суммы очевидно, что первая из сумм также может быть бесконечно большой. Еще нам потребуется несколько вспомогательных сумм, где p_n - самое большое простое число, n - количество простых чисел по нашему предположению.

$$(1) \quad \frac{1}{1} + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + ...$$

$$(2) \quad \frac{1}{1} + \frac{1}{3} + \frac{1}{9} + \frac{1}{27} + ...$$

$$(3) \quad \frac{1}{1} + \frac{1}{5} + \frac{1}{25} + \frac{1}{125} + ...$$

$$(4) \quad \frac{1}{1} + \frac{1}{7} + \frac{1}{49} + \frac{1}{343} + ...$$

$$...$$

$$(n) \quad \frac{1}{1} + \frac{1}{p_n} + \frac{1}{p_n^2} + \frac{1}{p_n^3} + ...$$

Анекдот. Бесконечное число математиков заходит в бар. Первый заказывает одно пиво. Второй – половину кружки, третий – четверть. Бармен говорит:
– Вот дурачьё!
...и наливает две кружки.

Каждая из данных сумм в терминах - **сходящийся ряд**, причем сумма (1) равна 2. Очевидно, что все оствшиеся суммы : (2), (3), (4), ..., (n) равны некоторому значению меньше 2.
Перемножим все имеющиеся суммы:

$$(\frac{1}{1}+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+...)\cdot(\frac{1}{1}+\frac{1}{3}+\frac{1}{9}+\frac{1}{27}+...)\cdot...\cdot(\frac{1}{1}+\frac{1}{p_n}+\frac{1}{p_n^2}+\frac{1}{p_n^3}+...)$$

Из вышеизложенного: каждый из множителей, кроме первого меньше 2, всего множителей n, тогда, очевидно, данное произведение **меньше** 2^n.
Раскрыв скобки, получим сумму, состоящую из слагаемых вида

$$\frac{1}{2^a\cdot 3^b\cdot 5^c\cdot ...\cdot p^z},$$

где знаменатель - все возможные комбинации простых чисел, причем в единственном *экземпляре*, тогда, согласно **Основной Теореме Арифметики**, в знаменателе какого-нибудь слагаемого найдется каждое натуральное число. Получается, что данное произведение равно сумме (*). Противоречие очевидно: сумма (*) может быть сколь угодно большой, а произведение ограничено сверху значением 2^n. Отсюда следует, что предположение об ограниченном количестве простых чисел неверно.
■

2.