Курс Дмитрия Ильинского

Тест Ферма

Через $\mathbb{Z}_n$ обозначается *система вычетов*, т.е. множество остатков по модулю n, $\mathbb{Z}_n^*$ — приведённая система вычетов, то есть множество остатков, взаимно-простых с n.

В этом листке есть задачи, рассказанные на лекции (они помечены кружком). Они стоят 1 балл. Задачи, не отмеченные кружком стоят 5 баллов. Для получения зачёта по этому листку достаточно набрать 15 баллов.

1°. Если $n = p$ — простое число, то

а) для любого $a \in \mathbb{Z}$ верно, что $a^n \equiv a \pmod n$;

б) если $(a, n) = 1$, то $a^{n-1} \equiv 1 \pmod n$.

Пусть $B_n = \{a \in \mathbb{Z}_n \mid (a, n) = 1, a^{n-1} \equiv 1 \pmod n\}$.

2°. Либо $B_n = \mathbb{Z}_n^*$, либо $|B_n| \leqslant \frac{1}{2}|\mathbb{Z}_n^*|$.

Числом Кармайкла называется такое число $n > 1$, что $B_n = \mathbb{Z}_n^*$.

3°. Пусть n — число, свободное от квадратов и для любого простого делителя $p \mid n$ верно, что $n-1$ делится на $p-1$. Тогда n — число Кармайкла.

4°. Пусть $n = p^k \cdot d$, где $(d, p) = 1$, p — простое и $k \geqslant 2$. **а)** Найдётся число a с условием: $a \equiv 1+p \pmod{p^k}$, $a \equiv 1 \pmod d$. **б)** n не может быть числом Кармайкла.

5°. Пусть n — число Кармайкла. Тогда

а) n свободно от квадратов (т.е. не делится на p^2 для простого p).

б) если n делится на простое число p, то $n - 1$ делится на $p - 1$.

6. n является числом Кармайкла тогда и только тогда, когда для любого $a \in \mathbb{Z}$ верно, что $a^n \equiv a \pmod n$.

7. Число Кармайкла является нечётным.

8. Пусть для натурального числа k числа $6k + 1$, $12k + 1$, $18k + 1$ являются простыми. Тогда число $(6k + 1) \cdot (12k + 1) \cdot (18k + 1)$ является числом Кармайкла.

Первообразные корни

В этом листке p — нечётное простое число.

Назовём *показателем* $\operatorname{ord}(x)$ элемента $x \in \mathbb{Z}_m^*$ такое минимальное $k \geqslant 1$, что $x^k = 1$.

9°. Докажите, что для каждого $x \in \mathbb{Z}_m^*$ показатель существует.

10°. Найдите показатель **а)** $1 \in \mathbb{Z}_m$; **б)** $-1 \in \mathbb{Z}_m$ **в)** всех элементов $\mathbb{Z}_m^*$ при $m = 4, 5, 6, 7$.

11°. Пусть $\operatorname{ord}(g) = k$, $g \in \mathbb{Z}_m$. Докажите, что

а) $1, g, g^2, \ldots, g^{k-1} \in \mathbb{Z}_m$ — попарно различные числа;

б) если $k \mid l - l'$, то $g^l = g^{l'}$;

в) $g^s = 1 \Leftrightarrow k \mid s$;

г) $\varphi(m) \vdots k$.

12°. Докажите, что $\operatorname{ord}(g^l) = \dfrac{\operatorname{ord}(g)}{(l, \operatorname{ord}(g))}$.

Число g называется *первообразным корнем* по модулю m, если $\operatorname{ord}(g) = \varphi(m)$.

13°. Найдите все первообразные корни для $\mathbb{Z}_m$, $m \leqslant 7$.

14.

а)° Пусть $\operatorname{ord}(g) = k$, $\operatorname{ord}(h) = m$ и $(k, m) = 1$. Тогда $\operatorname{ord}(gh) = km$.

