# ЛЕКЦИЯ 9.
# Основные понятия теории чисел

**9.1. Делители и простые числа.**

**9.2. Арифметика в классах вычетов.**

**9.3. Теорема Эйлера.**

**9.4. Дискретные логарифмы.**

**Обозначения:**

- ***N*** - множество **натуральных** чисел: целые положительные числа вида 1,2,…;
- ***Z*** - множество **целых** чисел: числа вида ***n***, ***-n*** и 0, где ***n*** - натуральное число;
- ***Q*** - множество **рациональных** чисел: числа вида ***p/q***, где ***p*** и ***q*** - целые числа и $q \neq 0$

Число ***a*** делится на число ***b*** $\neq$ 0, если существует число ***q*** такое, что $\frac{a}{b} = q \quad или \quad a = bq$

Число ***b*** - ***делитель*** числа ***a***, число ***a*** - ***кратное*** числа ***b***, число ***q*** - ***частное от деления a*** на ***b***.

Утверждение о том, что ***b*** делит ***a*** обозначают символом $b/a$. Если ***b*** не делит ***a***, то этот факт обозначают $b/a$.

***Лемма 1***. Если $c/b$ и $b/a$, то $c/a$

***Лемма 2***. Если ***m=a+b***, ***d/m*** и ***d/a***, то ***d/a***.

***Общим делителем*** двух или нескольких чисел называется число, являющееся делителем каждого из этих чисел.

***Наибольшим общим делителем (НОД)*** чисел $a_1,\ldots,a_n$ называется наибольший из их общих делителей - обозначается как $(a_1,\ldots,a_n)$

Число ***n>1*** называется ***простым,*** если оно не имеет других делителей, кроме ***1*** и ***n***.

*Например, числа 2, 3, 5, 7 являются простыми, т.к. они делятся только на 1 и на самих себя.*

Число ***n*** называется ***составным,*** если оно имеет делитель, отличный от 1 и ***n***.

*Например, числа 4, 6, 8 − составные числа.*

Если НОД $(a_1,\ldots,a_n) = 1$ , то числа $a_1,\ldots,a_n$ называют ***взаимно простыми.***

*Например: (2,5)=1; (10,21)=1.*

***Лемма 3.*** Если целое число ***b*** взаимно просто с каждым из целых чисел $a_1,\ldots,a_n$ , то ***b*** взаимно просто с их произведением $a_1 \times a_2 \times \ldots \times a_n$

***Теорема о делении с остатком.*** ***Если a и b целые числа, и b>0, то существуют единственные целые числа q и r такие, что a=b x q+r,*** $0 \le r < b$

Число ***q*** называют *неполным частным* при делении ***a*** на ***b***, число ***r*** называют **остатком** от деления ***a*** на ***b***.

***Лемма 4***. **Наименьший,** отличный от единицы, делитель натурального числа ***n>1*** есть ***простое число***.

***Следствие.*** Каждое натуральное число ***n***>1 имеет хотя бы *один* простой делитель.

***Лемма 5.*** Если ***p*** - простое число, то любое целое число ***a*** либо взаимно простое с ***p***, либо делится на ***p,*** т. е. ***p/a.***

## *Основная теорема арифметики.*

Любое натуральное число ***n>1*** представляется в виде произведения простых чисел, причем, единственным образом.

Разложение числа ***n*** на простые сомножители:

$$n = p_1 \times p_2 \times \ldots \times p_r$$

Пусть $p_1,\ldots,p_к$ − различные из чисел $p_1,\ldots,p_r$ ($r>k$), а $\alpha_1,\ldots,\alpha_k$ − ***кратности***, *с которыми они входят в исходное разложение. Тогда это разложение можно записать в виде:*

$$n = p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot \ldots \cdot p_k^{\alpha k}, \quad \begin{cases} p_i - простое \\ \alpha_i - целые\ числа \end{cases}$$

и называется оно ***каноническим разложением*** числа ***n*** на простые множители.

*Пример.* $261360 = 2^4 \cdot 3^3 \cdot 5 \cdot 11^2$

Согласно *теореме Евклида*, **множество простых чисел бесконечно.**

## *Решето Эратосфена* :

− напишем одно за другим числа 2,3,…***N;***

− число 2 является простым − оставляем, и зачеркиваем после него все числа, *кратные 2,* т.е. все четные числа;

− следующим за числом 2 является число 3, которое является простым. Оставляем 3, зачеркиваем все числа, кратные 3;

− продолжая этот процесс, находим все простые числа, не превышающие заданного числа ***N***.

