О вычислительных задачах теории чисел

Нестеренко Юрий Валентинович,
МГУ, мех-мат

11 марта 2009

Эйлер:

$$\pi = \sqrt{12}\left(1 - \frac{1}{3 \cdot 3} + \frac{1}{5 \cdot 3^2} - \frac{1}{7 \cdot 3^3} + \cdots\right)$$

Рамануджан:

$$\frac{1}{\pi} = \frac{2\sqrt{2}}{9801} \sum_{k=0}^{\infty} \frac{(4k)!(1103 + 26390k)}{(k!)^4 396^{4k}}$$

Д.Чудновский и Г.Чудновский:

$$\frac{1}{\pi} = 12 \sum_{k=0}^{\infty} \frac{(-1)^k (6k)!(13591409 + 545140134k)}{(3k)!(k!)^3 640320^{3k+3/2}}$$

Вычислено 1 241 100 000 000 десятичных знаков π.

Наименьшее решение в натуральных числах (x, y) системы

$$x^2 - 809xy + y^2 = \square \qquad x^2 + 809xy + y^2 = \square$$

имеет

$x =$ 48612127374682753879734012615486541079221674886667107637543720320014372770721079384696998324497515632441440955703198945897843286078018271914721863481894114509718514389686636807620849588739209429885046713311317415014859747150767009329160487279504601659448670724956727070404778212438816906296474640071381341278603662085006353458570617022732394722200649762206732460463437167087048738880705558669403360860226689391464937067563734096882219982127065475652958914792796412930094323220745083566969331042739488532908186295791616950584632560627788 8

Наименьшее решение уравнения

$$x^3 + y^3 = 382z^3$$

в натуральных числах:

$$x = 584775341199261263762183$$
$$90196344577607972745895728749$$

$$y = 167532622951258454638114$$
$$27438340702778576158801481539$$

$$z = 812205439348579389316771$$
$$95009290600931518540131945 74$$

Мнимые части первых 36 нулей дзета функции Римана

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

в критической полосе $0 < \mathbf{Re}\rho < 1$, $\mathbf{Im}\rho =$

14.134725142	21.022039639	25.010857580	30.424876126
32.935061588	37.586178159	40.918719012	43.327073281
48.005150881	49.773832478	52.970321478	56.446247697
59.347044003	60.831778525	65.112544048	67.079810529
69.546401711	72.067157674	75.704690699	77.144840069
79.337375020	82.910380854	84.735492981	87.425274613
88.809111208	92.491899271	94.651344041	95.870634228
98.831194218	101.317851006	103.725538040	105.446623052
107.168611184	111.029535543	111.874659177	114.320220915
...	...	...	

$$\mathbf{Im}\ \rho_{100} = 236.52422966581620580247550795566297868952949$$
$$52121891237009189609878191503842923328262614446040651$$
$$74015827315678371311908125834666026514272342744271055$$
$$94126955313116860411612083861052580225370086489053569$$
$$52178629047472560252682656348047799721211654634140173$$
$$07686882073420880127926644985268669489487216328558298$$
$$80662715386148660811208726059605599639741741411073319$$
$$32566901602812030379738385137490926579562946886420201$$
$$53912744034670408352710424679914028076197059813818175$$
$$38187168651059206275564809906201561105964206003064178$$
$$95025085615117282456966945585079945321497441545297219$$
$$12670586173851416950107038957215891410476462337128012$$
$$48443401149192190622936151728642860733202107967849957$$
$$63941101584694797174527131398342985780333845209666740$$
$$50617154905576061284758618968479553276456189470939...$$

Год	Число нулей $\zeta(s)$	Авторы
1903	15	J. P. Gram
1914	79	R. J. Backlund
1925	138	J.I. Hutchinson
1935	1,041	E. C. Titchmarsh
1953	1,104	A.M. Turing
1956	15,000	D.H. Lehmer
1956	25,000	D.H.Lehmer
1958	35,337	N.A. Meller
1966	250,000	R.S. Lehman
1968	3,500,000	J.B. Rosser, J.M. Yohe, L. Schoenfeld
1977	40,000,000	R. P. Brent
1979	81,000,001	R.P. Brent
1982	200,000,001	Brent, Lune, Riele, D.T. Winter
1983	300,000,001	J. van de Lune, H.J.J. te Riele
1986	1,500,000,001	J. van de Lune, H.J.J. te Riele, Winter
2001	10,000,000,000	J. van de Lune
2004	900,000,000,000	S. Wedeniwski
2004	10,000,000,000,000	X. Gourdon, P. Demichel

- Проверка на простоту и построение больших простых чисел
- Разложение больших чисел на множители
- Дискретное логарифмирование
- Эллиптические кривые

Сложные вычислительные задачи теории чисел.