б)° Пусть $\operatorname{ord}(g) = k$, $\operatorname{ord}(h) = m$. Найдётся элемент x, у которого показатель равен $\text{НОК}((k, m))$.

в)° Пусть $\operatorname{ord}(1) = k_1, \ldots, \operatorname{ord}(p-1) = k_{p-1}$. Найдётся элемент x, у которого показатель равен $\tau = \text{НОК}((k_1, \ldots, k_{p-1}))$.

г) Для каждого остатка $a \in \{1, \ldots, p-1\}$ верно, что $a^\tau \equiv 1 \pmod p$.

15. (*Теорема Лагранжа*) Многочлен $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ не может иметь больше n корней в $\mathbb{Z}_p$. **а)** Предположим, что теорема не верна, и найдутся корни $\alpha_1, \ldots, \alpha_{n+1}$. Покажите, что многочлен можно переписать в виде $f(x) = (x - \alpha_1) \ldots (x - \alpha_n) + b_{n-1}(x - \alpha_1) \ldots (x - \alpha_{n-1}) + \ldots + b_0$ для некоторых $b_{n-1}, \ldots, b_0 \in \mathbb{Z}_p$. **б)** Покажите, что $b_{n-1} = \ldots = b_0 = 0$. **в)** Покажите, что $(\alpha_{n+1} - \alpha_1) \ldots (\alpha_{n+1} - \alpha_n) = 0$, и приведите к противоречию

16°. Из последних двух задач выведите теорему о существовании первообразного корня: для каждого p найдётся a с $\operatorname{ord}(a) = p - 1$.

Курс Дмитрия Ильинского

Для зачёта по этому листку достаточно набрать 25 баллов. Задачи с кружком были на лекции и стоят 3 балла, без кружка — 5 баллов, со звездочкой — 15 баллов. Зачёт по курсу ставится, если имеется зачёт по обоим листкам.

Определение 1. Пусть p — простое число. Будем говорить, что a является *квадратичным вычетом по модулю* p , если $(a,p)=1$ и найдётся такой $x \in \mathbb{Z}_p$, что $a = x^2$, и *квадратичным невычетом*, если $(a,p)=1$ и такого $x \in \mathbb{Z}_p$, что $x^2 = a$ не существует.

Определение 2. Для простого нечётного p назовём *символом Лежандра* следующее выражение:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a \text{ — квадратичный вычет по модулю } p; \\ -1, & \text{если } a \text{ — квадратичный невычет по модулю } p; \\ 0, & \text{если } (a,p) \neq 1. \end{cases}$$

Читается: символ a по p.

Для символа Лежандра выполнены следующие тождества:

(1) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, если $a \equiv b \pmod p$.

(2) $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$

(3) Если $a = p_1 \dots p_s$, то $\left(\frac{a}{p}\right) = \left(\frac{p_1}{p}\right) \dots \left(\frac{p_s}{p}\right)$

(4) $\left(\frac{1}{p}\right) = 1$, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

(5)[Закон квадратичной взаимности] Для p, q —нечётных простых $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

Определение 3. Пусть m — нечётное число, $m = p_1 \dots p_s$. Назовём *символом Якоби* следующее выражение:

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_s}\right)$$

Для символа Якоби выполнены свойства (1)-(5), (в свойстве (5) надо брать нечётные p, q).

1. Пусть m — нечётное, $m = p_1 \dots p_s$. Тогда

а) $\frac{m-1}{2} = \frac{p_1-1}{2} + \frac{p_2-1}{2} + \dots + \frac{p_s-1}{2} + 2N$ для некоторого N.

б) $\frac{m^2-1}{8} = \frac{p_1^2-1}{2} + \frac{p_2^2-1}{2} + \dots + \frac{p_s^2-1}{2} + 2N$ для некоторого N.

в) Из свойства (3) для символа Лежандра следует свойство (3) для символа Якоби.

г) Из свойства (4) для символа Лежандра следует свойство (4) для символа Якоби.

