1 Индексы. Экспоненциальные сравнения.

1.1 Индексы.

Определение. Пусть $n = p^\alpha$ или $n = 2p^\alpha$, где p - простое нечётное и g - некоторый первообразный корень по модулю n, а a - некоторое число взаимнопростое с n. Тогда минимальное неотрицательное c, такое что $g^c \equiv a(mod\, n)$ разывается *индексом числа a по модулю n при основании g.* Данный индекс будем обозначать как $ind_g a$, то есть $c = ind_g a$.

Замечание. Нетрудно видеть, что $0 \leq ind_g a \leq \varphi(n) - 1$.

Пример. Как было показано в предыдущей лекции 2 - первообразный корень по модулю 9. Тогда индекс 4 по модулю 9 при основании 2 равен 2, то есть $ind_2 4 = 9$. Аналогично $ind_2 1 = 0$, $ind_2 2 = 1$, $ind_2 5 = 5$, $ind_2 7 = 4$, $ind_2 8 = 3$.

Замечание. Отметим, что данное определение введено корректно, то есть такой индекс всегда существует и единственен. Это следует из того факта, что множество $\{g, g^2, \ldots, g^{\varphi(n)}\}$ образует приведённую систему вычетов. Тогда отображение $\psi : a \to ind_g a$ является биекцией между приведённой системой вычетов по модулю n и $\{0, 1, \ldots, \varphi(n) - 1\}$.

Свойства:

1)$g^{ind_g a} \equiv a(mod\, n)$.

2)$ind_g a^m \equiv m\, ind_g a(mod\, \varphi(n))$ для любого натурального m.

Доказательство

Пусть $ind_g a = c$, $ind_g a^n = C$. Тогда $g^{cm} \equiv a^m(mod\, n)$ и $g^C \equiv a^m(mod\, n)$. Отсюда получаем $g^{cm} \equiv g^C(mod\, n)$. Исходя из того, что g - первообразный корень, получаем, что $cm \equiv C(mod\, \varphi(n))$.

3)$ind_g ab \equiv ind_g a \cdot ind_g b(mod\, \varphi(n))$.

Доказательство.

Пусть $ind_g a = c_1$, $ind_g b = c_2$, $ind_g ab = C$. Тогда $g^{c_1+c_2} \equiv ab(mod\, n)$ и $g^C \equiv ab(mod\, n)$. Отсюда получаем, что $g^{c_1+c_2} \equiv g^C(mod\, \varphi(n))$. Исходя из того, что g - первообразный корень, получаем, что $c_1 + c_2 \equiv C(mod\, \varphi(n))$.

4)$ind_g \left(\prod_{i=1}^{r} a_i^{m_i} \right) = \sum_{i=1}^{r} m_i ind_g a_i$ для любых положительных чисел m_i.

5)Пусть g_1, g_2 - два первообразных корня по модулю n. Тогда

$$ind_{g_1} a \cdot ind_{g_2} g_1 \equiv ind_{g_2} a(mod\, \varphi(n)).$$

Доказательство

Пусть $ind_{g_1} a = c_1$, $ind_{g_2} a = c_2$ и $ind_{g_2} g_1 = C$. Тогда $g_1 \equiv g_2^C(mod\, n)$ и $a \equiv g_1^{c_1}(mod\, n)$. Отсюда получаем, что $a \equiv g_1^{Cc_1}(mod\, n)$. Таким образом, $Cc_1 \equiv c_2(mod\, \varphi(n))(mod\, n)$, что и требовалось доказать.

6) Пусть g_1, g_2 - два првообразных корня, тогда

$$ind_{g_1} g_2 \cdot ind_{g_2} g_1 \equiv 1(mod\, \varphi(n)).$$

Доказательство

Следует из предыдущего свойства при $a = g_2$.

7)$ind_g 1 = 0$, $ind_g g^m = m$, $ind_g a = ind_g(a + nk), k, m \in \mathbb{N}$.