Пример (Дискретное логарифмирование). *Дано простое число p. Для заданных чисел $a, b \in \mathbb{Z}$ требуется решить сравнение*

$$a^x \equiv b \pmod{p}.$$

Пример (Факторизация целых чисел). *Дано составное натуральное число N. Требуется разложить его на нетривиальные множители.*

Лучшие из известных алгоритмов дискретного логарифмирования и факторизации, использующие вычисления в полях алгебраических чисел, требуют

$O(\exp(c(\ln p)^{1/3}(\ln\ln p)^{2/3}))$ и $O(\exp(c(\ln N)^{1/3}(\ln\ln N)^{2/3}))$

арифметических операций.

Ключевой обмен: Два лица A и B хотели бы выработать общий тайный ключ для последующего шифрования информации.

Алгоритм. *Данные: Простое число* p*, первообразный корень* g *по модулю* p*, секретный ключ* a *абонента* A *и секретный ключ* b *абонента* B*.*
Найти: Общий ключ $k \in \mathbb{Z}$, $0 < k < p$*, известный только абонентам* A *и* B*.*
1. Абоненту A *вычислить* $x \equiv g^a \pmod{p}$ *и передать результат абоненту* B*.*
2. Абоненту B *вычислить* $y \equiv g^b \pmod{p}$ *и передать результат абоненту* A*.*
3. Абоненту A *положить* $k \equiv y^a \pmod{p}$*,*
4. Абоненту B *положить* $k \equiv x^b \pmod{p}$*.*

Корректность алгоритма: $k \equiv (g^a)^b \equiv (g^b)^a \pmod{p}$.

Схема шифрования RSA: Абонент A выбирает два простых числа p, q и натуральное e, взаимно простое с $p-1$ и $q-1$. Затем он вычисляет $n = pq$ и d, удовлетворяющее сравнению

$$ed \equiv 1 \pmod{\varphi(n)}, \qquad \varphi(n) = (p-1)(q-1).$$

Открытым ключом абонента A будет пара (n, e). Секретная информация: d, p и q.

Алгоритм. *Данные: Открытый ключ (n, e) и секретный ключ d абонента A.*
Требуется: Передать абоненту A сообщение $x, 0 < x < n$ абонента B.
1. Абоненту B вычислить $y \equiv x^e \pmod{n}$ и переслать результат абоненту A.
2. Абоненту A положить $x \equiv y^d \pmod{n}$.

Корректность алгоритма: $x^{\varphi(n)} \equiv 1 \pmod{n}$. Поэтому $y^d \equiv x^{ed} \equiv x \pmod{n}$.

Алгоритм возведения в степень Пусть A — некоторое кольцо.

Алгоритм 1. Данные: *Элемент* $a \in A$ *и натуральное число* d.

Найти: *Элемент* a^d.

1. Представить d *в двоичной системе счисления, т.е. найти такие числа* $d_j \in \{0,\ 1\}$, *что* $d = d_0 2^r + \cdots + d_{r-1}2 + d_r,\ d_0 = 1$.
2. Положить $a_0 = a$ *и затем для* $i = 1, \ldots, r$ *вычислить*

$$a_i = a_{i-1}^2 \cdot a^{d_i}. \qquad (1)$$

3. Положить $a^d = a_r$.

Алгоритм вычисляет степень a^d, используя не более $2[\log_2 d]$ умножений в кольце A:

$$a_i = a^{d_0 2^i + \cdots + d_i}, \qquad 0 \le i \le r.$$

Проверка на простоту и построение больших простых чисел

Наибольшие из известных в настоящее время простых чисел.

