Лекция №10
Алгоритм квадратичного решета для факторизации целых чисел

Лектор: Н.Ю. Золотых Записал: Н. Дуничкина

20 декабря 2008

Содержание

1. Введение

$x^2 \equiv y^2 \pmod n$
$x \neq \pm y \pmod n$
Тогда $0 \equiv x^2 - y^2 \equiv (x-y)(x+y)$.
$(x+y, n)$, $(x-y, n)$ - нетривиальные делители n.

Будем искать q, такое что $q^2 \pmod n$ мало и польный квадрат в арифметическом смысле, но при этом q - большое.

Пусть

$$x = q$$
$$y = \sqrt{q^2 \mod n}$$

Считаем $(x+y, n)$. Если тривиальный, то ищем другое q.
$q = \lceil \sqrt{an} + b \rceil$, где a,b - малые $\in \mathbb{Z}$. Например, $a = 1$
$q = \sqrt{an} + b + \delta (0 \leq \delta < 1)$ Тогда
$q^2 = an + 2(b+\delta)\sqrt{an} + (b+\delta)^2 \equiv 2(b+\delta)\sqrt{an} + (b+\delta)^2 \pmod n$
q^2 $O(\sqrt{n})$. Какова вероятность, что из него можно извлечь квадратный корень?
Всего $\sqrt{m}$ чисел - полных квадратов, меньших или равных m.
$P = O(\frac{1}{\sqrt[4]{n}})$

Если числа ведут себя как случайные, то сколько надо перебрать a и b, чтобы найти нетривиальное сравнение в НОД?

Пример 1. $n = 561$
$a = 1, b = 0 \quad \lceil \sqrt{561} \rceil = 24$
$24^2 = 576 \equiv 15 \pmod n$ - не квадрат
$a = 1, b = 1 \quad \lceil \sqrt{561} + 1 \rceil = 25$
$25^2 = 625 \equiv 64 = 8^2$ Ура!
$(561, 25 - 8) = 17$ - найден делитель!
$(561, 25 + 8) = 33$

Трудоемкость $\sqrt[4]{n}$. Что можно сделать, чтобы уменьшить ее?

Пример 2. $n = 4633$
$67^2 \equiv -144 \pmod{n}$ не квадрат
$68^2 \equiv -9 \pmod{n}$
$(67 \cdot 68)^2 = (12 \cdot 3)^2$
$x = 67 \cdot 68 = 4556 = -77 \pmod{3}$
$y = 12 \cdot 3 = 36$
$(x - y, n) = 113$
$(x + y, n) = 41$

Определение 1. Возьмем некоторое B $e^{\sqrt{\ln n \cdot \ln \ln n}}$ и рассмотрим простые числа, не превышающие $B + (-1)$. Назовем это множество *факторной базой*

2. Алгоритм

1. Найти факторную базу
2. Для разных a и b вычислять $Q_i = \lceil \sqrt{an} + b \rceil$.

   Убедиться, что $Q_i^2 \mod n$ раскладывается по факторной базе. Если не раскладывается, то убрать их из рассмотрения. Если раскладывается, то собираем вместе все Q_i. Всего надо найти $\pi(B) + 2$ таких Q_i ($\pi(B)$ - число простых чисел, не превосходящих B).
3. Найти подсистему, приводящую к $x^2 \equiv y^2 \pmod{n}$.

   Если окажется, что $x \equiv \pm y$ (не повезло), то найти новое Q_i (решить снова)

Замечание 1. Если n 10^{130}, то B 10^7.

