Дискретные корни и их криптографическое значение

А.А. Болотов, Е.А. Прохоренко

Введение

В данной статье рассматривается задача извлечения корней по простому и составному модулям, так называемых дискретных корней. Эта теоретико-числовая задача имеет важное прикладное значение в современной криптографии. Ее решение позволяет получить целый класс односторонних (криптографических) функций [2], широко используемых в защите информации [3, 4].

Первый параграф является предварительным и посвящен задаче вычисления дискретных корней. В этом параграфе ставится задача вычисления дискретных корней по простому модулю и анализируется ее решение. В параграфе приводятся необходимые вспомогательные теоретико-числовые факты о количестве и структуре решений поставленной задачи в различных случаях. В частности, рассматривается случай составного модуля.

Во втором параграфе приводятся алгоритмы нахождения дискретных корней по простому модулю. Сначала рассматривается детерминированный алгоритм. Хотя этот алгоритм был известен в теории чисел давно, – в отечественной литературе его можно найти, например, уже в издании 1952 года известного, много раз переиздававшегося учебника И.М. Виноградова «Основы теории чисел» в разделе задач, – считается, что в криптографию он был введен в 1977 году Л. Адлеманом, К. Мандерсом и Г. Миллером [5], которые дополнительно исследовали его с точки зрения теории сложности.

Затем в этом параграфе приводятся вероятностные алгоритмы для вычисления квадратных и кубических корней по простому модулю. Отметим, что вероятностный алгоритм нахождения квадратных корней известен специалистам [9], а соответствующий алгоритм для кубических корней разработан и исследован авторами статьи и впервые описывается в данной работе.

Изучение сложности этих алгоритмов является важным в криптографии, так как с ней напрямую связано быстродействие криптосистем, использующих в качестве криптографической функции теоретико-числовую функцию возведения в степень. В отличие от детерминированного алгоритма, соответствующий вероятностный алгоритм использует меньшее количество операций, что позволит заметно сократить время работы криптосистем. В третьем параграфе статьи доказываются теоремы об оценке вероятности успешного завершения работы вероятностных алгоритмов. Эти результаты являются новыми как для случая квадратных корней, так и для случая кубических. Проведенный в этом параграфе анализ позволяет убедиться в целесообразности использования предложенных вероятностных алгоритмов.

Третий параграф статьи посвящен криптографическому значению дискретных корней. В этом параграфе приводится важная теорема о равносильности (по сложности) задачи разложения составного модуля на простые множители и задачи извлечения корней по составному модулю. Этот факт, в случае квадратных корней, известен в криптографии как теорема Рабина [6], хотя, по-видимому, был известен еще Эйлеру. Мы даем доказательство обобщения этой теоремы на случай корней произвольной простой степени.

1. Основные понятия и определения. Дискретные корни

В этом параграфе ставится задача вычисления дискретных корней по простому модулю и анализируется ее решение. Не описывая пока самих алгоритмов нахождения дискретных корней, мы приводим необходимые вспомогательные теоретико-числовые факты о количестве и структуре решений поставленной задачи в различных случаях. Материал этого параграфа является предварительным.

1.1. Задача дискретных корней

Пусть имеется некоторое простое число p.

Число a является вычетом степени m по модулю p, если $\exists x:\ x^m = a(\mathrm{mod}\, p)$.

Число g_0 называется первообразным корнем по простому модулю p, если $\forall m_1, m_2\ \ g_0^{m_1} = g_0^{m_2}(\mathrm{mod}\, p) \Leftrightarrow m_1 = m_2(\mathrm{mod}\, p-1)$.

Заметим, что данное определение отличается от классического определения первообразного корня, которое дается в курсах теории чисел [1], но для простого модуля они являются эквивалентными.

Число $\mathrm{ind}\, a$ называется индексом (по-другому, дискретным логарифмом) числа a при основании g_0 по модулю p (где g_0 является первообразным корнем по модулю p), если $g_0^{\mathrm{ind}\, a} = a(\mathrm{mod}\, p)$.

Нетрудно показать, что a является вычетом степени m по модулю p, если $(m, p-1) | \mathrm{ind}\, a$.

Для некоторого m и для некоторого вычета a степени m будем называть число x дискретным корнем степени m по модулю p, если $x^m = a(\mathrm{mod}\, p)$. При этом задачу нахождения всех дискретных корней по модулю p мы называем задачей дискретных корней.

Отметим также следующее утверждение, известное в курсе теории чисел, как теорема Ферма.

Для простого p и для любого a не делящегося на p имеет место следующее сравнение

$$a^{p-1} = 1(\mathrm{mod}\, p).$$

1.2. Корни степени k, где k – простое

Рассмотрим задачу дискретных корней в случае, когда степень корня сама является простым числом k.

Итак, мы имеем уравнение

$$x^k = a(\mathrm{mod}\, p). \tag{1.2.1}$$

Тривиальный случай $a = 0(\mathrm{mod}\, p)$ мы будем исключать из рассмотрения.

Лемма 1.2.1. *Уравнение (1.2.1) имеет:*

а) одно решение, если $(k, p-1) = 1$;

б) не имеет решений, если $(k, p-1) = k$ *и* $a^{\frac{p-1}{k}} \neq 1(\mathrm{mod}\, p)$;

в) имеет k *решений, если* $(k, p-1) = k$ *и* $a^{\frac{p-1}{k}} = 1(\mathrm{mod}\, p)$.

Доказательство. а) Если $(k, p-1) = 1$, то $\exists u, v:\ uk + v(p-1) = 1$, тогда решением уравнения (1.2.1) будет $x = a^u(\mathrm{mod}\, p)$.

Действительно, $x^k = a^{uk} = a^{1-v(p-1)} = a(\mathrm{mod}\, p)$. Докажем, что других корней нет.

Пусть g_0 – некоторый первообразный корень. И пусть $x = g_0^l(\mathrm{mod}\, p)$. Предположим, что $y = g_0^m(\mathrm{mod}\, p)$ – другой корень. Тогда $x^k = y^k(\mathrm{mod}\, p)$, то есть $kl = km(\mathrm{mod}\, p-1)$. Но тогда $(p-1)|k(l-m)$, следовательно, так как $(k, p-1) = 1$, то $(p-1)|(l-m)$. Поэтому $g_0^l = g_0^m(\mathrm{mod}\, p)$.

б) Если x – решение, то $a^{\frac{p-1}{k}} = x^{k\frac{p-1}{k}} = x^{p-1} = 1(\mathrm{mod}\, p)$. Следовательно, решений нет.