Номер	Число	Количество цифр	Открыто
1	$2^{43112609}-1$	12978189	Авг. 2008
2	$2^{37156667}-1$	11185272	Сент. 2008
3	$2^{32582657}-1$	9808358	Сент. 2006
4	$2^{30402457}-1$	9152052	Дек. 2005
5	$2^{25964951}-1$	7816230	Фев. 2005
6	$2^{24036583}-1$	7235733	Май 2004
7	$2^{20996011}-1$	6320430	Нояб. 2003
8	$2^{13466917}-1$	4053946	Дек. 2001
9	$19249 \cdot 2^{13018586}+1$	3918990	Май 2007
10	$27653 \cdot 2^{9167433}+1$	2759677	Июнь 2005

$$2^{uv} - 1 = (2^u - 1)(2^{u(v-1)} + \cdots + 2^u + 1)$$

$$p - \text{простое}, \quad M_p = 2^p - 1 - \text{число Мерсенна}$$

$$M_{11} = 2047 = 23 \cdot 89, \quad M_{23} = 8388607 = 47 \cdot 178481,$$

Теорема 1 (Люка 1878, Лемер, 1930). *Пусть m - нечетное число, $m \geq 3$, и последовательность $L_n, n \geq 0$, задается правилом*

$$L_0 = 4, \qquad L_{n+1} \equiv L_n^2 - 2 \pmod{2^m - 1}, \quad n \geq 0.$$

Число $2^m - 1$ будет простым тогда и только тогда, когда

$$L_{m-2} \equiv 0 \pmod{2^m - 1}.$$

• Наибольшие известные простые числа p, для которых $2p+1$ просто (числа Софи Жермен)

$$p = 48047305725 \cdot 2^{172403} - 1, \qquad 137211941292195 \cdot 2^{171960} - 1,$$
$$7068555 \cdot 2^{121301} - 1$$

• Наибольшие известные простые числа p, для которых $p+2$ просто ("близнецы")

$$p = 2003663613 \cdot 2^{195000} - 1, \qquad 194772106074315 \cdot 2^{171960} - 1,$$
$$100314512544015 \cdot 2^{171960} - 1$$

Методы отсеивания составных чисел: N — *составное число, и требуется доказать это.*

Выберем целое число $a, 1 < a < N$.
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*. (Малая теорема Ферма)
Существуют составные числа, для которых выполняется условие 2) при любом целом $a, (a, N) = 1$. Они называется **числами Кармайкла**. Множество их бесконечно.
Пример: $N = 561 = 3 \cdot 11 \cdot 17 \qquad (a, 561) = 1 \Rightarrow$.

$$a^2 \equiv 1 \pmod 3, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17},$$
$$560 = 2 \cdot 280 = 10 \cdot 560 = 16 \cdot 35 \quad \Rightarrow \quad a^{560} \equiv 1 \pmod{561}$$

Тест. *Пусть $N > 2$ — нечетное натуральное число. Определим целые числа s, t равенством $N - 1 = 2^s t$, где t нечетно. Выберем целое число $a, a > 1$.*
1) Если $(a, N) > 1$, то N составное число.
2) Если $(a, N) = 1$ и выполнены условия

$$a^t \not\equiv 1 \pmod{N}, \quad a^{2^k t} \not\equiv -1 \pmod{N}, \quad k = 0, 1, \ldots, s-1,$$

то N составное число.

$$a^{N-1} - 1 = (a^t - 1)(a^t + 1)(a^{2t} + 1) \cdots (a^{2^{s-1}t} + 1).$$

Для составного N при случайном выборе a с вероятностью $\geq \frac{3}{4}$ попадается a, доказывающее непростоту N. Среднее время работы соответствующего алгоритма есть $O(\log N)$.

Теорема. *Пусть N нечетно, $N-1 = F \cdot R$, причем для каждого простого делителя q числа F с некоторым целым b выполнены условия*

$$b^{N-1} \equiv 1 \pmod{N}, \qquad \left(b^{(N-1)/q} - 1,\, N\right) = 1. \qquad (2)$$

Тогда любой простой делитель p числа N удовлетворяет сравнению

$$p \equiv 1 \pmod{F}$$

Если при этом выполнено неравенство

$$R \leq F + 1$$

то N — простое.