8)Пусть число a принадлежит показателю δ по модулю n. Тогда

$$\delta = \frac{\varphi(n)}{(\varphi(n), ind_g a)}.$$

Пример. Для начала покажем, что 2 - первообразный корень по модулю 27. Действительно $\varphi(27) = 18 = 3^2 \cdot 2$ и $2^6 \not\equiv 1(mod\,18)$, $2^9 \not\equiv 1(mod\,18)$. Тогда по свойству 2 получаем $ind_2 13 \equiv ind_2 256 \equiv 8 ind_2 2 \equiv 8(mod\,18)$, то есть $ind_2 13 = 8$. Также $ind_2 5 \equiv ind_2 32 \equiv 5(mod\,18)$, то есть $ind_2 5 = 5$. Отсюда по свойству 7 получаем, что 5 также первообразный корень по модулю 27.

Тогда $ind_5 13 \equiv ind_2 13 \cdot ind_5 2 \equiv ind_2 13 \cdot (ind_2 5)^{-1} \equiv 11 \cdot 8 \equiv 16(mod\,18)$. Таким образом $ind_5 13 = 16$.

По свойству 3 получаем $ind_2 11 \equiv ind_2 65 \equiv ind_2(13 \cdot 5) \equiv ind_2 13 + ind_2 5 \equiv 13(mod\,18)$. Таким образом $ind_2 11 = 13$.

Лемма. По модулю $n = 2^\alpha$, $\alpha > 2$ не существует первообразных корней.

Доказательство

Рассмотрим произвольное нечётное число a. Пусть оно принадлежит показателю δ по модулю 2^α. Тогда $\delta | \varphi(n)$ и $\delta = 2^k$, $k \in \{0, 1, \ldots, \alpha - 1\}$. Отметим, что $a^2 \equiv 1(mod\,8)$, так как $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1(mod\,8)$. Тогда

$$a^2 = 1 + 8t_1,$$

Тогда $a^4 \equiv 1 + 16t_2$ и так далее:

$$a^8 = 1 + 32t_3,$$

$$\ldots\ldots$$

$$a^{2^{\alpha-2}} = 1 + 2^\alpha t_{\alpha-2} \equiv 1(mod\,2^\alpha).$$

Таким образом, $\delta \neq 2^{\alpha-1}$.

Теорема. Множество $\{(-1)^{c_0} 5^{c_1} | 0 \leq c_0 \leq 1, 0 \leq c_1 \leq 2^{\alpha-2} - 1\}$ образует приведённую систему вычетов по модулю $n = 2^\alpha$, $\alpha > 2$.

Доказательство

Отметим, что это очевидно при $\alpha = 1, 2$. Пусть далее $\alpha > 2$. Пусть δ - показатель которому принадлежит 5 по модулю n. Покажем, что $\delta = 2^{\alpha-2}$. Действительно

$$5 = 1 + 4$$

$$5^2 = 1 + 8 + 16$$

$$5^4 = 1 + 16 + 32u_2$$

$$\ldots\ldots$$

$$5^{2^{\alpha-3}} = 1 + 2^{\alpha-1} + 2^\alpha u_{\alpha-3}$$

$$5^{2^{\alpha-2}} = 1 + 2^\alpha + 2^{\alpha+1} u_{\alpha-2} \equiv 1(mod\,n).$$

Покажем, что все эти степени 5 за исключением последней несравнимы с 1 по модулю n. Предположим, что это не так, то есть существует $i <$

$\alpha - 2$, такое что $5^i \equiv 1(mod\, n)$. Но тогда $1 + 2^{i+2} + 2^{i+3}u_i \equiv 1(mod\, n)$, то есть $2^\alpha | 2^{i+2} + 2^{i+3}u_i$, что очевидно неверно. Получаем противоречие. Таким образом $\delta = 2^{\alpha-2}$. Тогда рассмотрим следующий набор чисел

$$1,\ 5,\ 5^2, \ldots, 5^{2^{\alpha-2}-1},$$

$$-1,\ -5,\ -5^2, \ldots, -5^{2^{\alpha-2}-1}.$$

Заметим, что их количество равно $2^{\alpha-1}$. Покажем, что они все попарно несравнимы по модулю n. Понятно, что числа из одной строчки попарно несравнимы по модулю n исходя из свойств показателей. Числа из разных строк не сравнимы так как все числа из первой строки сравнимы с 1 по модулю 4, а все со второй сравнимы с -1 по модулю 4. Таким образом все эти числа образуют приведённую систему вычетов по модулю n.