в) Пусть g_0 – некоторый первообразный корень. И пусть $p-1 = kl$. Тогда имеем k различных корней из единицы: $1, g_0^l, g_0^{2l}, \ldots, g_0^{(k-1)l}$. Так как уравнение (1.2.1) не может иметь более чем k решений, то мы получили все корни из единицы.

Так как $a^{\frac{p-1}{k}} = 1(\mathrm{mod}\, p)$, то $g_0^{\mathrm{ind}\, a\frac{p-1}{k}} = 1(\mathrm{mod}\, p)$.

Следовательно, $(p-1)|(\mathrm{ind}\, a)\frac{p-1}{k} \Rightarrow k|\,\mathrm{ind}\, a \Rightarrow a$ вычет степени k.

Тогда $\exists x:\ x^k = a(\mathrm{mod}\, p)$. Таким образом, мы имеем k различных корней из a: $x, xg_0^l, xg_0^{2l}, \ldots, xg_0^{(p-1)l}$.

Так как уравнение (1.2.1) не может иметь более чем k решений, то мы получили все корни из a. Лемма доказана.

Остается выяснить, как можно получать корни из единицы по простому модулю p, не зная первообразного корня.

Если $(k, p-1) = 1$, то 1 – единственный корень из единицы. Если же $(k, p-1) = k$, то имеет место следующая лемма.

Лемма 1.2.2. *Возьмем некоторое* b *из кольца* $\mathbb{Z}_p$ *так, чтобы* $b^{\frac{p-1}{k}} \neq 1(\mathrm{mod}\, p)$. *Таких* b *в* $\mathbb{Z}_p$ *существует ровно* $\frac{k-1}{k}(p-1)$, *поэтому можно найти* b *простым перебором. Тогда* $1, g, g^2, \ldots, g^{(p-1)}$ – *различные корни из единицы, где* $g = b^{\frac{p-1}{k}}(\mathrm{mod}\, p)$.

Доказательство. Очевидно, что полученные числа являются корнями из единицы. Докажем, что все эти корни различны.

Предположим, что $g^l = 1(\mathrm{mod}\, p)$ для некоторого $l:\ 0 < l < k$. Пусть для некоторого первообразного корня g_0 имеем $b = g_0^t(\mathrm{mod}\, p)$. Тогда $(p-1)|l\frac{p-1}{k}t \Rightarrow k|lt$, но так как $(k, l) = 1$, то $k|t \Rightarrow b^{\frac{p-1}{k}} = g_0^{\frac{p-1}{k}t} = 1(\mathrm{mod}\, p)$, что противоречит выбору b.

Следовательно, все числа $g, g^2, \ldots, g^{(p-1)}$ отличны от единицы. Поэтому, предположив, что для некоторых $l, m:\ g^l = g^m(\mathrm{mod}\, p)$, при $l \neq m(\mathrm{mod}\, p-1)$, мы придем к противоречию, получив, что $g^{l-m} = 1(\mathrm{mod}\, p) \Rightarrow l - m = 0(\mathrm{mod}\, p-1)$. Отсюда следует, что все эти корни различны. Лемма доказана.

1.3. Квадратные и кубические корни

Рассмотрим два частных случая задачи дискретных корней по простому модулю $p \neq 2$ – степени $k = 2$ и $k = 3$. Поскольку далее в статье мы приводим вероятностные алгоритмы нахождения квадратных и кубических корней, целесообразно рассмотреть эти два случая отдельно.

Итак, для квадратных корней мы имеем уравнение

$$x^2 = a(\mathrm{mod}\, p). \tag{1.3.1}$$

Так как $p \neq 2$ – простое, то $(2, p-1) = 2$. Поэтому, согласно лемме (1.2.1), уравнение (1.3.1) либо не имеет решений, либо имеет два решения. Заметим, что случай $a = 0(\mathrm{mod}\, p)$ мы исключаем из рассмотрения.

Корнями из единицы будут, очевидно, числа 1 и -1. Поэтому, когда $a^{\frac{p-1}{2}} \neq 1(\mathrm{mod}\, p)$, уравнение не имеет решений, а при $a^{\frac{p-1}{2}} = 1(\mathrm{mod}\, p)$ имеет два решения $\pm x$.

Во втором случае имеем уравнение

$$x^3 = a(\mathrm{mod}\, p). \tag{1.3.2}$$

Пусть $(3, p-1) = d$ и $u, v:\ 3u + v(p-1) = d$. Если $d = 1$, то уравнение (1.3.2) имеет единственное решение: $x = a^u(\mathrm{mod}\, p)$.

Пусть $d = 3$. Тогда выберем некоторый кубический невычет b. Имеем три корня из единицы: $1, g, g^2$, где $g = b^{\frac{p-1}{3}}(\mathrm{mod}\, p)$. Итак, согласно лемме (1.2.1), при $a^{\frac{p-1}{3}} \neq 1(\mathrm{mod}\, p)$ корней нет, при $a^{\frac{p-1}{3}} = 1(\mathrm{mod}\, p)$ имеем три корня: x, xg, xg^2.

1.4. Корни произвольной степени

Умея решать задачу дискретных корней простой степени, мы можем сводить к ней задачу дискретных корней произвольной степени.

Рассмотрим уравнение

$$x^n = a(\mathrm{mod}\, p). \tag{1.4.1}$$

Пусть $(n, p-1) = d$, $p - 1 = md$ и $n = ld$.

Лемма 1.4.1. *Существует ровно d различных корней уравнения (1.4.1) при $a = 1$.*

Доказательство. Пусть g_0 – первообразный корень. Тогда $G = \{1, g_0^m, g_0^{2m}, \ldots, g_0^{(d-1)m}\}$ – различные корни из единицы. Докажем, что других корней нет. Предположим, что $c = g_0^L(\mathrm{mod}\, p)$ – корень из единицы. Тогда $(p-1)|nL \Rightarrow md|ldL$. Но так как $(m, l) = 1$ (иначе $(n, p-1) > d$), то $m|L$. Пусть $L = mT \Rightarrow g_0^L = g_0^{mT}(\mathrm{mod}\, p)$. Следовательно, $c \in G$. Лемма доказана.

