Лекция №6
Теорема Кармайкла. Тест Соловей-Штрассена

Лектор: Н.Ю. Золотых Записал: В. Логунов

25 октября 2008

Содержание

1. Определения

Определение 1. Число n называется *псевдопростым по основанию* a $(1 < a < n)$, если НОД$(a, n) = 1$ и $a^{n-1} \equiv 1 \pmod{n}$.

Определение 2. *Число Кармайкла* — составное число, псевдопростое по любому основанию a, взаимно простому с исходным.

Пример 1. Числа Кармайкла: $561 = 3 \cdot 11 \cdot 17$; $1105 = 5 \cdot 13 \cdot 17$

Определение 3. Введём следующее обозначение: $\mathbb{Z}_n^*$ - мультипликативная группа вычетов взаимнопростых с n в кольце вычетов $\mathbb{Z}_n$.

2. Теорема Кармайкла

Теорема 1 (Кармайкл, 1912)**.** *Пусть n — нечетное составное, тогда:*

1. *если $n \div p^2$, где p — простое, то n — не число Кармайкла;*
2. *если $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$, где $p_i \neq p_j$ при $i \neq j$, то для того, чтобы n являлось числом Кармайкла необходимо и достаточно, чтобы $(n-1) \div (p_i - 1)$ $(i = \overline{1, k})$;*
3. *если $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$, где $p_i \neq p_j$ при $i \neq j$ и n — число Кармайкла, то $k \geq 3$.*

Доказательство. В доказательстве мы будем пользоваться леммой (теоремой Гаусса):

Теорема 2 (Гаусс)**.** *$\mathbb{Z}_n^*$ является циклической группой тогда и только тогда, когда $n = 2, 4, p^m, 2 \cdot p^m$, где $m \geq 1$, а p — простое нечетное.*

Доказательство теоремы Кармайкла:

1. Доказателство утверждения 1.

   Пусть $n = p^t \cdot m$, $t \geq 2$, p — простое, $p \geq 2$

   От противного докажем, что n — не число Кармайкла.

   Пусть n — число Кармайкла.

   Тогда, по лемме (2) в группе $\mathbb{Z}_{p^2}^*$ есть порождающий элемент. Обозначим его через a.

Обозначим $ord_{p^2}\, a$ порядок элемента a по $\mod p^2$.

$ord_{p^2}\, a = p \cdot (p-1)$ (это верно, потому что $\left|\mathbb{Z}^*_{p^2}\right| = p \cdot (p-1)$, в $\mathbb{Z}^*_{p^2}$ вошли все вычеты по модулю p^2, кроме $0,\ p,\ 2 \cdot p,\ \ldots,\ (p-1) \cdot p$)

Докажем, что n не является псевдопростым по основанию a.

Пусть не так. Тогда n является псевдопростым по основанию a, т.е. $a^{n-1} \equiv 1 \pmod n \Rightarrow a^{n-1} \equiv 1 \pmod{p^2}$ (по определению (опр. 1))

С другой стороны $ord_{p^2}\, a = p \cdot (p-1) \Rightarrow a^{p(p-1)} \equiv 1 \pmod{p^2}$ (по определению порождающего элемента)

Из этого следует, что $(n-1) \vdots p(p-1) \Rightarrow n \not\vdots p$.

Получили противоречие. Таким образом, n — не является псевдопростым числом по основанию a. Следовательно n — не число Кармайкла, что и требовалось доказать.

2. Доказателство утверждения 2.

   (a) Докажем первую часть утверждения — достаточность.
   Дано:

   - $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$, где p_i — простое число, $p_i \neq p_j$ при $i \neq j$
   - $(n-1) \vdots (p_i - 1)$

   Доказать: n — число Кармайкла.
   Доказательство:
   $(n-1) \vdots (p_i - 1) \Rightarrow \exists m_i : n - 1 = m_i \cdot (p_i - 1)$, тогда $\forall a$: НОД$(a, n) = 1$, $1 < a < n \Rightarrow a^{n-1} = (a^{p_i - 1})^{m_i} \equiv 1 \pmod{p_i}$ (по теореме Ферма).
   По китайской теореме об остатках: $a^{n-1} \equiv 1 \pmod n$, где $n = p_1 \cdot \cdots \cdot p_k$.
   Таким образом, n — число Кармайкла (по определению 2), что и требовалось доказать.

   (b) Докажем вторую часть утверждения — необходимость.
   Дано:

   - $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$, где p_i - простое число, $p_i \neq p_j$ при $i \neq j$
   - n — число Кармайкла.