Замечание. Вместо 5 можно рассматривать 3, Теорема всё также будет верна. Доказательство аналогичное.

Метод использованный в данной теореме может быть полезен при решении некоторых задач:

Задача. Покажите, что 2 является первообразным корнем по модулю 3^n.

Решение

Заметим, что $\varphi(3^n) = 2 \cdot 3^{n-1}$. Тогда $\delta = 2 \cdot 3^k$ либо $\delta = 3^k$, $k \in \{0, \ldots, n-1\}$. Также заметим, что

$$2^2 = 1 + 3.$$

Возведём в куб: $2^{2\cdot 3} = 1 + 3^2 + 2 \cdot 3^3$ и продолжим:

$$2^{2\cdot 3^2} = 1 + 3^3 + 3^4 u_0,$$

$$\ldots\ldots$$

$$2^{2\cdot 3^{n-2}} = 1 + 3^{n-1} + 3^n u_{n-2},$$

$$2^{2\cdot 3^{n-1}} = 1 + 3^n + 3^{n+1} u_{n-1} \equiv 1(mod\, 3^n).$$

Покажем, что все эти степени 3 за исключением последнего не сравнимы с 1 по модулю 3^n. Предположим, что это не так, то есть существует $i < n-1$, такое что $3^i \equiv 1(mod\, n)$. Но тогда $1 + 3^{i+1} + 3^{i+2}u_i \equiv 1(mod\, n)$, то есть $3^n | 3^{i+1} + 3^{i+2}u_i$, что очевидно неверно. Получаем противоречие. Таким образом $\delta \neq 2 \cdot 3^k$. Если же $\delta = 3^k, k < n-1$, то $3^{2\delta} = 3^{2\cdot 3^k} \equiv 1(mod\, n)$, что как мы доказали неверно.

Таким образом $\delta = 3^{n-1}$ либо $\delta = 2 \cdot 3^{n-1}$. Заметим, что $2^{3^{n-1}} \equiv (-1)^{3^{n-1}} \equiv -1(mod\, n)$ Таким образом, $\delta = 3^{n-1}$ - не является показателем, которому принадлежит 2 по модулю 3^n.

Значит $\delta = 2 \cdot 3^{n-1}$, то есть 2 - первообразный корень.

Определение. Пусть $n = 2^\alpha, \alpha > 1$ и a - некоторое число взаимнопростое с n. Тогда пару неотрицательных чисел $(c_0, c_1), 0 \leq c_0 \leq 1, 0 \leq c_1 \leq 2^{\alpha-2} - 1$ будем называть *системой индексов числа a по модулю n*, если

$(-1)^{c_1}5^{c_2} \equiv a(mod\, n)$. В случае $\alpha = 0, 1$ такой системой индексов будем считать пару $(0, 0)$.

Замечание. Отметим, что данное определение задано корректно, то есть для каждого числа существует система индексов и она единственна. Для $\alpha > 2$ это следует из Теоремы, для $\alpha = 1, 2$ это можно получить непосредственной проверкой. Тогда отображение $\psi : a \to (c_0, c_1)$ является биекцией между приведённой системой вычетов по модулю n и $\{0, 1\} \times \{0, 1, \ldots, 2^{\alpha-2} - 1\}$.

Замечание. Из этой теоремы следует то, что $\mathbb{Z}_{2^\alpha} \simeq \mathbb{Z}_{2^{\alpha-2}} \times \mathbb{Z}_2$ для $\alpha > 2$. Изоморфизмом будет являться отображение ψ.

Пример. Рассмотрим $n = 32$. Тогда система индексов числа 17 по модулю 32 равна $(0, 4)$, так как $5^4 \equiv 17(mod\, 32)$. Система индексов числа 15 по модулю 32 равна $(1, 4)$, так как $(-1)^1 5^4 \equiv 15(mod\, 32)$.

Система индексов чисел 1 и 3 по модулю 4 равны $(0, 0)$ и $(1, 0)$ соответственно.

