

Элементы теории чисел

Механико-математический факультет МГУ

1 поток 1 курса, осень 2026г.

Лекция 6: Представление рациональных чисел
бесконечными десятичными дробями. Быстрый алгоритм
возведения в степень. Некоторые приложения в
криптографии. Построение больших простых чисел.

Основные определения и утверждения прошлой лекции

- Совокупность представителей всех классов вычетов по заданному модулю $m \geq 2$ называется *полной системой вычетов* по модулю m . Полная система состоит из m чисел.
- Любой набор представителей всех классов вычетов, состоящих из чисел, взаимно простых с модулем, называется *приведенной системой вычетов*. Приведённая система состоит из $\varphi(m)$ чисел.

Теорема

Пусть $a, m \geq 2$, – целые взаимно простые числа. Тогда

1. если x пробегает полную систему вычетов по модулю m , то $ax + b$, где b – любое целое число, также пробегает полную систему вычетов по модулю m ;
2. если x пробегает приведенную систему вычетов по модулю m , то ax также пробегает приведенную систему вычетов по этому модулю.

Основные определения и утверждения прошлой лекции

Теорема (Теорема Вильсона.)

Для любого простого числа p выполняется сравнение

$$(p - 1)! + 1 \equiv 0 \pmod{p}.$$

Теорема (Теорема Эйлера)

Если целое число a , взаимно просто с модулем m , то

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Теорема (Малая теорема Ферма)

Если целое число a не делится на простое число p , то

$$a^{p-1} \equiv 1 \pmod{p}.$$

§4.6. Рациональные числа и бесконечные десятичные дроби.

Рассмотрим представления рациональных чисел α бесконечными десятичными дробями, т.е. в виде рядов с целыми коэффициентами a_j

$$\alpha = a_0 + \sum_{k=1}^{\infty} \frac{a_k}{10^k} = a_0, a_1 a_2 \dots, \quad \text{и } 0 \leq a_k \leq 9 \text{ при } k \geq 1. \quad (1)$$

• Существует не более одного представления числа α в виде (1), содержащего бесконечное количество цифр, отличных от 9. Это следует из того, что

$$10^r \alpha = a_0 10^r + \dots + a_{r-1} 10 + a_r + \sum_{k=1}^{\infty} \frac{a_{r+k}}{10^k} = [10^r \alpha] + \{10^r \alpha\},$$

$$a_0 = [\alpha], \text{ и } a_r \equiv [10^r \alpha] \pmod{10}, \quad 0 \leq a_r < 10 \text{ при } r \geq 1.$$

Сумма ряда, соответствующего бесконечной периодической десятичной дроби есть рациональное число. Это достаточно доказать для чисто периодической дроби $\alpha = 0,(a_1a_2 \dots a_m)$. Обозначив $A = a_110^{m-1} + \dots + a_{m-1}10 + a_m$ и пользуясь формулой для суммы геометрической прогрессии, найдем

$$\begin{aligned}\alpha &= \sum_{k=0}^{\infty} 10^{-km} \left(\frac{a_1}{10} + \frac{a_2}{10^2} + \dots + \frac{a_m}{10^m} \right) = \\ &= A \sum_{k=0}^{\infty} 10^{-(k+1)m} = A \sum_{k=1}^{\infty} 10^{-km} = \frac{A \cdot 10^{-m}}{1 - 10^{-m}} = \frac{A}{10^m - 1}.\end{aligned}$$

- Заметим, что если при этом $\alpha = \frac{a}{b}$ – несократимое представление в виде отношения натуральных чисел, то $b \cdot A = a \cdot (10^m - 1)$ и $b \mid (10^m - 1)$, т.е. $10^m \equiv 1 \pmod{b}$.

Пусть теперь $\alpha = \frac{a}{b}$, где $0 < a < b$ и $(b, 10) = 1$. Обозначим буквой d показатель, которому принадлежит число 10 по модулю b . Тогда $10^d \equiv 1 \pmod{b}$ и с некоторым натуральным числом c выполняется равенство $10^d - 1 = bc$.