Лемма 1.4.2. *Если a – вычет степени n, то существует ровно d различных корней уравнения (1.4.1).*

Доказательство. Так как a – вычет степени n, то $\exists x:\ x^n = a(\mathrm{mod}\, p)$. Тогда $X = \{x, xg_0^m, xg_0^{2m}, \ldots, xg_0^{(d-1)m}\}$ – различные корни

уравнения (1.4.1). Докажем, что других корней нет. Предположим, что y – тоже корень уравнения (1.4.1). Тогда $x^n = y^n(\mathrm{mod}\, p)$. Следовательно, $(yx^{-1}) \in G \Rightarrow y = g_0^{im}x(\mathrm{mod}\, p) \Rightarrow y \in X$. Лемма доказана.

Пусть $un + v(p-1) = d$. И пусть $a' = a^u(\mathrm{mod}\, p)$.

Лемма 1.4.3. *Если a – вычет степени n, то уравнение (1.4.1) равносильно уравнению*

$$x^d = a'(\mathrm{mod}\, p). \tag{1.4.2}$$

Доказательство.

(1.4.1) $\Rightarrow$ (1.4.2):

$$x^n = a(\mathrm{mod}\, p) \Rightarrow x^d = x^{un+v(p-1)} = x^{un} = a^u = a'(\mathrm{mod}\, p).$$

(1.4.1) $\Leftarrow$ (1.4.2):

Если a – вычет степени n, то a' является вычетом степени d. Поэтому уравнения (1.4.1) и (1.4.2) имеют ровно d корней. Кроме того, в силу ($\Rightarrow$), каждый корень (1.4.1) является также корнем и (1.4.2). Отсюда следует равносильность уравнений. Лемма доказана.

Заметим, что условие, что a – вычет степени n, в лемме имеет значение так как, если d делит uL (где $L = \mathrm{ind}\, a$) и не делит L, то уравнение (1.4.2) имеет d решений, а уравнение (1.4.1) – ни одного.

Итак, решая уравнение $x^n = a(\mathrm{mod}\, p)$, мы сводим его к уравнению $x^d = a'(\mathrm{mod}\, p)$ и, раскладывая d на простые множители, решаем поочередно задачи нахождения корней простой степени.

Пример. Найти корни уравнения $x^{12} = 7(\mathrm{mod}\, 19)$.
$(12, 18) = 6$; $-12 + 18 = 6$; $u = -1$;
$a' = 7^{-1} = 11(\mathrm{mod}\, 19)$;
$x^{12} = 7(\mathrm{mod}\, 19) \Leftrightarrow x^6 = 11(\mathrm{mod}\, 19)$;
Из уравнения $(x^3)^2 = 11(\mathrm{mod}\, 19)$ получаем два уравнения:
$x^3 = 7(\mathrm{mod}\, 19)$ и $x^3 = 12(\mathrm{mod}\, 19)$.
Отсюда получаем 6 корней: 4, 6, 9, 10, 13, 15.

2. Алгоритмы вычисления дискретных корней

В этом параграфе мы приводим алгоритмы, которые позволяют эффективно вычислять дискретные корни по простому модулю. Первый из них – детерминированный. В случае квадратных корней он известен в криптографии как теорема Адлемана [5], хотя (как уже отмечалось) его можно встретить и в более ранних работах [1, 8], в которых, однако, не оценивалась его сложность.

Второй и третий алгоритмы – вероятностные, вычисляющие квадратные и кубические корни по простому модулю соответственно. Алгоритм для кубических корней разработан авторами и приводится впервые.

Мы также даем оценки числа операций и вероятности успешного выбора, используемого в вероятностных алгоритмах.

2.1. Алгоритм быстрого возведения в степень

Приведем хорошо известный алгоритм модульного возведения многочлена в степень. Пусть у нас есть многочлен $r(x) = A_0 + A_1x + \ldots + A_{k-1}x^{k-1} (\mathrm{mod}\, p)$, где p – простое. И пусть известно, что $x^k = a (\mathrm{mod}\, p)$.

Требуется найти коэффициенты многочлена $r^t(x)$.

Разложим t в двоичную систему: $t = e_0 + e_1 2 + e_2 2^2 + \ldots + e_m 2^m$; $e_i \in \{0; 1\}$.

Найдем $r^2(x) = r(x)r(x)$, принимая во внимание, что $x^k = a (\mathrm{mod}\, p)$, и приводя подобные члены. То есть степень многочлена $r^2(x)$ не больше, чем $k - 1$.

Далее находим

$r^4(x) = r^2(x)r^2(x)$;

$r^8(x) = r^4(x)r^4(x)$ и так далее.

$r^t(x)$ есть произведение тех многочленов, степени которых входят в разложение t.

Аналогично возводятся в степень и числа. Отметим, что для этой задачи известны и более быстрые алгоритмы.

Примеры:

1) $k = 1$ – быстрое возведение в степень числа.
   $p = 13$; $t = 11$; $r(x) = x = 2$;
   $11 = 1 + 2 + 2^3$;
   $r = 2$;
   $r^2 = 4$;
   $r^4 = 4 \cdot 4 = 3(13)$;
   $r^8 = 3 \cdot 3 = 9(13)$;
   $r^{11} = rr^2r^8 = 2 \cdot 4 \cdot 9 = 7(13)$.

2) $k = 2$; $x^2 = 8(17)$;
   $p = 17$; $t = 14$; $r(x) = 2 + 3x$;
   $14 = 2 + 4 + 8$;
   $r(x) = 2 + 3x$;
   $r^2(x) = 4 + 12x + 9 \cdot 8 = 8 + 12x(17)$;
   $r^4(x) = 64 + 2 \cdot 8 \cdot 12x + 144 \cdot 8 = 9 + 5x(17)$;
   $r^8(x) = 81 + 90x + 25 \cdot 8 = 9 + 5x(17)$;
   $r^{14}(x) = r^2(x)r^4(x)r^8(x) = (8+12x)(9+5x)(9+5x) = 8+12x(17)$.

Оценим количество операций приведенного алгоритма. Если степень t порядка p, то приведенный алгоритм использует $\log p$ шагов. Для перемножения двух чисел порядка p классическим способом требуется $\log^2 p$ операций. Полагая, что $k \ll p$, имеем, что на каждом шаге совершается $O(1)$ умножений. Поэтому всего затрачивается $O(\log^3 p)$ операций. Более точная оценка возникает при использовании быстрых алгоритмов умножения.