Определение. Пусть $n = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}, \alpha_0 \neq 0$, где p_i - простые нечётные и a - некоторое число взаимнопростое с n, g_i - первообразный корень по модулю $p_i^{\alpha_i}$, $i \in \overline{1, r}$. Тогда упорядоченный набор $(c, c_0, c_1, \ldots, c_r)$ будем называть *системой индексов числа a по модулю n*, если (c, c_0) - система индексов числа a по модулю 2^{α_0}, а $c_i = ind_{g_i} a$, $i \in \overline{1, r}$, .

Замечание. Иногда в случае $\alpha_0 = 0, 1$ рассматривается система индексов $(c_1, \ldots, c_r)$.

Замечание. Зафиксируем некоторые $g_1, g_2, \ldots, g_r$. Исходя из ранее приведённых замечаний касательно определений индекса и системы индексов по модулю степени двойки получаем, что каждому числу соответствует единственная система индексов. Действительно, пусть одному и тому же числу a, соответствует две разных системы индексов, у которых не совпадают i-тые значения. Тогда мы получим, что у числа есть два разных индекса по модулю $p_i^{\alpha_i}$ либо две разные системы индексов по модулю 2^{α_0}, что неверно. Существование такой системы индексов следует из того, что для любого a взаимнопростого с n существуют (c, c_0), такие что $a \equiv (-1)^c 5^{c_0} (mod\, 2^{\alpha_0})$; $c_i, i \in \overline{1, r}$, такие что $a \equiv g_i^{c_i} (mod\, p_i^{\alpha_i})$.

Тогда отображение $\psi : a \to (c, c_0, c_1, \ldots, c_r)$ является биекцией между приведённой системой вычетов по модулю n и соответствующим множеством.

Пример. Найдём какую-нибудь систему индексов 157 по модулю 1144. Разложим 1144 на множители: $1144 = 2^3 \cdot 11 \cdot 13$. Найдём индексы и системы индексов 157 по модулю 8, 11 и 13 соответственно.

$157 \equiv 5 \equiv (-1)^0 5^1 (mod\, 8)$. Заметим, что 2 - первообразный корень по модулю 11 и 13, так как $\varphi(11) = 2 \cdot 5$ и $2^2 \not\equiv 1(mod\, 11)$, $2^5 \not\equiv 1(mod\, 11)$; $\varphi(13) = 2^2 \cdot 3$ и $2^4 \not\equiv 1(mod\, 13)$, $2^6 \not\equiv 1(mod\, 13)$.

$ind_2 157 \equiv ind_2 3 \equiv 8(mod\, 10)$, $ind_2 157 \equiv ind_2 1 \equiv 0(mod\, 12)$. Получаем, что $(0, 1, 8, 0)$ - система индексов 157 по модулю 1144.

Найдём систему индексов 7 по модулю 1144. $7 \equiv (-1)5^0 (mod\, 8)$, $ind_2 7 = 7(mod\, 10)$, $ind_2 7 \equiv 11(mod\, 12)$. Таким образом $(1, 0, 7, 11)$ - система индексов 7 по модулю 1144.

1.2 Экспоненциальные сравнения.

Рассмотрим показательное сравнение $a^x \equiv b(mod\, n)$, $(a,n) = (b,n) = 1$. Пусть $n = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ - каноническое разложение n. Тогда исходное сравнение равносильно системе сравнений $a^x \equiv b(mod\, 2^{\alpha_0})$, $a^x \equiv b(mod\, p_i^{\alpha_i})$, $i = \overline{1,r}$. Пусть $(\gamma, \gamma_0, \gamma_1, \dots, \gamma_r)$ и $(\delta, \delta_0, \delta_1, \dots, \delta_r)$ системы индексов a и b соответственно. То есть $a \equiv (-1)^{\gamma} 5^{\gamma_0} (mod\, 2^{\alpha_0})$, $a \equiv g_i^{\gamma_i} (mod\, p_i^{\alpha_i}), i \in \overline{1,r}$ и $b \equiv (-1)^{\delta} 5^{\delta_0} (mod\, 2^{\alpha_0})$, $b \equiv g_i^{\delta_i} (mod\, p_i^{\delta_i}), i \in \overline{1,r}$, где g_i - первообразные корни по модулю $p_i^{\alpha_i}$. Тогда получаем, что данное сравнение равносильно следующей системе линейных сравнений:

$$\begin{cases} x\gamma \equiv \delta (mod\, c) \\ x\gamma_0 \equiv \delta_0 (mod\, c_0) \\ x\gamma_i \equiv \delta_i (mod\, c_i), i \in \overline{1,r} \end{cases}$$