*Например**, N=40**:*

*2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40.*

***Простые** числа:*

*2,3,5,7,11,13,17,19,23,29,31,37.*

Особый класс простых чисел составляют числа вида $2^n - 1$ ***простые числа Мерсенна***

*В 1992 г. найдено 32−е число Мерсенна (Его запись содержит 227 832 цифры и требует около ста страниц текста).*

**Длина десятичной записи предыдущего открытого числа была *9808358*.**

# Арифметика в классах вычетов

Целые числа ***a*** и ***b*** (***a***,***b*** $\in z$) называются ***сравнимыми по модулю n*** $\in N$ (***n***$\neq 0$), если разность ***a и b*** делится на ***n,*** т. е. ***n***/***a-b***.

Сравнимость чисел ***a*** и ***b*** по модулю ***n*** обозначают символом $a \equiv b(\mathrm{mod}\,\mathbf{n})$, называемым ***сравнением по модулю n***.

Числа ***a*** и ***b*** сравнимы по модулю ***n*** тогда и только тогда, когда существует целое ***t***(***t*** $\in$ ***z***) такое, что $a = b + nt$

также и только тогда, когда они имеют одинаковые остатки ***r*** при делении на ***n,*** т.е. ***a = n*** $q_1$ ***+ r, b = n*** $q_2$ ***+ r.***

Т.е. все целые числа ***Z*** по модулю ***n*** разбиваются по ***n*** непересекающихся классов сравнимых между собой чисел (т.е. *имеющих одинаковые остатки при делении на* ***n***). Каждое число ***r,*** входящее в какой - либо из классов, называется ***вычетом*** числа ***a*** по модулю ***n***, а каждый класс - ***классом вычетов*** по модулю ***n***. Число разных классов вычетов равно ***n***.

**Полной системой вычетов** (по модулю ***n*** или ***m***) называют множество из ***m*** (или ***n***) целых чисел $\{r_1,\ldots,r_m\}$, если для любого целого числа ***a*** существует точно одно число $r_i \quad (i = 1,\ldots,m)$ из множества $\{r_1,\ldots,r_m\}$ такое, что $a = r_i(\mathrm{mod}\,m)$

Свойства

сравнений по модулю ***m*** (или ***n***) напоминают свойства обычных числовых равенств:

1. Два числа, сравнимые с третьим, сравнимы между собой.
2. Сравнения по одному и тому же модулю можно почленно складывать: $[a_1 + a_2](\mathrm{mod}\,m) = [a_1(\mathrm{mod}\,m) + a_2(\mathrm{mod}\,m)](\mathrm{mod}\,m)$
3. Сравнения по одному и тому же модулю можно почленно перемножать: $[a_1 \cdot a_2](\mathrm{mod}\,m) = [a_1(\mathrm{mod}\,m) \cdot a_2(\mathrm{mod}\,m)](\mathrm{mod}\,m)$

***Правила сокращения сравнений несколько отличаются от правил сокращения равенств.***

4. Если $aU \equiv aV(\mathrm{mod}\,m)$ и $(a,m) = 1$, то $U \equiv V(\mathrm{mod}\,m)$

   Если $aU \equiv aV(\mathrm{mod}\,am)$, то $U \equiv V(\mathrm{mod}\,m)$

Пример, когда это условие **не выполнено**:

$6 \times 3 = 18 \equiv 2 \bmod 8,$

$6 \times 7 = 42 \equiv 2 \bmod 8,$

Однако, $3 \neq 7 \bmod 8.$

Для произвольного модуля сравнения ***m*** (или ***n***) в результате умножения чисел от 0 до (***m*** - 1) на множитель *a* **не получается полного набора всех вычетов**,

Для произвольного модуля сравнения ***m*** (или ***n***) в результате умножения чисел от 0 до (***m*** - 1) на множитель *a* **не получается полного набора всех вычетов**, когда *a* и ***m*** имеют *общие множители*.

# *Алгоритм Евклида*

Алгоритм ***Евклида*** опирается на следующую теорему:
для любого неотрицательного целого числа ***a*** и любого положительного целого числа ***b*** справедливо следующее:

$$(a, b) = (b, a \bmod b). \qquad (9.2)$$

Чтобы определить наибольший общий делитель, равенство (9.2) можно использовать **повторно.**
В алгоритме ***Евклида*** **многократно** применяется равенство (9.2) для определения наибольшего общего делителя.

Пример. Чтобы найти **(1970,1066),** выполним следующие действия:

| | |
|---|---|
| **1970 = 1*1066 + 904** | ***(1066,904)*** |
| **1066 = 1*904+162** | ***(904,162)*** |
| **904 = 5*162+94** | ***(162,94)*** |
| **162 = 1*94+68** | ***(94,68)*** |
| **94 = 1*68+26** | ***(68,26)*** |
| **68 = 2*26+16** | ***(26,16)*** |
| **26 = 1*16+10** | ***(16,10)*** |
| **16 = 1*10+6** | ***(10,6)*** |
| **10 = 1*6+4** | ***(6,4)*** |
| **6 = 1*4+2** | ***(4,2)*** |
| **4 = 2*2+0** | ***(2,0)*** |

Следовательно, **(1970,1066)=2.**

**Обобщенный алгоритм Евклида** определяет:

**1.** наибольший общий делитель двух положительных целых чисел
и, *если эти числа оказываются* ***взаимно простыми***,
**2**. ***мультипликативное обратное*** одного из них по модулю другого.