2.2. Детерминированный алгоритм извлечения дискретных корней по простому модулю

Пусть даны некоторые простые p, k и имеется некоторый вычет a степени k по модулю p. Приведем алгоритм, который вычисляет

корни уравнения

$$x^k = a(\mathrm{mod}\, p) \qquad (2.2.1)$$

В первом параграфе было показано, что если k и $(p-1)$ взаимно просты, то уравнение (3.2.1) имеет единственный корень, который тривиально находится.

Пусть $p = k^t h + 1$, где $(h, p-1) = 1$ и $t > 0$.

Пусть $1, g, g^2, \ldots, g^{k-1}$ – корни из единицы, где $g = b^{\frac{p-1}{k}} \neq 1(\mathrm{mod}\, p)$ (см. Лемму 1.2.2).

Так как a – вычет степени k по модулю p, то $a^{\frac{p-1}{k}} = a^{k^{t-1}h} = 1(\mathrm{mod}\, p) \Rightarrow a^{k^{t-2}h} = g^i(\mathrm{mod}\, p)$. Через g^i будем обозначать некоторый корень из единицы. При некотором неотрицательном s_2 получим $a^{k^{t-2}h} b^{k^{t-1}h \cdot s_2} = 1(\mathrm{mod}\, p) \Rightarrow a^{k^{t-3}h} b^{k^{t-2}hs_2} = g^i(\mathrm{mod}\, p)$.

При некотором неотрицательном s_3
$a^{k^{t-3}h} b^{k^{t-2}h \cdot s_3} = 1(\mathrm{mod}\, p) \Rightarrow a^{k^{t-4}h} b^{k^{t-3}hs_3} = g^i(\mathrm{mod}\, p)$ и так далее.
Наконец, получим
$a^h b^{khs_k} = 1(\mathrm{mod}\, p) \Rightarrow a^{h+(p-1-h)} b^{khs_k} = a^{(p-1-h)}(\mathrm{mod}\, p) \Rightarrow$
$x^{(p-1-h)} = g^i a^{\frac{h+(p-1-h)}{k}} b^{hs_k} = g^i a^{\frac{p-1}{k}} b^{hs_k}(\mathrm{mod}\, p)$ и $(p-1-h, p-1) = 1$, откуда мы легко находим x.

Сложность этого алгоритма равна, очевидно, $O(\log^4 p)$. Но если число t много меньше чем $\log p$, то тогда число операций можно считать равным $O(\log^3 p)$.

2.3. Вероятностные алгоритмы для квадратных и кубических корней

Пусть решается уравнение

$$x^2 = a(\mathrm{mod}\, p), \qquad (2.3.1)$$

где a – квадратичный вычет, p – простое.

Возьмем некоторое число α из поля $\mathbb{Z}_p$ и вычислим $\frac{p-1}{2}$-ю степень многочленов $(\alpha + x)$ и $(\alpha - x)$ из $\mathbb{Z}_p[x]$ по модулю многочлена $P_2(x) = x^2 - a$ посредством алгоритма описанного выше.

Пусть $(\alpha + x)^{\frac{p-1}{2}} = A_0 + A_1 x(\mathrm{mod}\, x^2 - a)$.

Очевидно, что тогда $(\alpha - x)^{\frac{p-1}{2}} = A_0 - A_1 x(\mathrm{mod}\, x^2 - a)$.

Пусть теперь x является корнем уравнения (3.3.1). Тогда

$$(\alpha + x)^{\frac{p-1}{2}} = A_0 + A_1 x = e_0(\mathrm{mod}\, p), \qquad (2.3.2)$$

$$(\alpha - x)^{\frac{p-1}{2}} = A_0 - A_1 x = e_1(\mathrm{mod}\, p). \qquad (2.3.3)$$

Заметим, что значения e_0, e_1 мы не знаем, поэтому будем называть их виртуальными. Но, известно, что они могут принимать значения лишь из множества $\{0, 1, -1\}$. Если получится, что один из e_i равен нулю, то это значит, что мы сразу нашли решение. Поэтому будем считать, что e_i отличны от нуля.

Если e_0 и e_1 различны, то, сложив (1.3.2) и (1.3.3), получим, что $A_0 = 0(\mathrm{mod}\, p)$ и тогда $x = \pm A_1^{-1}(\mathrm{mod}\, p)$.

В противном случае выбираем новое α до тех пор, пока не получим $A_0 = 0(\mathrm{mod}\, p)$, то есть пока e_0 и e_1 не будут различны.

В дальнейшем мы докажем, что вероятность того, что для некоторого выбранного α мы получим $A_0 = 0(\mathrm{mod}\, p)$, больше чем $1/2$.

Пусть теперь решается уравнение

$$x^3 = a(\mathrm{mod}\, p), \qquad (2.3.4)$$

где a – кубический вычет, p – простое.

Если 3 не делит $(p-1)$, тогда по алгоритму Евклида находим такие u и v, что $3u + (p-1)v = 1$. И затем находим x по формуле:

$$x = x^{1-(p-1)v} = x^{3u} = a^u(\mathrm{mod}\, p).$$

Поэтому мы будем решать уравнение (3.3.4) в случае, когда корень находится не так просто, то есть когда $3|(p-1)$.

Будем считать, что нам известны кубические корни из единицы: $1, g, g^2$ (см. лемму 1.2.2). Отметим сразу, что если нам требуется найти один корень уравнения (2.3.4) то находить корни из единицы нам не нужно.

Возьмем некоторое число α из поля $\mathbb{Z}_p$ и, считая x корнем уравнения (2.3.4), будем анализировать систему:

$$(\alpha + x)^{\frac{p-1}{3}} = A_0 + A_1 x + A_2 x^2 = e_0(\mathrm{mod}\, p); \qquad (2.3.5)$$

$$(\alpha + gx)^{\frac{p-1}{3}} = A_0 + A_1 gx + A_2 g^2 x^2 = e_1 (\mathrm{mod}\, p); \qquad (2.3.6)$$

$$(\alpha + g^2 x)^{\frac{p-1}{3}} = A_0 + A_1 g^2 x + A_2 g x^2 = e_2 (\mathrm{mod}\, p); \qquad (2.3.7)$$

где A_0, A_1, A_2 находим аналогично случаю квадратных корней, возводя многочлен $(\alpha + x)$ из $\mathbb{Z}_p[x]$ в $\frac{p-1}{3}$-ю степень по модулю многочлена $P_2(x) = x^3 - a$.

Как и для квадратных корней будем считать, что виртуальные значения e_i отличны от нуля. В противном случае мы сразу определяем решение. То есть e_0, e_1, e_2 могут принимать значения только из множества корней из единицы $\{1, g, g^2\}$.