где $c_i = \varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1}$, $i \in \overline{1,r}$,

$$c = \begin{cases} 2, \alpha_0 \geq 2 \\ 1, \alpha = 0,1 \end{cases}$$

$$c_0 = \begin{cases} 2^{\alpha_0 - 2}, \alpha_0 \geq 2 \\ 1, \alpha = 0,1 \end{cases}$$

Данная система может быть решена с помощью китайской теоремы об остатках.

Замечание. Заметим, что от сравнения $a^x \equiv b(mod\, n)$, где a и b не обязательно взаимнопросты с n без особого труда можно перейти к сравнению рассмотренному ранее.

Задача. Решить сравнение $157^x \equiv 7(mod\, 1144)$.

Решение

Как ранее было доказано, $1144 = 2^3 \cdot 11 \cdot 13$. А также найдены системы индексов 157 и 7 соответственно: $(0,1,8,0)$ и $(1,0,7,11)$. Нетрудно видеть $c = 2$, $c_0 = 2$, $c_1 = 10$, $c_2 = 12$. Таким образом мы сводим экспоненциальное сравнение к следующей системе линейных сравнений:

$$\begin{cases} 0x \equiv 1 (mod\, 2) \\ x \equiv 0 (mod\, 2) \\ 8x \equiv 7 (mod\, 10) \\ 0x \equiv 11 (mod\, 12) \end{cases}$$

Очевидно это сравнение не имеет решений.

Возможен и другой подход к решению таких сравнений:

Задача. Решить сравнение $5^x \equiv 229(mod\, 1001)$.

Решение.

Заметим, что $1001 = 7 \cdot 11 \cdot 13$. Тогда исходное сравнение можно записать как систему

$$\begin{cases} 5^x \equiv 229 (mod\, 7) \\ 5^x \equiv 229 (mod\, 11) \\ 5^x \equiv 229 (mod\, 13) \end{cases}$$

Пусть δ_m - показатель, которому принадлежит 5 по модулю m. Тогда $\delta_m | \varphi(m)$. Пользуясь этим, находим $\delta_7 = 6$, $\delta_{11} = 5$ и $\delta_{13} = 4$. Также отметим, что $5 \equiv 229 (mod\, 7)$, $229 \equiv 9 \equiv 5^4 (mod\, 11)$ и $229 \equiv 8 \equiv 5^3 (mod\, 13)$. Тогда исходная истема эквивалентна

$$\begin{cases} x \equiv 1 (mod\, 6) \\ x \equiv 4 (mod\, 5) \\ x \equiv 3 (mod\, 4) \end{cases}$$

Что равносильно

$$\begin{cases} x \equiv 1 (mod\, 3) \\ x \equiv 4 (mod\, 5) \\ x \equiv 3 (mod\, 4) \end{cases}$$

Используя китайскую теорему об остатках получаем, что $x \equiv 19 (mod\, 60)$, то есть $x = 19 + 60$, $k \in \mathbb{N}_0$.

Замечание. Если x_0 - некоторое решение сравнения $a^x \equiv b (mod\, n)$, $(a, n) = (b, n) = 1$, то все решения могут описаны следующим образом $x = x_0 + k\delta$, $k \in \mathbb{N}$, где δ - показатель, которому принадлежит a по модулю n.

1.3 Задачи для самостоятельного решения.

Задача 1

а)Найдите две различные системы индексов 7 по модулю 120.
б)Решите сравнение $3^x \equiv 92 (mod\, 143)$.

Задача 2

а)Докажите, что 2 - первообразный корень по модулю 5^n.
b)Найдите первообразный корень по модулю 7^n.