   Доказать: $(n-1) \vdots (p_i - 1)$
   Доказательство:
   Рассмотрим порождающий элемент в группе $\mathbb{Z}^*_{p_i}$ a_i: $ord_{p_i}\, a_i = p_i - 1$ (это верно, так как p_i — простое число).
   $a_i^{n-1} \equiv 1 \pmod n \Rightarrow (n-1) \vdots (p_i - 1)$ для всех i, что и требовалось доказать.

3. Доказателство утверждения 3.

   $k \neq 1$ — по определению 2 (так как число Кармайкла — составное).

   Пусть $k = 2$. Тогда $n = p \cdot q$, где p, q — простые числа.

   Пусть $p < q$. $n - 1 = p \cdot (q-1) + p - 1 \equiv (p-1) \pmod{(q-1)} \Rightarrow (n-1) \not\vdots (q-1)$ (так как $p < q$).

   Получили противоречие с утверждением 2 данной теоремы. Значит $k \neq 2$.

   Таким образом, получили, что $k \geq 3$, что и требовалось доказать.

Доказательство теоремы закончено. □

Следствие 1. *Чисел Кармайкла бесконечно много.*

3. Тест Соловей–Штрассена

Теорема 3. *Пусть n — нечетное. Тогда для того, чтобы n было простым необходимо и достаточно, чтобы для каждого $a \in \mathbb{Z}_n^*$ было выполнено $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$.*

Доказательство. Необходимость следует из критерия Эйлера для символа Лежандра.

Докажем достаточность методом от противного.

Пусть $\forall a \in \mathbb{Z}_n^*\colon\ a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$, но n — составное.

$a^{n-1} = (a^{\frac{n-1}{2}})^2 \equiv \left(\frac{a}{n}\right)^2 \pmod{n}$

$\left(\frac{a}{n}\right)^2 = 1 \Rightarrow a^{n-1} \equiv 1 \pmod{n}$

Таким образом, n — число Кармайкла (по определению 2).

Следовательно, $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$, где p_i — простое число, $i = \overline{1,k}$ (по теореме (1))

Рассмотрим b такое, что $\left(\frac{b}{p_1}\right) \equiv -1 \pmod{n}$

Найдем такое a, что:

$$\begin{cases} a \equiv b \pmod{p_1} \\ a \equiv 1 \pmod{p_i}, \quad i = \overline{2,k} \end{cases}$$

Такое a существует по китайской теореме об остатках и принадлежит $\mathbb{Z}_n^*$ (так как взаимно просто с n).

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdot \underbrace{\left(\frac{a}{p_2}\right) \cdot \dots \cdot \left(\frac{a}{p_k}\right)}_{1} = \left(\frac{a}{p_1}\right) = \left(\frac{b}{p_1}\right) = -1$$

$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$

$\left(\frac{a}{n}\right) = -1 \Rightarrow a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$

$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) = -1 \pmod{p_1}$

$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) = -1 \pmod{p_2}$ (противоречие с тем, что $a \equiv 1 \pmod{p_i}$ $i = \overline{2,k}$)

Значит, неверно наше предположение о том, что n — составное. □

Определение 4. Нечетные составные числа n, для которых $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ для фиксированного a называются *эйлеровыми псевдопростыми числами по* $\mod a$.

4. Алгоритм Соловей-Штрассена

Вход: n — нечетное число

Выход: Сообщение о непростоте или возможной простоте числа

```
1: for i = 1, ..., k do
2:    a := rand(2, ...,n − 1);
3:    if НОД(a, n) > 1 then
4:       PRINT 'n — составное';
5:       RETURN;
6:    if a^((n−1)/2) ≢ (a/n) then
7:       PRINT 'n — составное';
8:       RETURN;
9: PRINT 'n — вероятно простое'
```

Вероятность ошибки, если выдан ответ 'вероятно простое', не превосходит $\left(\frac{1}{2}\right)^k$

Теорема 4. *Пусть n — нечетное составное. Тогда*

1. *Если n — эйлерово псевдопростое по основанию $a \in \mathbb{Z}_n^*$, то оно псевдопростое по основанию a;*
2. *Если n — эйлерово псевдопростое по основаниям a, $b \in \mathbb{Z}_n^*$, тогда n — эйлерово псевдопростое по основаниям $a \cdot b$ и $a \cdot b^{-1}$;*
3. *$E_n = \left\{a \in \mathbb{Z}_n^*\colon a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}\right\}$ — подгруппа в $\mathbb{Z}_n^*$;*

4. *Если n не является Эйлеровым псевдопростым по какому-либо основанию, тогда* $|E_n| \leq \frac{1}{2}|\mathbb{Z}_n^*|$.