# *Функция Эйлера*

**обозначается символом *ф(n)* и представляет собой для каждого целого числа *n*, *n>1*, число положительных целых значений, которые меньше *n* и являются взаимно простыми с *n*.**
**Значение *ф(1)* оказывается при этом *неопрёделенным*, но считается, что оно равно 1.**

**Некоторые значения функции Эйлера *ф(n)***

| *n* | *ф(n)* | *n* | *ф(n)* | *n* | *ф(n)* |
|---|---|---|---|---|---|
| 1 | 1 | 11 | 10 | 21 | 12 |
| 2 | 1 | 12 | 4 | 22 | 10 |
| 3 | 2 | 13 | 12 | 23 | 22 |
| 4 | 2 | 14 | 6 | 24 | 8 |
| 5 | 4 | 15 | 8 | 25 | 20 |
| 6 | 2 | 16 | 8 | 26 | 12 |
| 7 | 6 | 17 | 16 | 27 | 18 |
| 8 | 4 | 18 | 6 | 28 | 12 |
| 9 | 6 | 19 | 18 | 29 | 28 |
| 10 | 4 | 20 | 8 | 30 | 8 |

Для простого $p$ $\quad \phi(p) = p - 1.$

Для произведения простых чисел $p$ и $q$ $\quad n = pq$

получим: $\phi(n) = \phi(pq) = \phi(p) \times \phi(p) = (p-1) \times (q-1)$

**Доказательство**.

Значениями, не являющимися *взаимно простыми* с $n$, будут значения множеств

$\{p, 2p, \ldots (q-1)p\}$ и $\{q, 2q, \ldots, (p-1)q\}$, а также $0$.

Соответственно $\phi(n) = pq - [(q-1) + (p-1) + 1] =$

$= pq - (p + q) + 1 =$

$= (p-1) \times (q-1) =$

$= \phi(p) \times \phi(q).$

***Теорема Эйлера***

Для любых *взаимно простых* чисел $a$ и $n$ (т.е. таких, что $(a,n)=1$)

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

*Альтернативная формулировка* теоремы:

$$a^{\phi(n)+1} \equiv a \pmod{n}.$$

Следствие для эффективности применения *алгоритма* ***RSA***.

Для любых двух простых чисел $p$ и $q$ и чисел $n = pq$ и $m$ (здесь $0 < m < n$) выполняется следующее условие:

$$m^{\phi(n)+1} = m^{(p-1)(q-1)+1} \equiv m \bmod n.$$

Альтернативная форма того же следствия:

$$[m^{\phi(n)}]^k \equiv 1 \bmod n,$$

$$m^{k\phi(n)} \equiv 1 \bmod n,$$

$$m^{k\phi(n)+1} = m^{k(p-1)(q-1)+1} \equiv m \bmod n.$$

*Из теоремы Эйлера следует малая* ***теорема Ферма****:*

*Если* ***p*** *- простое число и* $p / a$ *, то*

$$a^{p-1} \equiv 1 (\bmod p)$$

## *Тест Рабина*

для проверки чисел на **простоту**

Пусть имеется число

$N = 2^S t + 1$, где ***t*** - нечетно,

и требуется установить, простое оно или составное.

1. Выбирается случайное число $1 \le a \le N$ и проверяются два условия:

1) $N$ не делится на $a$;

2) $a^t = 1 \pmod N$ или существует целое $k$ $(0 \le k \le s)$, для которого

$$a^{2^k t} = -1 (\bmod N)$$

2. Если *оба* условия выполняются, то вероятность того, что число **N** окажется **составным**, равна ***1/4.***

3. Если провести не один, а ***n*** аналогичных тестов, выбирая *случайное* ***a***, то можно установить простоту числа с вероятностью $4^{-n}$.

*За счет выбора большого* ***n*** *можно добиться того, что вероятность ошибочного выбора простого числа для создания криптосистемы окажется ниже, чем вероятность ее взлома существующими методами (например,* пробой на ключ*).*

# *Показатель числа a по модулю n*

Если ***a*** и ***n*** являются взаимно простыми (***(a,n) = 1***) , то существует по крайней мере одно целое число $\gamma$, удовлетворяющее соотношению $a^{\gamma} \equiv 1 (\mathrm{mod}\, n)$ – это число $\gamma = \phi(n)$, существование которого обеспечивается теоремой ***Эйлера***.