Как для простого $F > 2$ построить простое $N > F^2$.

1. Выбрать случайным образом четное число R на промежутке $F \le R \le 4F + 2$ и положить $N = FR + 1$.

2. Испытать число N с помощью тестов, отсеивающих составные числа. Если при этом выяснится, что N — составное число, следует выбрать новое значение R и опять повторить вычисления.

3. Если число N, выдержало испытания достаточно много раз, выбрать случайным образом число $b, 1 < b < N$, и проверить для него выполнимость условий

$$b^{N-1} \equiv 1 \pmod{N}, \qquad \left(b^R - 1, N\right) = 1. \tag{3}$$

Если эти соотношения выполняются, то N — простое.

4. Если условия (3) нарушаются, выбрать другое значение b и повторять эти операции до тех пор, пока такое число не будет обнаружено.

Алгоритм (А.Коэн-Х.Ленстра, 1984)**.** *Дано натуральное число N. Установить составное оно или простое.*
1. Выбираются натуральные числа s и t, взаимно простые с N и обладающие следующими свойствами:
а) t не очень велико,
б) $s > N^{1/2}$,
в) для любого целого a, взаимно простого с s, имеет место сравнение $a^t \equiv 1 \pmod{s}$.
г) известны разложения на множители чисел s и t.
2. Число N подвергается ряду тестов, подобных малой теореме Ферма, в некоторых кольцах целых алгебраических чисел. Если какой-либо тест не проходит, то число N — составное.
3. Определить числа

$$r_i \equiv N^i \pmod{s}, \quad 1 \le r_i < s, \qquad i = 0, 1, \ldots, t.$$

Если ни одно из чисел r_i не является делителем N, то N — простое число.

1. Алгоритм Коэна-Ленстры не требует информации о делителях чисел $N \pm 1$ или других подобных чисел.
2. Сложность алгоритма есть $O((\log N)^{c \log\log\log N})$.
3. Один из тестов алгоритма имеет вид

$$(3\zeta + 2)^{\left[\frac{N}{3}\right]} \cdot (-3\zeta - 1)^{\left[\frac{2N}{3}\right]} \equiv \xi \pmod{N\mathbb{Z}[\zeta]},$$

где $\zeta = e^{2\pi i/3}$ и ξ некоторый кубический корень из 1.
4. При $t = 5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$ и

$$\begin{aligned} s =& 2^6 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 71 \cdot \\ & \cdot 73 \cdot 113 \cdot 127 \cdot 181 \cdot 211 \cdot 241 \cdot 281 \cdot 337 \cdot 421 \cdot 631 \cdot 1009 \cdot \\ & \cdot 2521 \sim 1,532 \cdot 10^{52}, \end{aligned}$$

алгоритм позволяет проверять простоту всех чисел $\leq 10^{100}$.

Существует полиномиальный алгоритм проверки чисел на простоту. Количество битовых операций, требующихся ему для завершения работы есть величина порядка $O(\log^{10,5} N)$. Существенным недостатком этого алгоритма, не позволяющим использовать его на практике, является потребность очень большой памяти, которая имеет порядок $O(\log^6 N)$ бит, что при больших N намного превосходит память, требующуюся алгоритму Коэна-Ленстры.

Разложение больших чисел на множители

Алгоритмы разложения чисел на множители распределяются на группы в зависимости от количества нужных для работы арифметических операций.

1) Алгоритмы **экспоненциальной** сложности используют $O(N^c)$ арифметических операций.

2) Алгоритмы **субэкспоненциальной** сложности требуют для своей работы $O(e^{c(\ln N)^\alpha(\ln\ln N)^\beta})$ арифметических операций. Здесь α, β, c — положительные постоянные, $\alpha + \beta = 1$. Для наиболее быстрого из субэкспоненциальных алгоритмов — **метода решета числового поля**, имеем $\alpha = \frac{1}{3}, \beta = \frac{2}{3}$.

Алгоритмы полиномиальной сложности, $\alpha = 0, \beta = 1$, для задачи факторизации не известны, и весьма вероятно, что их не существует.