• Записав теперь $ac < 10^d - 1$ в десятичной системе счисления $B = ac = b_1 10^{d-1} + \dots + b_{d-1} 10 + b_d$, и действуя, как на предыдущем слайде, получим представление α в виде бесконечной периодической дроби

$$\frac{a}{b} = \frac{B}{10^d - 1} = \sum_{k=0}^{\infty} \frac{1}{10^{kd}} \left(\frac{b_1}{10} + \frac{b_2}{10^2} + \dots + \frac{b_d}{10^d} \right) = 0, (b_1 \dots b_d).$$

• Период в бесконечном десятичном разложении числа α записывается теми же цифрами, что и числитель в представлении $\alpha = \frac{B}{10^d - 1}$. При этом нужно иметь в виду, что период может начинаться с некоторого количества нулей, так $\frac{1}{99} = 0, (01)$.

Если рациональное число α больше единицы, числитель дроби $\alpha = \frac{a}{b}$, $(a, b) = 1$, можно представить в виде $a = bq + r$, $0 \leq r < b$ и разложив $\frac{r}{b}$ в бесконечную периодическую дробь, получим $\frac{a}{b} = q, (b_1 \dots b_d)$. При $r = 0$ имеем $\alpha = q = q, (0)$.

- Если знаменатель дроби $\frac{a}{b}$ не взаимно прост с 10, т.е. делится на 2 или на 5, то обозначив $k = \max(\nu_2(b), \nu_5(b))$, его можно умножить на такое натуральное число $u = 2^s 5^t$ (степень 2 или степень 5), что получится равенство $ub = 10^k v$, где $(v, 10) = 1$. Тогда

$$\frac{a}{b} = 10^{-k} \frac{ua}{v} = 10^{-k} \cdot c_0, (c_1 \dots c_m).$$

- Получившееся представление даёт конечную десятичную дробь в случае $v = 1$ и бесконечную периодическую дробь, если $v > 1$.

Заметим также, что в случае $(b, 10) = 1$, длина минимального периода равна показателю, которому принадлежит 10 по модулю b . Как доказано на прошлой лекции, длина периода в этом случае не превосходит $\varphi(b)$. Минимальную длину периода $\varphi(b)$ имеют, как можно проверить, рациональные числа со знаменателями

$$b = 7, 17, 19, 23, 29, 47, 49, 59, 61, 97.$$

Список исчерпывает все такие $b \leq 100$.

Пусть $\alpha = \frac{a}{b}$ – несократимое представление с $(b, 10) = 1$. Пусть также $\frac{a}{b} = 0, (b_1 \dots b_d)$ и $c \equiv 10a \pmod{b}$, $0 < c < b$. Тогда с некоторым целым q имеем

$$\frac{c}{b} = q + 10\frac{a}{b} = q + b_1 + 0, (b_2 \dots b_d b_1) = 0, (b_2 \dots b_d b_1).$$

Период дроби $\frac{c}{b}$ получается из периода $\frac{a}{b}$ циклическим сдвигом на одну позицию.

Если допустить в этом случае не чисто периодические разложения, то

$$\frac{c}{b} = 0, b_2 \dots b_d(b_1 b_2 \dots b_d)$$

и можно сказать, что бесконечные разложения дробей $\frac{a}{b}$ и $\frac{c}{b}$ имеют одинаковые периоды.

В частности, если показатель 10 по модулю b равен $\varphi(b)$, то бесконечные десятичные разложения всех дробей $\frac{a}{b}, 1 \leq a < b, (a, b) = 1$ имеют одинаковые периоды. Например,

$$\frac{1}{7} = 0, (142857)$$

$$\frac{2}{7} = 0, (285714),$$

$$\frac{3}{7} = 0, (428571)$$

$$\frac{4}{7} = 0, (571428),$$

$$\frac{5}{7} = 0, (714285)$$

$$\frac{6}{7} = 0, (857142).$$

§4.7. Быстрый алгоритм возведения в степень.

Простейший алгоритм для вычисления $a^d \pmod{N}$, последовательно умножающий на a результат предыдущего вычисления, требует $d - 1$ умножений. В действительности это вычисление можно провести намного быстрее.

- Вычислим, например, $2^{436} \pmod{437}$. Для краткости мы нигде не указываем модуль сравнения, равный 437:

$$\begin{array}{ll} 2^3 \equiv 4 \cdot 2 = 8, & 2^6 \equiv 8^2 = 64, \\ 2^{13} \equiv 64^2 \cdot 2 \equiv -111, & 2^{27} \equiv (-111)^2 \cdot 2 \equiv 170, \\ 2^{54} \equiv 170^2 \equiv 58, & 2^{109} \equiv 58^2 \cdot 2 \equiv 173, \\ 2^{218} \equiv 173^2 \equiv 213, & 2^{436} \equiv 213^2 \equiv 358. \end{array}$$

- Вычисления не раскладывают число 437 на множители, но доказывают, что оно составное. Действительно, $437 = 19 \cdot 23$.