Пример 3. $n = 85907$ $B = 10$
$\lceil \sqrt{3 \cdot 85907} \rceil = 507$ ($a = 3$, $b = 0$)
$\lceil \sqrt{8 \cdot 85907} \rceil = 829$
$501^2 \equiv -6720 = -1 \cdot 2^6 \cdot 3 \cdot 5 \cdot 7$ (берем близкие числа к 507, добавляя b в Q_i, здесь $b = -6$)
$507^2 = -672 = -1 \cdot 2^5 \cdot 3 \cdot 7$
$508^2 = 343 = 7^3$
$829^2 = -15 = -1 \cdot 3 \cdot 5$

Хотим взять и перемножить какие-то числа слева. Получим квадрат. Хотим, чтобы и справа был квадрат. Для этого надо, чтобы степени сичел из факторной базы были четные.

Вводим коэффициенты $\alpha_i \in \mathbb{Z}_2$:
$\alpha_i = 0$ - не берем число в произведение $\alpha_i = 1$ - берем.
Получаем:
$501^2 \cdot 507^2 \cdot 508^2 \cdot 829^2 = (-1)^{\alpha_1+\alpha_2+\alpha_4} \cdot 2^{6\alpha_1+5\alpha_2} \cdot 3^{\alpha_1+\alpha_2+\alpha_4} \cdot 5^{\alpha_1+\alpha_4} \cdot 7^{\alpha_1+\alpha_2+3\alpha_3}$
Хотим, чтобы

$$\alpha_1 + \alpha_2 + \alpha_4 \equiv 0 \pmod{2}$$
$$6\alpha_1 + 5\alpha_2 \equiv 0 \pmod{2}$$
$$\alpha_1 + \alpha_2 + \alpha_4 \equiv 0 \pmod{2}$$
$$\alpha_1 + \alpha_4 \equiv 0 \pmod{2}$$
$$\alpha_1 + \alpha_2 + 3\alpha_3 \equiv 0 \pmod{2}$$

Это система линейных однородных уравнений в поле $\mathbb{Z}_2$. Система 5×4. Скорее всего единственное тривиальное решение, но может быть и нет. Если взять число Q_i на 1 больше, чем число элементов в факторной базе, то число неизвестных будет больше, чем число уравнений, и всегда будет существовать нетривиальное решение.

3. Квадратичное решето

Померанц, 1982

Возникает вопрос, как ускорить поиск Q_i.

Пусть a - фиксировано.

$Q_b = (\lceil\sqrt{an} + b\rceil)^2 \mod n$

Можно ли ускорить процедуру нахождения тех Q_b, для которых возможно разложение по факторной базе?

Померанц предложил рассматривать массив S:

$\ldots$	$S[-2]$	$S[-1]$	$S[0]$	$S[1]$	$S[2]$	$\ldots$

$S[b] = \log Q_b$ - записывается в ячейках массива.

Для любого p из факторной базы найти $b \in \mathbb{Z}_p$, такие что

$Q_b \vdots p \Longleftrightarrow (\lceil\sqrt{an}\rceil + b)^2 \mod n \equiv 0 \pmod p$

Возникает вопрос, сколько таких b для заданного p из факторной базы? (p - простое).

$(\lceil\sqrt{an}\rceil + b)^2 - qn \equiv 0 \pmod p$

Так как $0 < b < p$, то q можем найти. Все известно, кроме b. Надо решить квадратное уравнение в поле $\mathbb{Z}_p$.

Если $\left(\frac{qn}{p}\right) = 1$ (вычет), то 2 решения b_1 и b_2.

Если $\left(\frac{qn}{p}\right) = -1$, то нет решений. Эти значения a и b бесполезны.

В факторной базе надо оставить только вычеты.

Для всех i

$$S[b_1 + ip] - = \log p$$

$$S[b_2 + ip] - = \log p$$

Пытаемся разложить по факторной базе только те Q_b, для которых $S[b] \approx 0$

Эта процедура позволяет сократить время, хотя и не повлияет на порядок. но делить все равно будем меньше.