Лемма 2.3.1. $A_0 = 0 \Leftrightarrow e_0, e_1, e_2$ различны.

Доказательство. ($\Leftarrow$) Сложив (2.3.5), (2.3.6) и (2.3.7) и пользуясь тем, что сумма всех корней из единицы равна нулю (лемма 3.2.1), имеем $3A_0 = 0 (\mathrm{mod}\, p)$.

($\Rightarrow$) Сложив (2.3.5), (2.3.6) и (2.3.7), имеем

$$e_0 + e_1 + e_2 = 0 (\mathrm{mod}\, p).$$

Предположим, что из e_0, e_1, e_2 существуют хотя бы два одинаковых значения. Если одинаковы все три значения, то тогда получаем, что один из корней из единицы есть ноль. Если одинаковы только два значения, то, без ограничения общности, будем считать, что $e_0 = e_1 = 1$ и $e_2 = g$. Тогда $e_0 + e_1 + e_2 = 2 + (-1 - g^2) = 1 - g^2 = 0 (\mathrm{mod}\, p) \Rightarrow g^2 = 1 (\mathrm{mod}\, p)$; что противоречит выбору g. Лемма доказана.

Случай 1. $A_0 = 0$.

$$(*) \quad \begin{cases} A_1 x + A_2 x^2 = e_0 (\mathrm{mod}\, p) & (1) \\ A_1 gx + A_2 g^2 x^2 = e_1 (\mathrm{mod}\, p) & (2) \\ A_1 g^2 x + A_2 gx^2 = e_2 (\mathrm{mod}\, p) & (3) \end{cases}$$

Лемма 2.3.2. *Случай 1 ограничивается двумя вариантами:*

$$1a)\ e_0 = 1;\ e_1 = g;\ e_2 = g^2;$$

$$1b)\ e_0 = g^2;\ e_1 = g;\ e_2 = 1^2;$$

Доказательство. Заметим, что при замене уравнения переходят друг в друга по схеме:

$x \to gx$ $\quad (1) \to (2) \to (3) \to (1)$;

$x \to g^2 x$ $\quad (1) \to (3) \to (2) \to (1)$.

Решая систему $(*)$ мы получим лишь другой корень.

Далее проведем доказательство с помощью таблицы:

e_0	e_1	e_2	Замена	Переход из исходного случая	Случай
1	g	g^2	$x \to x$	...	1a
1	g^2	g	$x \to g^2 x$	$(1) \to (3) \to (2) \to (1)$	1b
g	1	g^2	$x \to gx$	$(1) \to (2) \to (3) \to (1)$	1b
g	g^2	1	$x \to gx$	$(1) \to (2) \to (3) \to (1)$	1a
g^2	1	g	$x \to g^2 x$	$(1) \to (3) \to (2) \to (1)$	1a
g^2	g	1	$x \to x$	...	1b

Лемма доказана.

Случай 1a). Умножим (1) на g и вычтем из (2). Получим, что $A_2 = 0 \Rightarrow x = A_1^{-1} (\mathrm{mod}\, p)$ – корень.

Случай 1b). Умножим (3) на g и вычтем из (2). Получим, что $A_1 = 0 \Rightarrow A_2 x^2 = g^2 (\mathrm{mod}\, p)$. Умножая на gx, имеем $x = A_2 ag (\mathrm{mod}\, p)$.

Случай 2. $A_0 \neq 0$.

Случай 2.1). $\exists$ только два уравнения, у которых совпадают e_i.

Лемма 2.3.3. *Случай 2.1) ограничивается двумя вариантами:*

$$2.1a)\ e_0 = e_1 \neq e_2$$

$$2.1b)\ e_0 = e_2 \neq e_1$$

Доказательство. Оставшийся случай 2.1c) $e_1 = e_2 \neq e_0$ получаем из 2.1a) заменой $x \to gx$. Лемма доказана.

2.1a) Вычитая из уравнения (2) уравнение (1), получаем

$$A_1 (g - 1)x + A_2 (g^2 - 1)x^2 = 0 (\mathrm{mod}\, p)$$

$\Rightarrow A_1 + A_2(g+1)x = 0(\mathrm{mod}\, p)$
$\Rightarrow A_1 - A_2 g^2 x = 0(\mathrm{mod}\, p)$
$\Rightarrow x = A_1 A_2^{-1} g(\mathrm{mod}\, p)$

2.1b) Вычитая из уравнения (3) уравнение (1), получаем $A_1(g^2-1)x + A_2(g-1)x^2 = 0(\mathrm{mod}\, p)$
$\Rightarrow -A_1 g^2 + A_2 x = 0(\mathrm{mod}\, p)$
$\Rightarrow A_1 - A_2 g x = 0(\mathrm{mod}\, p)$
$\Rightarrow x = A_1 A_2^{-1} g^2(\mathrm{mod}\, p)$

Случай 2.2). $e_0 = e_1 = e_2 \Rightarrow A_1 = A_2 = 0$ – не успех. Берем другое α и повторяем алгоритм.

Замечание. В случае 2 $A_1 = 0 \Rightarrow A_2 = 0$ ($A_2 = 0 \Rightarrow A_1 = 0$). Но так как $e_0 \neq e_1$ ($e_1 \neq e_2$; $e_0 \neq e_2$), то, вычитая из (1) (2) (из (2) (3); из (1) (3)), получаем, что такой случай невозможен.

В первом случае A_1 и A_2 не могут быть одновременно равны нулю.

Таким образом, имеем следующую таблицу для нахождения x:

$A_0 = 0$	$A_1 = 0$	$x = aA_2(\mathrm{mod}\, p)$
$A_0 = 0$	$A_2 = 0$	$x = A_2^{-1}(\mathrm{mod}\, p)$
$A_0 \neq 0$	$A_1 \neq 0$ и $A_1 \neq 0$	$x = A_1 A_2^{-1}(\mathrm{mod}\, p)$
$A_0 \neq 0$	$A_1 = A_2 = 0$	не успех

2.4. Оценки вероятностей

Оценим теперь вероятности удачного выбора α для каждого из приведенных вероятностных алгоритмов.

Теорема 2.4.1. *Вероятность удачного выбора α для вероятностного алгоритма нахождения квадратных корней больше* $1/2$.