Рассмотренный пример есть частный случай общего алгоритма.

Алгоритм 1

Данные: Целые числа $a, N > 1, d > 0$.

Найти: $a^d \pmod{N}$.

1. Представить d в двоичной системе счисления, т.е. найти такие цифры $d_j \in \{0, 1\}$, что

$$d = d_0 2^n + \dots + d_{n-1} 2 + d_n, \quad d_0 = 1.$$

2. Положить $a_0 = a$ и затем для $i = 1, \dots, n$ вычислить

$$a_i \equiv a_{i-1}^2 \cdot a^{d_i} \pmod{N}. \quad (2)$$

3. Положить $a^d \equiv a_n \pmod{N}$.

• В случае $d_i = 0$ алгоритм вычисляет $a_i \equiv a_{i-1}^2 \pmod{N}$, если же $d_i = 1$, то $a_i \equiv a_{i-1}^2 \cdot a \pmod{N}$.

Докажем теперь, что алгоритм работает правильно, и количество выполняемых им арифметических операций не очень велико.

Теорема 14

Алгоритм действительно вычисляет $a^d \pmod{N}$. Он использует для этого не более $2\lceil \log_2 d \rceil$ умножений по модулю N .

Доказательство.

При всех $i = 0, 1, \dots, n$ справедливы сравнения

$$a_i \equiv a^{d_0 2^i + \dots + d_i} \pmod{N}. \quad (3)$$

Докажем это индукцией по i . При $i = 0$ утверждение выполняется, т.к. $d_0 = 1$. Подставляя (3) в равенство $a_{i+1} = a_i^2 \cdot a^{d_{i+1}}$, находим равенство (3) для a_{i+1} . Это доказывает (3) для всех i . При $i = n$ получаем $a_n = a^d$, что доказывает правильность алгоритма. □

Доказательство второго утверждения теоремы.

Для доказательства второго утверждения обозначим символом $c(d)$ количество умножений по модулю N , необходимых алгоритму для вычисления $a^d \pmod{N}$. Докажем индукцией по d неравенство

$$c(d) \leq 2[\log_2 d]. \quad (4)$$

Обозначим для этого $m = d_0 2^{n-1} + \dots + d_{n-1}$. Тогда $d = 2m + d_n \geq 2m$.

При $d = 1$, 2 неравенство (4), очевидно, выполняется. Пусть теперь $d \geq 3$. В силу алгоритма справедливы соотношения

$$\begin{aligned} c(d) &= c(m) + 1 + d_n \leq c(m) + 2 \leq \\ &\leq 2[\log_2 m] + 2 = 2[\log_2 2m] \leq 2[\log_2 d], \end{aligned}$$

доказывающие нужное неравенство.

В первом пункте алгоритма нужно представить показатель степени d в двоичной системе счисления. Это можно сделать достаточно быстро. Положим $q_0 = d$ и обозначим через $q_1, q_2, \dots, q_n$ — частные при делении предыдущего числа q на 2. Тогда получаются следующие равенства

$$\begin{aligned}d = q_0 = 2q_1 + r_0, q_1 = 2q_2 + r_1, q_2 = 2q_3 + r_2, \dots, \\ q_{n-1} = 2q_n + r_{n-1}, q_n = 2q_{n+1} + r_n,\end{aligned}$$

где все остатки r_k удовлетворяют неравенствам $0 \leq r_k < 2$. Из этих условий следует, что $q_k \geq 2q_{k+1}$ и потому последовательность q_k убывает. Пусть n — наименьшее такое, что $q_n < 2$. Тогда $q_n = 1$ и $q_{n+1} = 0$.

Умножив каждое из равенств $q_k = 2q_{k+1} + r_k$ на 2^k при $k = 0, 1, \dots, n$, складывая получившиеся выражения и уничтожая одинаковые слагаемые в левой и правой частях, получаем

$$\sum_{k=0}^n q_k 2^k = \sum_{k=0}^n q_{k+1} 2^{k+1} + \sum_{k=0}^n r_k 2^k,$$

$$d = q_0 = 2^n r_n + 2^{n-1} r_{n-1} + \dots + 2^2 r_2 + 2r_1 + r_0.$$

Но это и есть двоичное представление числа d . Причём старшая цифра равняется последнему остатку, а цифры с меньшими номерами равны последовательно возникающим остаткам. Для согласования обозначений положим $d_k = r_{n-k}$.