Метод пробных делений. Каждое простое число содержится в последовательности

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, \ldots,$$

состоящей из $2, 3$ и всех чисел вида $6n \pm 1, n \in \mathbb{N}$. Правило порождения этой последовательности имеет вид

$$d_{2k} = d_{2k-1} + 2, \quad d_{2k+1} = d_{2k} + 4, \quad k \geq 2.$$

Алгоритм, проверяющий делимость N на числа из последовательности d_i, требует $O(N^{1/2})$ арифметических операций и $O(1)$ памяти.

ρ–метод Полларда: Пусть $f(x)$ — "достаточно случайный" многочлен, скажем $f(x) = x^2 + 1$.

Алгоритм. Дано: *составное число* N.

Найти: *нетривиальный делитель* N .

1. Выбрать случайно $x_0 \in \mathbb{Z}, 1 < x_0 < N$, *и положить*

$$x \equiv f(x_0) \pmod{N}, \qquad y \equiv f(x) \pmod{N}.$$

2. Вычислить $d = (y - x, N)$. *Если* $1 < d < N$ *алгоритм останавливается, нетривиальный делитель* d *числа* N *найден.*

3. Если $d = N$, *перейти в п. 1.*

4. Положить

$$x \equiv f(x) \pmod{N}, \quad z \equiv f(y) \pmod{N}, \quad y \equiv f(z) \pmod{N}$$

и перейти в пункт 2 алгоритма.

При некоторых допущениях среднее время работы есть $O(p^{1/2})$, где p — наименьший простой делитель N, т.е. $O(N^{1/4})$.

Субэкспоненциальные алгоритмы:

1. Выбирают некоторое конечное множество

$$\mathcal{B} = \{p_0 = -1, p_1, p_2, \ldots, p_\ell\},$$

где $p_1, \ldots, p_\ell$ — различные простые числа **база разложения**.

2. Строится последовательность пар целых чисел $(R_i, z_i), i = 1, 2, \ldots$, таких, что

$$z_i^2 \equiv R_i \pmod{N}, \qquad i = 1, 2, \ldots . \tag{4}$$

3. С помощью метода пробных делений на элементы $\mathcal{B}$ пытаются разложить числа R_i на простые множители. Если

$$R_i = \prod_{j=0}^{\ell} p_j^{\alpha_{i,j}},$$

то индекс i помещают в некоторое множество $\mathcal{L}$. В противном случае этот индекс отбрасывается.

$$z_i^2 \equiv \prod_{j=0}^{\ell} p_j^{\alpha_{i,j}} \pmod{N}, \qquad i \in \mathcal{L} \qquad \ell + 1 = |\mathcal{B}|.$$

4. При $|\mathcal{L}| > \ell + 1$ найти нетривиальное решение $b_i \in \{0, 1\}$ системы

$$\sum_{i \in \mathcal{L}} b_i \alpha_{i,j} \equiv 0 \pmod{2}, \qquad 0 \le j \le \ell. \tag{5}$$

Тогда

$$x^2 = \left(\prod_{i \in \mathcal{L}} z_i^{b_i} \right)^2 \equiv \prod_{j=0}^{\ell} \prod_{i \in \mathcal{L}} p_j^{b_i \alpha_{i,j}} = \prod_{j=0}^{\ell} p_j^{\sum_{i \in \mathcal{L}} b_i \alpha_{i,j}} = y^2 \pmod{N}.$$

При

$$x = \prod_{i \in \mathcal{L}} z_i^{b_i}, \qquad c_j = \frac{1}{2} \sum_{i \in \mathcal{L}} b_i \alpha_{i,j} \in \mathbb{Z}, \qquad y = \prod_{j=0}^{\ell} p_j^{c_j},$$

имеем

$$x^2 \equiv y^2 \pmod{N}. \tag{6}$$

5. Вычислить $d = (x - y, N)$. Если $1 < d < N$, то d — собственный делитель N.

При $|\mathcal{L}|$ существенно превышающем $\ell+1$ можно найти несколько пар (x, y), удовлетворяющих (6), что важно, если для первой из этих пар выполняется $d = 1$ или $d = N$.