Определение 2. Эта процедура называется *процедурой просеивания.*

Определение 3. Рассмотренный алгоритм называется *алгоритмом квадратичного решета.*

Алгоритм квадратичного решета находится на втором месте среди алгоритмов факторизации. Его сложность есть $O\left(e^{c\sqrt{\ln n \cdot ln \ln n}}\right)$

4. Использование цепных дробей

Хотим найти нетривиальное решение сравнения

$$x^2 \equiv y^2 \pmod n$$

Определение 4. *Цепная дробь* - это дробь вида

$$\theta = a_1 + \frac{1}{\theta_1} = a_1 + \frac{1}{a_2 + \frac{1}{\theta_2}} = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\theta_3}}} = \cdots,$$

где $\theta > 0$, $\theta \in \mathbb{R}$.

Если исходное число - рациональное, то разложение рано или поздно закончится. Если действительное, то может бесконечно продолжаться.

Заметим, что $a_1 = \lfloor\theta\rfloor$.

Что будет, если разложение оборвем в каком-то месте?

$\frac{1}{\theta_i} \longrightarrow 0$, то получим в правой части

$\frac{p_i}{q_i}$ - i-я подходящая дробь для числа θ. Это очень хорошее рациональное приближение для θ.

Теорема Лагранжа говорит, что $\left|\theta - \frac{p_i}{q_i}\right| \leq \frac{1}{q_i^2}$

Пример 4. $\pi = 3 + \frac{1}{7+\frac{1}{15+\frac{1}{\theta_3}}}$

$\frac{p_1}{q_1} = 3$
$\frac{p_2}{q_2} = \frac{22}{7}$
$\frac{p_3}{q_3} = \frac{333}{106}$
$\frac{p_4}{q_4} = \frac{355}{113}$. Эту подходящую дробь знали уже в Др.Китае.

Если $\theta = \frac{p}{q}$, то разложение в цепную дробь - алгоритм Евклида для нахождения (p, q).

В алгоритме мы в качестве Q брали $Q = x$. Чтобы они были меньше и корень по возможности извлекался, Q можно выбирать, исходя из следующего:

$\sqrt{n} \approx \frac{p_i}{q_i}$

Используя теорему Лагранжа:

$\left|\frac{p_i^2}{q_i^2} - n\right| = \left|\frac{p_i}{q_i} - \sqrt{n}\right| \left(\frac{p_i}{q_i} + \sqrt{n}\right) \approx 2\sqrt{n} \left|\frac{p_i}{q_i} - \sqrt{n}\right| \leq \frac{2\sqrt{n}}{q_i^2}$

Отсюда

$$\left|p_i^2 - q_i^2 n\right| \leq 2\sqrt{n}$$

$$p_i^2 \mod n \leq 2\sqrt{n}$$

Приходим к алгоритму, который предложили Brillhart, Morrison в 1975. Надо искать подходящие дроби для квадратичной иррациональности.

Пример 5. $\theta = \sqrt{45}$

$$a_1 = 6 \Longrightarrow \theta_1 = \frac{1}{\sqrt{45} - 6} = \frac{\sqrt{45} + 6}{9}$$

$$a_2 = 1 \Longrightarrow \theta_2 = \frac{9}{\sqrt{45} - 3} = \frac{\sqrt{45} + 3}{4}$$

$$a_3 = 2 \Longrightarrow \theta_3 = \frac{4}{\sqrt{45} - 5} = \frac{\sqrt{45} + 5}{5}$$

$$\theta = 6 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2 + \cdots}}}$$

Теорема 1. *Цепная дробь периодическая, то есть последовательность a_1, $a_2 \cdots$, начиная с некоторого момента начинает повторяться $\Longleftrightarrow$ иррациональность θ является квадратичной иррациональностью, то есть*

$$\theta = \frac{a + \sqrt{D}}{b}$$

Доказательство. Теорема слеует из того факта, что числитель и знаменатель ограничены. Знаменатель есть $\sqrt{45}$ - (что-то меньшее). Числитель ограничен значением $2 \cdot \sqrt{45} + 1$ $\square$