Доказательство. Найдем количество различных пар $(z_1; z_2)$, таких, что $z_1 = \alpha + x(\mathrm{mod}\, p)$, $z_2 = \alpha - x(\mathrm{mod}\, p)$ – одновременно являются вычетами или невычетами и таких что $\alpha \neq 0$ и $x \neq 0$.

$$\alpha = (z_1 + z_2)2^{-1}(\mathrm{mod}\, p);$$
$$x = (z_1 - z_2)2^{-1}(\mathrm{mod}\, p).$$

Для каждого z_1 – вычета $-z_1$ также будет вычетом, если $4|(p-1)$. Поэтому в этом случае имеем $\frac{p-1}{2}(\frac{p-1}{2} - 2)$ комбинаций. Аналогично для невычетов. Всего получаем $\frac{(p-1)(p-5)}{2}$ комбинаций, если $4|(p-1)$, и $\frac{(p-1)(p-3)}{2}$ в противном случае.

Очевидно, что различным парам $(z_1; z_2)$ соответствуют различные пары (α, x). То есть всего существует $\frac{(p-1)(p-5)}{2}$ неудачных пар (α, x), если $4|(p-1)$, и $\frac{(p-1)(p-3)}{2}$ в противном случае. Докажем теперь, что для каждого фиксированного x таких пар одинаковое количество.

Пусть $K_x = \{(\alpha, x) : (\alpha + x)$ и $(\alpha - x)$ – одновременно вычеты или невычеты$\}$.

Построим соответствие между классами K_x и K_y. $\Omega : (\alpha, x) \to (\alpha \cdot l, xl)$, где l находим из равенства $xl = y(\mathrm{mod}\, p)$. Очевидно, что если $(\alpha+x)$ и $(\alpha-x)$ – одновременно вычеты, то и $(\alpha+x)l$ и $(\alpha-x)l$ – одновременно вычеты. Аналогично для невычетов.

Следовательно, $(\alpha \cdot l, xl) \in K_y$. Таким образом, мы получили взаимооднозначное соответствие. То есть $|K_x| = |K_y|$ для любых x, y. Поэтому для любого x $|K_x| = \frac{(p-5)}{2}$ или $\frac{(p-3)}{2}$.

Окончательно получаем, что для каждого x существует:
a) $\frac{(p-5)}{2}$ неудачных α, если $4|(p-1)$;
b) $\frac{(p-3)}{2}$ неудачных α в противном случае.
Всего мы можем выбирать α из $p-1$ числа. Отсюда следует требуемая оценка.

Теорема 2.4.2. *Вероятность удачного выбора α для вероятностного алгоритма нахождения кубических корней больше* $2/3$.

Доказательство. Найдем количество различных троек $(z_1; z_2; z_3)$, таких, что $z_1 = \alpha + x(\mathrm{mod}\, p)$, $z_2 = \alpha + gx(\mathrm{mod}\, p)$, $z_3 = \alpha + g^2 x(\mathrm{mod}\, p)$ одновременно являются вычетами или невычетами по одному и тому же корню из единицы (то есть $z_1^{\frac{(p-1)}{3}} = z_2^{\frac{(p-1)}{3}} = z_3^{\frac{(p-1)}{3}} (\mathrm{mod}\, p)$), и таких, что $\alpha \neq 0$ и $x \neq 0$.

$$z_3 = (-g)(z_1 + gz_2)(\mathrm{mod}\, p);$$
$$\alpha = (z_2 - gz_1)(1-g)^{-1}(\mathrm{mod}\, p);$$

$$x = (z_1 - z_2)(1 - g)^{-1} (\mathrm{mod}\, p).$$

Определим количество различных пар $(z_1; z_2)$, таких, что $z_1 = \alpha + x (\mathrm{mod}\, p)$, $z_2 = \alpha + gx (\mathrm{mod}\, p)$ одновременно являются вычетами или невычетами по одному и тому же корню из единицы, и таких, что $\alpha \neq 0$, $x \neq 0$ и $z_3 \neq 0$ (z_3 однозначно определяется по z_1 и z_2). Тогда, очевидно, число аналогичных троек будет не более этого количества.

Для каждого z_1 – вычета gz_1 и $-g^2 z_1$ также будут вычетами, если $9|(p-1)$. Поэтому в этом случае имеем $\frac{(p-1)}{3}(\frac{(p-1)}{3} - 3)$ комбинаций. Аналогично для невычетов. Всего получаем $\frac{(p-1)(p-10)}{3}$ комбинаций, если $9|(p-1)$, и $\frac{(p-1)(p-4)}{3}$ в противном случае.

Очевидно, что различным парам $(z_1; z_2)$ соответствуют различные пары (α, x). То есть всего существует менее чем $\frac{(p-1)(p-10)}{3}$ неудачных пар (α, x), если $9|(p-1)$, и менее чем $\frac{(p-1)(p-4)}{3}$ в противном случае. Так же, как и в предыдущей теореме, доказывается, что для каждого фиксированного x таких пар одинаковое количество.

Окончательно получаем, что для каждого x существует менее чем:
a) $\frac{(p-10)}{3}$ неудачных α, если $4|(p-1)$;
b) $\frac{(p-4)}{3}$ неудачных α в противном случае.
Всего мы можем выбирать α из $p-1$ числа. Отсюда следует требуемая оценка.

Нетрудно заметить, что при одном выполнении оба алгоритма используют лишь $O(\log^3 p)$ операций, то есть они значительно лучше, чем детерминированный алгоритм, с точки зрения теории сложности.

3. Криптографический случай. Дискретные корни по составному модулю $n = pq$

Этот параграф посвящен криптографическому значению дискретных корней. Здесь определяется понятие криптографической

функции, а также дается доказательство важной теоремы о равносильности по сложности задачи разложения составного модуля на множители и задачи нахождения дискретных корней. Заметим, что задачи считаются равносильными по сложности в том случае, если решение одной дает эффективное решение другой, и наоборот.

3.1. Односторонние и криптографические функции

Большую роль в криптографии с открытым ключом играют функции, обратные которых являются трудновычислимыми с точки зрения теории сложности [7]. Такие функции называются односторонними [2].

Определение. Функция $f : X \to Y$ называется криптографической, если существует некоторая дополнительная (секретная) информация, при наличии которой f не является односторонней, а при отсутствии – является.

Приведем пример криптографической функции. Пусть p и q – достаточно большие простые числа. В криптографии часто рассматривается случай, когда модуль n берется равным pq.

Функция $f(x) = x^2 (\mathrm{mod}\, n)$ – криптографическая функция, секретом в которой является разложение n на p и q. Напомним, что при $n > 2^{1000}$ эта задача является на сегодняшний день практически неосуществимой.