Квадратичное решето: Пусть $f(x) = ax^2 + 2bx + c$, $a > 0$ и $N = b^2 - ac$. Тогда

$$af(x) = (ax + b)^2 - (b^2 - ac) \equiv (ax + b)^2 \pmod{N}$$

$$z_i = ai + b, \quad R(i) = af(i), \qquad i \in \left[-\frac{b}{a} - M,\ -\frac{b}{a} + M\right]$$

$$M = N^{\varepsilon}, \quad a \sim \frac{\sqrt{2N}}{M} \quad \Rightarrow \quad |f(i)| = O(N^{1/2+\varepsilon}).$$

Просеивание: Если $f(i) \equiv 0 \pmod{p^t}$, то при любом целом ℓ выполняется также сравнение $f(i + \ell p^t) \equiv 0 \pmod{p^t}$. Это позволяет фиксировать сразу некоторое множество чисел i, для которых в разложение $f(i)$ на простые множители входит простое число p в степени не меньшей t. Поиск нужных чисел i ускоряется.

• Выбирая разными способами a, b, c можно для каждого многочлена $f(x)$ производить свое просеивание. Изложенная схема называется **квадратичное решето с несколькими полиномами**. Этот алгоритм может раскладывать на множители числа, доходящие до 10^{135}.

• Приняв на веру ряд недоказанных гипотез о распределении простых чисел, можно показать, что при некотором выборе $\mathcal{B}$, в зависимости от N, алгоритм требует $O(e^{\sqrt{(1+o(1))\ln N \ln\ln N}})$ арифметических операций.

• **Решето в числовых полях:** Пусть θ — корень многочлена $f(x) \in \mathbb{Z}[x]$ и $m \in \mathbb{Z}$ таково, что $f(m) \equiv 0 \pmod N$. Если при некоторых $a, b \in \mathbb{Z}$

$$a + bm = u^2, \qquad a + b\theta = g(\theta)^2, \qquad g(x) \in \mathbb{Z}[x],$$

то

$$u^2 = a + bm \equiv g(m)^2 = v^2 \pmod N.$$

Выбор многочлена $f(x)$ и числа m в зависимости от N. Подходящие числа a, b находятся с помощью просеивания в кольцах $\mathbb{Z}[\theta]$ и $\mathbb{Z}$.
Сложность алгоритма: $O(e^{c(\ln N)^{1/3}(\ln\ln N)^{2/3}})$ операций.
Рекорды: 1) $N = 2^{1039} - 1$, май 2007, $f(x) = 2x^6 - 1, m = 2^{173}$. Просеивание выполнялось 6 месяцев. В пересчете на Athlon64 / Opteron [2.2GHz] это эквивалентно примерно 100 годам. Количество соотношений 16570808010.
2) RSA-200, май 2005

Дискретное логарифмирование

(решение сравнения $a^x \equiv b \pmod{p}$)

• Наименьшее целое неотрицательное число x, удовлетворяющее соотношению $a^x \equiv b \pmod{p}$ называется *индексом* или *дискретным логарифмом* числа b по основанию a и обозначается $\log_a b$ или просто $\log b$.

• Для любых $b, c \in (\mathbb{Z}/p\mathbb{Z})^*$ справедливы равенства

$$\log_a(bc) \equiv \log_a b + \log_a c \pmod{p-1},$$

$$\log_c b \equiv \frac{\log_a b}{\log_a c} \pmod{p-1}.$$

Метод Гельфонда (метод больших и малых шагов): сложность $O(p^{1/2} \ln p)$ арифметических операций.

Алгоритм. Данные: *Простое число* $p \geq 3$, *первообразный корень* a *по модулю* p, *число* $b \in \mathbb{Z}$, $p \nmid b$.

Найти: *Решение сравнения* $a^x \equiv b \pmod{p}$.

1. Вычислить $H = [\sqrt{p}] + 1$ *и* $c = a^H \bmod p$.