д)* Из свойства (5) для символа Лежандра следует свойство (5) для символа Якоби.

Положим

$$B_{SS}(n) = \{a \mid a \text{ — нечётное, взаимно-простое с } n \text{ и } a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod n\}.$$

2. (*Тест Соловея-Штрассена*) Для нечётного n

а)° $B_{SS}(n) \subset B_n$.

б)° Если $B_{SS}(n) = \mathbb{Z}_n^*$, то n — простое.

в)° Если $B_{SS}(n) \neq \mathbb{Z}_n^*$, то $|B_{SS}(n)| \leqslant \frac{1}{2}|\mathbb{Z}_n|^*$.

Пусть $n - 1 = 2^l \cdot m$ для некоторой степени k и нечётного числа m. Рассмотрим множество

$$B_{MR}(n) = \{a \in \mathbb{Z}_n^* \mid a^m = 1 \text{ или } a^{m2^k} = -1 \text{ для некоторого } 0 \leqslant k < l\}.$$

3. (*Тест Миллера-Рабина*) Для нечётного n

а)° $B_{MR}(n) \subset B_n$

б)° Если $B_{MR}(n) = \mathbb{Z}_n^*$, то n — простое.

4.

а) Если $n \equiv 3 \pmod 4$, то $B_{MR}(n) \subset B_{SS}(n)$.

б)* Если $n \equiv 1 \pmod 4$, то $B_{MR}(n) \subset B_{SS}(n)$.

Теорема 1. (Миллер-Рабин) *Если $n > 9$ — нечётное составное число, то $|B_{MR}(n)| \leqslant \frac{1}{4}|\mathbb{Z}_n^*|$.*

Теорема 2. *(б/д) Для любого α по модулю p^α существует первообразный корень g.*

5. Докажите теорему в случае, когда $n = p^\alpha$ — степень простого числа.

Обозначим через M_0 множество остатков $a \in \mathbb{Z}_n$, для которых $a^m \equiv 1 \pmod n$, M'_k — множество чисел $a \in \mathbb{Z}_n$, для которых $a^{m \cdot 2^k} \equiv -1 \pmod n$, $k = 0, \ldots, l-1$.

6.

а) $|M_0| = |M'_0|$.

б) $B_{MR} = M_0 \cup M'_0 \cup M'_1 \cup \ldots \cup M'_k$.

в) Пусть n содержит в разложении k простых $p_1, \ldots p_s$. Обозначим через N_k множество остатков $a \in \mathbb{Z}_n$, для которых $a^{m \cdot 2^k} \equiv \pm 1 \pmod{p_i}$ для всех $i = 1, \ldots, s$, причём хотя бы по одному модулю 1, и по одному -1. Тогда $|N_k| = 2^s |M'_k|$, $N_k \cap M'_k = \emptyset$.

г) Если $s \geqslant 3$, то $|B_{MR}| \leqslant \frac{1}{6}|\mathbb{Z}_n^*|$.

д) Если $s = 2$, то $|B_{MR}| \leqslant \frac{1}{4}|\mathbb{Z}_n^*|$.

Источники литературы

Хорошие записки по всем вероятностным тестам есть у Keith Conrad (легко ищутся поиском).

http://www.math.uconn.edu/ kconrad/blurbs/ugradnumthy/solovaystrassen.pdf

http://www.math.uconn.edu/ kconrad/blurbs/ugradnumthy/millerrabin.pdf

http://www.math.uconn.edu/ kconrad/blurbs/ugradnumthy/carmichaelkorselt.pdf

Также неплохой обзор есть у Rene Schoof (доступен в интернете)

Rene Schoof *Four primality testing algorithms* // Algorithmic Number Theory MSRI Publications Volume 44, 2008

На русском языке есть курс Богопольского

Спецкурс «Алгоритмическая теория чисел и элементы теории криптографии» (доступ по интернету: *http://math.nsc.ru/ bogopolski/Articles/SpezkNumber.pdf*), Лекция 8.