В предыдущем параграфе было показано, что задача извлечения дискретных корней по простому модулю эффективно решается. Поэтому, если нам известны p и q, то мы находим четыре значения функции $f^{-1}(x^2) (\mathrm{mod}\, n)$, пользуясь китайской теоремой об остатках [1]. С другой стороны, если нам известны четыре различных корня $\pm x$ и $\pm y$ уравнения $x^2 = a (\mathrm{mod}\, n)$, тогда $(x-y)(x+y) = 0 (\mathrm{mod}\, n)$, и $(x-y, n) = p$ или q, так как $x - y \neq 0 (\mathrm{mod}\, n)$. Этот факт известен в криптографии как теорема Рабина [6].

Перейдем к доказательству аналогичного утверждения, но уже в более общем случае корней произвольной простой степени.

3.2. Равносильность задач нахождения дискретных корней по составному модулю $n = pq$ и задачи разложения n на множители

Рассмотрим уравнение

$$x^k = a(\mathrm{mod}\, n), \tag{3.2.1}$$

где $n = pq$, p, q, k – простые.

Пусть g – некоторый корень из единицы.

$g_p := g(\mathrm{mod}\, p)$ – корень из единицы по модулю p;

$g_q := g(\mathrm{mod}\, q)$ – корень из единицы по модулю q.

Лемма 3.2.1. *Если* $g_p \neq 1(\mathrm{mod}\, p)$ *и* $g_q \neq 1(\mathrm{mod}\, q)$, *то* $S = \sum_{i=0}^{k-1} g^i = 0(\mathrm{mod}\, n)$.

Доказательство. Рассмотрим сумму $S_p = 1 + g_p + \ldots + g_p^{k-1}(\mathrm{mod}\, p)$. Умножим обе части на g_p. Тогда слева сумма не изменится. Следовательно, $(g_p - 1)S_p = 0(\mathrm{mod}\, p)$. Но так как $g_p \neq 1(\mathrm{mod}\, p)$ и p – простое, то $S_p = 0(\mathrm{mod}\, p)$. Аналогично, $S_q = 0(\mathrm{mod}\, q)$. Следовательно, $S = 0(\mathrm{mod}\, n)$. Лемма доказана.

Теорема 3.2.2. *Задача разложения* n *на простые множители равносильна по сложности задаче нахождения всех корней уравнения (3.2.1) в случае, если существует более чем один корень этого уравнения.*

Замечание. Если уравнение (3.2.1) имеет единственное решение, то равносильность задач разложения модуля на простые делители и нахождения единственного корня уравнения (3.2.1) позволило бы разлагать на множители любой составной модуль.

Действительно, предположим нам известен алгоритм, который по двум числам x и a, таким что $x^k = a(\mathrm{mod}\, n)$, определяет разложение n на простые p и q. Тогда, выбирая произвольное x, мы вычисляем $a = x^k(\mathrm{mod}\, n)$ и с помощью этого виртуального алгоритма находим p и q.

Доказательство. Зная разложение $n = pq$, мы, решая сначала уравнение (3.2.1) по модулю p и q отдельно, находим все корни, объединяя полученные решения по китайской теореме об остатках.

Теперь рассмотрим обратную задачу. Пусть нам известны все решения уравнения (3.2.1). Исключив из рассмотрения случай, когда уравнение имеет одно решение, нам осталось рассмотреть два случая:

1. Уравнение (3.2.1) имеет k решений. То есть $(k,(p-1))(k,(q-1)) = k$.
2. Уравнение (3.2.1) имеет k^2 решений. То есть $(k,(p-1))(k,(q-1)) = k^2$.

Возьмем из множества решений уравнения (3.2.1) два различных корня x и z. Тогда $g = xz^{-1}(\mathrm{mod}\, n)$, будет являться корнем из единицы по модулю n. Причем, так как $x \neq z(\mathrm{mod}\, n)$, в силу выбора корней, то $g \neq 1(\mathrm{mod}\, n)$. Тогда мы знаем k различных корней уравнения (3.2.1) – $x, gx, g^2x, \ldots, g^{k-2}x, g^{k-1}x = z(\mathrm{mod}\, n)$. Это следует из условия простоты k и $g \neq 1(\mathrm{mod}\, n)$.

Пусть

$g_p := g(\mathrm{mod}\, p)$ – корень из единицы по модулю p;

$g_q := g(\mathrm{mod}\, q)$ – корень из единицы по модулю q;

$S = 1 + g + \ldots + g^{k-1}(\mathrm{mod}\, n)$ – сумма корней из единицы по модулю n;

$S_p = 1 + g_p + \ldots + g_p^{k-1}(\mathrm{mod}\, p)$ – сумма корней из единицы по модулю p;

$S_q = 1 + g_q + \ldots + g_q^{k-1}(\mathrm{mod}\, q)$ – сумма корней из единицы по модулю q.

В первом случае положим для определенности, что $k|(p-1)$ и $k|(q-1)$. Тогда $g_q = 1(\mathrm{mod}\, q)$ и, так как $g \neq 1(\mathrm{mod}\, n)$, то $g_p \neq 1(\mathrm{mod}\, p)$.

Следовательно, $S_p = 0(\mathrm{mod}\, p)$ и $S_q = k(\mathrm{mod}\, q)$. По китайской теореме об остатках имеем $S = S_p vq + S_q up = kup(\mathrm{mod}\, n)$, где $u = p^{-1}(\mathrm{mod}\, q)$ и $v = q^{-1}(\mathrm{mod}\, p)$.

Так как значение S мы знаем, то разложение n мы получаем с помощью алгоритма Евклида, находя наибольший общий делитель:

$$(S, n) = (kup, n) = p.$$

Во втором случае имеем $k|(p-1)$ и $k|(q-1)$. Если один из g_p или g_q равен единице по модулям p и q соответственно (одновременное равенство единице невозможно, так как $g \neq 1(\mathrm{mod}\, n)$), то мы находим разложение также как и в первом случае.

Поэтому, будем считать, что $g_p \neq 1(\mathrm{mod}\, p)$ и $g_q \neq 1(\mathrm{mod}\, q)$. Но

тогда, по лемме 3.2.1, $S = \sum_{i=0}^{k-1} g^i = 0(\mathrm{mod}\, n)$.

Выберем из множества решений уравнения (2.2.1) корень y так, чтобы $y \neq xg^i(\mathrm{mod}\, n)$ $i = 0, 1, \ldots, k-1$.