2. Составить два набора чисел

$$S_1 = \{c^u \bmod p : 1 \leq u \leq H\}, \quad S_2 = \{ba^v \bmod p : 1 \leq v \leq H\}.$$

3. Упорядочить по возрастанию оба набора S_1 *и* S_2. *Найти совпавшие элементы этих наборов, то есть такие числа* u, v, *для которых*

$$c^u \equiv ba^v \pmod{p}.$$

4. Положить

$$\log_a b = Hu - v.$$

Линейное решето: Вход: числа a, b, p.
Выход: Дискретный логарифм $\log_a b$.
1) Выбрать множество $S = \{p_1, p_2, \ldots, p_t\} \subset (\mathbb{Z}/p\mathbb{Z})^*$ такое, что "существенная часть"$(\mathbb{Z}/p\mathbb{Z})^*$ может быть представлена в виде произведения некоторых элементов из S.
2) Выбрать случайным образом $k, 0 \leq k < p-1$ и попытаться представить a^k в виде произведения элементов из S

$$a^k \equiv \prod_{i=1}^{t} p_i^{c_i} \pmod{p}, \qquad c_i \geq 0.$$

Если попытка безуспешна, выбрать новое k, иначе имеем

$$k \equiv \sum_{i=1}^{t} c_i \log_a p_i \pmod{p-1}.$$

3) Повторять шаг 2) до тех пор, пока не будет найдено более t соотношений.

4) Решить систему из линейных уравнений относительно неизвестных $\log_a p_i$, $l < i < t$, определенную в шаге 3.
5) Выбрать случайным образом целое k, $0 < k < p - 1$ и попытаться найти разложение:

$$ba^k \equiv \prod_{i=1}^{t} p_i^{d_i} \pmod{p}.$$

Если этого не удалось сделать, повторить шаг 5. В противном случае определить

$$\log_a b \equiv \sum_{i=1}^{t} d_i \log_a p_i \pmod{p-1}.$$

• Сложность алгоритма $O(e^{c(\ln N)^{1/2}(\ln\ln N)^{1/2}})$

• Наиболее быстрый алгоритм — решето числового поля имеет сложность $O(e^{c(\ln N)^{1/3}(\ln\ln N)^{2/3}})$.

Рекорд: $p = \left[10^{159} \cdot \pi\right] + 119849$. Было построено 831266637 соотношений. Необходимое для этого время в пересчете на один 3.2 GHz Xeon64 PC равно 3,3 года. После упрощений матрица системы имела 2177226 строк, 2177026 столбцов и 289976350 ненулевых элементов. Решение соответствующей системы линейных уравнений в целом заняло 14 CPU лет в пересчете на один 3.2 GHz Xeon64. После этой предварительной работы вычисление индивидуального логарифма требует нескольких часов.

Эллиптические кривые

Эллиптическая кривая — множество точек (x, y), удовлетворяющих уравнению

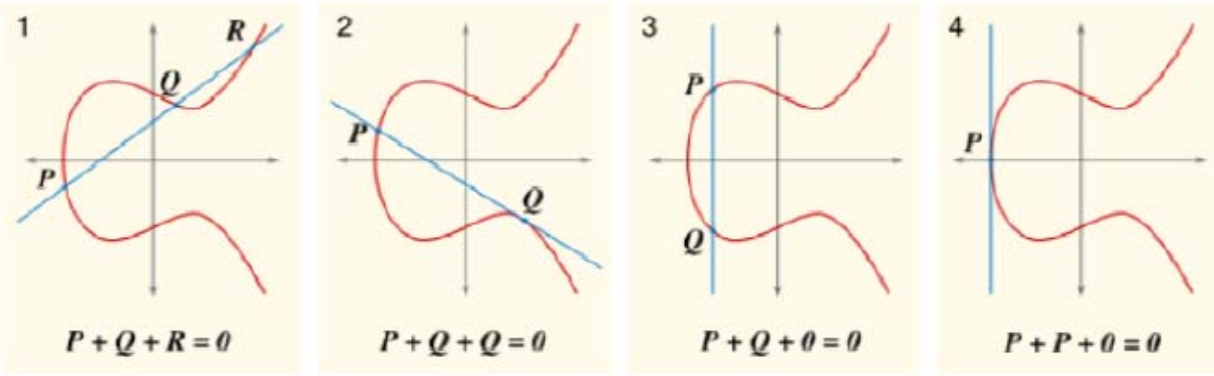
$$y^2 = x^3 + ax + b, \qquad \Delta = 4a^3 + 27b^2 \neq 0. \tag{7}$$

Будет предполагаться, что $a, b \in \mathbb{Q}$.