• Пользуясь этим алгоритмом, например, находим

$$26 = 2 \cdot 13 + 0, \quad 13 = 6 \cdot 2 + 1, \quad 6 = 3 \cdot 2 + 0, \quad 3 = 1 \cdot 2 + 1, \quad 1 = 0 \cdot 2 + 1,$$

$$26 = (1, 1, 0, 1, 0)_2 = 2^4 + 2^3 + 2^1.$$

§4.7. Некоторые приложения в криптографии

Шифрование – это процесс преобразования осмысленного текста в бессмысленный, имеющий целью сокрытие информации исходного текста от несанкционированного доступа.

- Процесс должен быть обратимым, т.е. он должен допускать однозначное восстановление оригинального текста по его бессмысленному образу.
- Важным свойством этого преобразования является также наличие секретной информации (ключей), необходимой как для шифрования, так и для обратного преобразования – расшифрования. Злоумышленник, не знающий нужного ключа, не сможет ни зашифровать текст, ни расшифровать его образ. Знание же секретного ключа позволяет вычислять значения обратного отображения очень быстро.

В симметричных методах зашифрования и расшифрования сообщений применяется один и тот же ключ. Поэтому для безопасности передачи зашифрованного сообщения по открытым каналам необходимо предварительно обеим сторонам в тайне выработать единый ключ, и лишь после этого начинать обмен информацией.

- Во время Второй мировой войны Германия использовала шифровальную машину «Энигма» для защиты военных и дипломатических сообщений с помощью симметричного алгоритма. Ключи зашифрования и расшифрования были реализованы в виде настроек этой машины.
- Операторам шифровальных машин каждый месяц выдавался список ключей, в котором указывалось, как нужно настроить шифровальную машину на определённый день месяца, т.е. шифровальщики для безопасности меняли ключи каждый день.
- Идентичные списки ключей должны были выдаваться операторам отправителей и операторам получателей секретной информации.

При таком способе шифрования и большом объёме шифруемой информации возникают очевидные трудности, связанные с распределением ключей.

- Не очень простой и надёжный, но использовавшийся на практике способ решения этой проблемы – поручить доставку секретного ключа доверенному курьеру. Это можно сделать в армии и в условиях войны.
- Но при массовом появлении персональных компьютеров, лавинообразном увеличении пересылаемой личной информации, обмена информацией между банками, промышленными корпорациями, торговыми и другими организациями, ... устроить надёжную и безопасную связь для большого числа абонентов при таком распределении ключей невозможно.

Общая идея асимметричных методов заключается в том, что для зашифрования сообщения применяется один ключ, а для расшифрования – другой. Ключ для зашифрования открыто передается по любому каналу связи, в то время как ключ для расшифрования держится в секрете.

- Эти ключи (открытый и секретный), как правило связаны друг с другом некоторым соотношением. Но параметры этого соотношения подбираются такими, чтобы время, требуемое для построения секретного ключа по открытому, было несравнимо больше того времени, которое нужно для построения открытого ключа по секретному.
- Выбрав секретный ключ и построив по нему ключ открытый, можно безопасно передать его по открытому каналу связи. Ведь время вычисления секретного ключа по доступному всем открытому настолько велико, что к моменту вычисления секретного ключа и расшифрованию с его помощью отправленной информации она полностью потеряет свою актуальность.

Идея асимметричного шифрования и первые конструкции таких алгоритмов появились в конце 70-х годов прошлого века.

- Любая информация может быть закодирована последовательностью натуральных чисел. После кодирования процессы зашифрования и расшифрования информации представляются, как некоторые алгоритмы, перерабатывающие одни массивы целых чисел в другие.
- Участников обмена информацией, в ближайших примерах их будет двое, принято считать одушевлёнными лицами и присваивать им имена.
- Обычно легальных действующих лиц именуют Алиса и Боб. Их роль подобна латинским буквам a и b в описаниях алгебраических преобразований, злоумышленник получает имя Ева и так далее. Действующие лица могут быть и компьютерами, которые иногда для удобства описания наделяются чувствами и желаниями.