Рассмотрим произведение:

$\Pi = (y-x)(y-gx)\ldots(y-g^{k-1}x) = y^k + (-1)^i \sum_{i=0}^{k-1} y^{k-i}x^iT_i + (-1)^k g^{1+2+\ldots+(k-1)}x^k(\mathrm{mod}\, n)$, где T_i – сумма всевозможных i произведений из набора $\{1, g, g^2, \ldots, g^{k-1}\}$ без повторений.

Заметим, что в поле рассматриваемое произведение, очевидно, равно $\Pi = y^k - x^k$. Это следует из того, что в поле многочлен $P(y) = y^k - x^k$, имеющий k различных корней, а именно $x, gx, g^2x, \ldots, g^{k-2}x, g^{k-1}x$, раскладывается в произведение $P(y) = (y-x)(y-gx)\ldots(y-g^{k-1}x)$.

Докажем, аналогичное утверждение для кольца методом прямой проверки.

Очевидно, что в T_i имеется C_i^k слагаемых.

Так как k – простое, то $(-1)^k g^{1+2+\ldots+(k-1)} = g^{\frac{k(k-1)}{2}} = -1(\mathrm{mod}\, n)$ и $k|C_i^k$.

Докажем, что при приведении подобных слагаемых T_i примет вид: $T_i = \frac{C_i^k}{k}(1 + g + g^2 + \ldots + g^{k-1})(\mathrm{mod}\, n)$, то есть что каждая степень встретится одинаковое количество раз.

Обозначим за K_{it} множество всевозможных i произведений из набора $\{1, g, g^2, \ldots, g^{k-1}\}$ без повторений, сумма степеней которых равна t.

Построим соответствие Ψ_{tw} : $K_{it} \Leftrightarrow K_{iw}$ по правилу $\Psi_{tw}(g^a g^b g^c \ldots g^s) = g^{a+l} g^{b+l} g^{c+l} \ldots g^{s+l} = g^a g^b g^c \ldots g^s g^{il} = g^{t+il}(\mathrm{mod}\, n)$, где l однозначно находится из условия $t + il = w(\mathrm{mod}\, k)$.

Так как k – простое, то Ψ_{tw} является взаимооднозначным соответствием. Поэтому для любых t, w $|K_{it}| = |K_{iw}|$, откуда и следует выражение для T_i.

Из выбора g имеем, что $\forall i$: $0 < i < k$ $T_i = 0(\mathrm{mod}\, n) \Rightarrow \Pi = y^k - x^k = 0(\mathrm{mod}\, n)$.

Но из выбора y мы получаем, что ни один из множителей Π не равен нулю по модулю n. Следовательно, $\exists i, j$: $((y - g^i x), n) = p$ или $((y - g^j x), n) = q$. То есть мы получили разложение n. Теорема доказана.

Заключение

Подведем итоги полученных результатов.

В статье подробно рассмотрена задача извлечения дискретных корней по простому и составному модулям. Взяв в качестве модуля n произведение двух простых чисел, мы получаем криптографическую функцию

$$f(x) = x^k(\mathrm{mod}\, n).$$

Секретной информацией в этом случае является разложение n на простые множители p и q. Действительно, из теоремы 3.2.2 следует, что если мы не знаем разложения n, то мы не сможем вычислять обратные значения функции. И наоборот, если мы не можем найти обратные значения функции, то мы не знаем p и q. С этой точки зрения задача поставлена корректно.

Если же нам известно разложение модуля на простые, то мы решаем задачу раздельно для модулей p и q, а затем по китайской теореме об остатках определяем решения по составному модулю. Для этого нужно воспользоваться алгоритмом извлечения корней по простому модулю.

Для вычисления корней по простому модулю мы можем применять:

– вероятностный алгоритм в случае, когда $k = 2$ или $k = 3$. При этом вероятность успешного завершения алгоритма с первой попытки будет соответственно больше, чем $1/2$ или $2/3$, а количество операций будет порядка $\log^3 p$;

– детерминированный алгоритм в случае, когда $k > 3$ или же когда значение модуля без единицы содержит в своем разложении маленькую степень числа k. Сложность детерминированного алгоритма будет порядка $\log^4 p$.

Список литературы

[1] Виноградов И.М. Основы теории чисел. М.: Наука, 1965.

[2] Diffie W., Hellmann M. New directions in cryptography // IEEE Transaction on Information Theory IT-22. 1976.

[3] Саломаа А. Криптография с открытым ключом. М.: Мир, 1996.

[4] Stinson D.R. Cryptography: Theory and Practice. CRC Press, 1995.

[5] Adleman L., Manders K., Miller G. On Taking Roots in Finite Fields // 20th IEEE FOCS. Vol. 20. 1977.

[6] Rabin M.O. Digitalized Signatures and Public Key Functions as Intractable as factorization // MIT Laboratory for Computer Science. January, 1979. TR 212.

[7] Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

[8] Berlekamp E.R. Factoring Polynomials over Large Finite Fields // Mathematics of Computation. Vol. 24. 1970.

[9] Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. CRC Press, 1999.

Обзор основных нейросетевых моделей

В.В. Псиола

Введение

Людей всегда интересовало собственное мышление, устройство нервной системы. Уже в конце средних веков ученые имели общее представление о нервной системе человека. Во второй половине XIX века существовали две школы: ретикуларисты (reticularists) – считавшие, что нервная система представляет сеть из непрерывных нервных волокон, покрывающая все тело человека, и нейронисты (neuronists) – считавшие, что существует огромное число отдельных связанных клеток – нейронов.

В 1880 году К. Голди (Camilo Goldi) разработал новую технику окрашивания нервных волокон, и в 1888 доктор С.Р. Каджал (Santiago Ramon y Cajal) с помощью этой техники доказал несостоятельность модели ретикуларистов. В 1906 Голди и Каджал получили нобелевскую премию в медицине за свое открытие. Это принято считать началом современной науки о нервной системе человека [1].

Детальное изучение структуры нейрона (особенно после изобретения электронного микроскопа) позволило выделить некоторые основные его части: тело клетки, аксон, дендриты, синаптические связи. Подсчитать количество нейронов в мозге человека очень сложно, лишь приблизительно можно оценить количество нейронов в коре головного мозга как 3×10^{10}, общее количество нейронов как 10^{11}, количество синаптических связей как 10^{15}. Скорость передачи импульсов между нейронами головного мозга можно оценить как $0{,}5-2$ м/с [1].