Не известен алгоритм, позволяющий по заданной кривой определить, есть ли на ней хотя бы одна рациональная точка, т.е. разрешимо ли уравнение (7) в рациональных числах.

Основная проблема: Найти все рациональные точки (x, y) на кривой.

Сложение точек на эллиптической кривой



$P = (x_1, y_1)$ и $Q = (x_2, y_2)$ на кривой, допустим, что $x_1 \neq x_2$.

Пусть $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$. Тогда можно определить **сумму** точек

$R = P + Q = (x_3, y_3)$ следующим образом:

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = -y_1 + \lambda(x_1 - x_3)$$

Введенная операция ассоциативна и коммутативна. Кривая становится группой.

Морделл, 1922: Все рациональные точки кривой

$$y^2 = x^3 + ax + b$$

могут быть получены из конечного числа проведением хорд и касательных.

Теорема 2. *Существуют рациональные точки* $P_1, \ldots, P_r$ *такие, что любая рациональная точка* P *кривой (7) единственным способом представляется в виде*

$$P = n_1 P_1 + \cdots + n_r P_r + Q,$$

где Q *– точка конечного порядка.*

Возможен случай $r = 0$.

Число r называется **рангом** кривой.

Для многих кривых ранг и образующие группы рациональных точек P_j вычислены, но **общий алгоритм вычисления ранга и образующих не известен**.

Эллиптическая кривая

$$y^2 = x^3 - 263^2 x, \qquad x = \frac{u}{w}, \quad y = \frac{v}{w} \qquad u, v, w \in \mathbb{Z}$$

$$u = 29768422965044611015563235088021925107517338423561136,$$

$$v = -21038120743602203009156378299860489437387927635254294 0,$$

$$w = 10294932300991528227913591867633955888159532499345 3$$

Кривая имеет ранг 1, указанная точка — образующая.

Гипотеза: *Существуют эллиптические кривые сколь угодно большого ранга.*

Кривая ранга ≥ 28, Elkies (2006)

$$y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502 \cdot x + 3448161179503055646703298569039072037485594435931918036126600829629193944873224342900$$

Независимые точки бесконечного порядка: $x =$

$-212415009125438107329213746 3,$
$233450986603470175688475453 7,$
$-167173605406236906387903866 3,$
$213913026013915666649298213 7,$
$153470676446712072388547733 7,$
$-273107948787567703334157506 3,$
$277572626684457164970545853 7,$
$149438572932718895754183381 7,$
$186843822862088735850906525 7,$
$200894510882574377486654253 7,$
$234836054091802516965163293 7,$
$-147208400709048117447000866 3,$
$292412860770806121336328893 7,$
$537499389106606189329393453 7,$
$170969076823335452333400855 7,$
$245095401135359314407259518 7,$
$296925470927355916746467493 7,$
$271191493494169260133288293 7,$
$200785860779968545287783289 37,$
$215808245024073477431781069 7,$
$200464545824705902240322493 7,$
$297574945094799626494709133 7,$
$-210249046768628515014734786 3,$
$311583179915063034902194537,$
$277393100834186523144377181 7,$
$215658118814376840936346138 7,$
$386633049987241250881565913 7,$
$223086828977357602377867873 7$

p — простое число. Эллиптическая кривая E над полем $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ — множество точек $(x, y) \in \mathbb{F}_p$, удовлетворяющих уравнению

$$y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{F}_p, \quad 4a^3 + 27b^2 \neq 0.$$

$P = (x_1, y_1)$ и $Q = (x_2, y_2)$, $x_1 \neq x_2$ — точки на кривой. Тогда $R = P + Q = (x_3, y_3)$ определяется следующим образом:

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = -y_1 + \lambda(x_1 - x_3), \quad \lambda = \frac{y_1 - y_2}{x_1 - x_2}$$

Кривая E становится конечной группой.

• Решение уравнения $P = nQ$, где $P, Q \in E$ и n неизвестное натуральное число — аналог задачи дискретного логарифмирования.

• Субэкспоненциальные алгоритмы дискретного логарифмирования на эллиптических кривых неизвестны.

• Рекорд: логарифмирование при $p \sim 10^{109}$.

• За логарифмирование при $p > 10^{130}$ предложена премия 20000 USD (Certicom)