Алгоритм шифрования RSA

Допустим, что Боб хотел бы получать письма от Алисы, но так, чтобы никто не смог узнать их содержание. Для этого он

1. выбирает два простых числа p , q и вычисляет их произведение $N = pq$,
2. случайным образом выбирает два натуральных числа e , d , меньших $\varphi(N) = (p - 1)(q - 1)$, и удовлетворяющих сравнению

$$e \cdot d \equiv 1 \pmod{\varphi(N)}.$$

3. пересылает по открытой почте пару чисел (N, e) Алисе (открытый ключ Боба), но никому не сообщает свой секретный ключ – число d .

- Числа p и q также нужно держать в секрете, но они используются только на стадии генерации чисел N , e , d и впоследствии p , q могут быть уничтожены. Любые целые e и d , удовлетворяющие сравнению в п. 2, взаимно просты с $\varphi(N)$.

Зашифрование и расшифрование

Допустим, что секретное письмо x Алисы удовлетворяет условиям

$$1 < x < N, \quad (x, N) = 1.$$

Для того, чтобы **зашифровать** сообщение x , Алисе достаточно вычислить

$$y \equiv x^e \pmod{N}, \quad 0 < y < N. \quad (5)$$

• Число y представляет собой письмо Алисы в зашифрованном виде и может быть переслано Бобу через Интернет. Согласно теореме Эйлера справедливо сравнение

$$y^d \equiv x^{ed} = x \cdot x^{ed-1} \equiv x \pmod{N}. \quad (6)$$

• Боб, получив зашифрованное письмо Алисы y , находит **оригинал письма**

$$x \equiv y^d \pmod{N}, \quad 0 < x < N. \quad (7)$$

Если письмо Алисы по длине больше N , его можно разбить на блоки меньшей длины, чем N , и шифровать каждый блок отдельно. Если же письмо не взаимно просто с N , то к нему можно дописать время отправления или небольшой набор из нулей и единиц, чтобы обеспечить это условие.

- Возведение в степень по модулю, решение линейных сравнений с одной переменной выполняются сравнительно быстро. Для злодея сложность расшифрования письма с помощью алгоритма RSA зависит от сложности нахождения секретного ключа d . Последний может быть найден очень легко, если известно значение функции Эйлера $\varphi(N) = (p - 1)(q - 1)$. Но для этого нужно найти числа p, q , т.е. разложить число N на простые сомножители. Эта фундаментальная задача очень сложна.

- Для чисел N размером в 2048 битов при использовании самых мощных в настоящее время компьютеров требуются годы для её решения.

Числа Кармайкла.

Справедливы следующие утверждения:

1. Если наибольший общий делитель $(a, N) > 1$, то N — составное число.

2. Если $(a, N) = 1$ и $a^{N-1} \not\equiv 1 \pmod{N}$, то N — составное число.

• К сожалению, утверждений 1-2 не достаточно для доказательства того, что испытываемое число N — составное. Существуют составные числа, для которых выполняется сравнение $a^{N-1} \equiv 1 \pmod{N}$ при любом целом a , $(a, N) = 1$.

Определение 1

Составное число N называется числом Кармайкла, если при любом a , $(a, N) = 1$, выполняется сравнение

$$a^{N-1} \equiv 1 \pmod{N}.$$

$$N = 561 = 3 \cdot 11 \cdot 17.$$

Для каждого целого a , $(a, 561) = 1$, имеем
 $(a, 3) = (a, 11) = (a, 17) = 1$ и по малой теореме Ферма
выполняются сравнения

$$a^2 \equiv 1 \pmod{3}, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17}.$$

Так как 560 делится на 2, 10 и 16, то число $a^{560} - 1$ делится на каждую из разностей $a^2 - 1$, $a^{10} - 1$, $a^{16} - 1$. Значит, $a^{560} - 1$ делится на 3, 11, 17 и потому делится на произведение этих чисел, т.е. делится на 561. Число 561 есть число Кармайкла.

- В 1994г. было доказано, что множество чисел Кармайкла бесконечно. Существование чисел Кармайкла показывает необходимость уточнения свойств 1-2 для доказательства простоты чисел.

§4.8. Построение больших простых чисел.

Сейчас мы обсудим так называемые $(N - 1)$ - методы доказательства простоты чисел. Они позволяют, используя некоторую информацию о свойствах простых делителей числа $N - 1$, заключить, что N - простое число.

- Существуют также $(N + 1)$ и $(N^2 + 1)$ - методы, есть и другие обобщения излагаемых ниже идей, но мы их здесь не касаемся.

Теорема 15 (Лемер, Поклингтон)

Пусть N нечётно, $N - 1 = F \cdot R$, причём для каждого простого делителя q числа F с некоторым целым b выполнены условия

$$b^{N-1} \equiv 1 \pmod{N}, \quad \left(b^{(N-1)/q} - 1, N\right) = 1.$$

Тогда любой простой делитель p числа N удовлетворяет сравнению $p \equiv 1 \pmod{F}$.

$$b^{N-1} \equiv 1 \pmod{N}, \quad \left(b^{(N-1)/q} - 1, N\right) = 1. \quad (8)$$

Пусть p — простой делитель N , q — простой делитель F и b — число, удовлетворяющее (8). Первое из сравнений (8) означает, что b не делится на p . Обозначим $a = b^R$. Тогда a не делится на p и по малой теореме Ферма выполняется сравнение $a^{p-1} \equiv 1 \pmod{p}$. Обозначим буквой d показатель, которому число a принадлежит по модулю p . На прошлой лекции было доказано, что $d \mid p-1$ и, значит,

$$\nu_q(d) \leq \nu_q(p-1). \quad (9)$$

Доказательстве теоремы 15

Из (8) следует, что

$$a^F \equiv 1 \pmod{p}, \quad a^{F/q} \not\equiv 1 \pmod{p}.$$

Отсюда точно так же, как и (9) выводятся свойства $d|F$ и $d \nmid F/q$, что возможно лишь в случае, когда

$$\nu_q(F) = \nu_q(d). \quad (10)$$

Из (9) и (10) находим

$$\nu_q(F) = \nu_q(d) \leq \nu_q(p-1).$$

Так как последнее неравенство справедливо для любого простого делителя q числа F , то $F|p-1$ или $p \equiv 1 \pmod{F}$.

Следствие 1

Пусть F – простое нечётное число, R – чётное число, удовлетворяющие условиям $R \leq 4F + 2$ и $N = FR + 1$. Если

$$b^{N-1} \equiv 1 \pmod{N}, \quad (b^R - 1, N) = 1. \quad (11)$$

с некоторым целым b из промежутка $1 < b < N$, то N – простое число.

Доказательство.

Согласно теореме 15 при $q = F$ каждое простое p , делящее N удовлетворяет сравнению $p \equiv 1 \pmod{F}$. Кроме того, p нечетно, так что $p \equiv 1 \pmod{2F}$ и $p \geq 2F + 1$. Для составного N с некоторым простым $p|N$ имеем неравенства

$$(2F + 1)^2 \leq p^2 \leq N = FR + 1 \leq 4F^2 + 2F + 1,$$

что неверно. Значит, N — простое число. □

Предположим теперь, что построенное нечётное число N действительно является простым, и мы хотим доказать это с помощью Следствия 1. Если при выбранном b условия

$$b^{N-1} \equiv 1 \pmod{N}, \quad \left(b^{(N-1)/q} - 1, N\right) = 1. \quad (12)$$

нарушаются, нужно выбрать другое значение b и повторять эти операции до тех пор, пока такое число не будет обнаружено.

- Сколь долго придётся перебирать числа b , пока не будет найдено такое, для которого выполнены условия (12)?
- Для простого числа N первое условие (12), согласно малой теореме Ферма, будет выполняться всегда.
- Числа b , для которых нарушается второе условие (12), удовлетворяют сравнению $b^R \equiv 1 \pmod{N}$. В следующей главе будет доказано, что среди натуральных чисел x , $1 \leq x < N$, имеется не более R чисел, удовлетворяющих сравнению $x^R \equiv 1 \pmod{N}$. Поэтому на промежутке $1 \leq x < N$ имеется не более R чисел, для которых нарушаются условия (12).

Это означает, что, выбирая случайным образом число b на промежутке $1 \leq x < N$, при простом N можно с вероятностью большей, чем $\frac{N-1-R}{N-1} = 1 - F^{-1}$, найти число b , для которого будут выполнены условия следствия 1, и тем доказать, что N действительно является простым числом.

- Построенное таким способом простое число N будет удовлетворять неравенству $N > F^2$, т.е. будет записываться вдвое большим количеством цифр, чем исходное простое число F .
- Заменяв теперь число F на найденное простое число N и повторив с этим новым F все указанные выше действия, можно построить ещё большее простое число.
- Начав с какого-нибудь простого числа, скажем, записанного 10 десятичными цифрами (простоту его можно проверить, например, делением на маленькие табличные простые числа), и повторив указанную процедуру достаточное число раз, можно построить простые числа нужной величины.

Конец 6-й лекции