**Наименьшее** из чисел $\gamma$ называется ***показателем* числа *a* по модулю *n*.**

Показатель числа ***a*** по модулю ***n*** является ***делителем*** числа ***ф(n)***.

В частном случае, когда показатель числа ***a*** по модулю ***n*** равен ***ф(n)***, (наивысший из показателей числа ***a*** по модулю ***n***), то ***a*** называется ***первообразным (примитивным) корнем по модулю n***.

Для **наименьшего из положительных** $\gamma$ , при которых выполняется условие $a^{\gamma} \equiv 1 (\mathrm{mod}\, n)$, используются также еще следующие названия:

- порядок числа ***a*** по модулю ***n***,
- показатель, которому принадлежит ***a*** по модулю ***n***,
- **длина периода последовательности**, генерируемой степенями ***a***.

Чтобы убедиться в истинности последнего пункта, рассмотрим степени числа 7 по модулю 19:

**$7^1 = 7 \bmod 19$,**
**$7^2 = 49 = 2*19 + 11 = 11 \bmod 19$,**
**$7^3 = 343 = 18*19 + 1 = 1 \bmod 19$,**
**$7^4 = 2401 = 126*19 + 7 = 7 \bmod 19$,**
**$7^5 = 16807 = 884*19 + 11 = 11 \bmod 19$.**

Последовательность является **периодической** с периодом, равным наименьшему положительному показателю ***n***, при котором $7^n = 1 \pmod{19}$.

## Степени целых чисел по модулю 19

| $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $a^7$ | $a^8$ | $a^9$ | $a^{10}$ | $a^{11}$ | $a^{12}$ | $a^{13}$ | $a^{14}$ | $a^{15}$ | $a^{16}$ | $a^{17}$ | $a^{18}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 4 | 8 | 16 | 13 | 7 | 14 | 9 | 18 | 17 | 15 | 11 | 3 | 6 | 12 | 5 | 10 | 1 |
| 3 | 9 | 8 | 5 | 15 | 7 | 2 | 6 | 18 | 16 | 10 | 11 | 14 | 4 | 12 | 17 | 13 | 1 |
| 4 | 16 | 7 | 9 | 17 | 11 | 6 | 5 | 1 | 4 | 16 | 7 | 9 | 17 | 11 | 6 | 5 | 1 |
| 5 | 6 | 11 | 17 | 9 | 7 | 16 | 4 | 1 | 5 | 6 | 11 | 17 | 9 | 7 | 16 | 4 | 1 |
| 6 | 17 | 7 | 4 | 5 | 11 | 9 | 16 | 1 | 6 | 17 | 7 | 4 | 5 | 11 | 9 | 16 | 1 |
| 7 | 11 | 1 | 7 | 11 | 1 | 7 | 11 | 1 | 7 | 11 | 1 | 7 | 11 | 1 | 7 | 11 | 1 |
| 8 | 7 | 18 | 11 | 12 | 1 | 8 | 7 | 18 | 11 | 12 | 1 | 8 | 7 | 18 | 11 | 12 | 1 |
| 9 | 5 | 7 | 6 | 16 | 11 | 4 | 17 | 1 | 9 | 5 | 7 | 6 | 16 | 11 | 4 | 17 | 1 |
| 10 | 5 | 12 | 6 | 3 | 11 | 15 | 17 | 18 | 9 | 14 | 7 | 13 | 16 | 8 | 4 | 2 | 1 |
| 11 | 7 | 1 | 11 | 7 | 1 | 11 | 7 | 1 | 11 | 7 | 1 | 11 | 7 | 1 | 11 | 7 | 1 |
| 12 | 11 | 18 | 7 | 8 | 1 | 12 | 11 | 18 | 7 | 8 | 1 | 12 | 11 | 18 | 7 | 8 | 1 |
| 13 | 17 | 12 | 4 | 14 | 11 | 10 | 16 | 18 | 6 | 2 | 7 | 15 | 5 | 8 | 9 | 3 | 1 |
| 14 | 6 | 8 | 17 | 10 | 7 | 3 | 4 | 18 | 5 | 13 | 11 | 2 | 9 | 12 | 16 | 15 | 1 |
| 15 | 16 | 12 | 9 | 2 | 11 | 13 | 5 | 18 | 4 | 3 | 7 | 10 | 17 | 8 | 6 | 14 | 1 |
| 16 | 9 | 11 | 5 | 4 | 7 | 17 | 6 | 1 | 16 | 9 | 11 | 5 | 4 | 7 | 17 | 6 | 1 |
| 17 | 4 | 11 | 16 | 6 | 7 | 5 | 9 | 1 | 17 | 4 | 11 | 16 | 6 | 7 | 5 | 9 | 1 |

А) **Все** последовательности заканчиваются числом **1**.

Б) **Длина** последовательности является ***делителем*** ***ф*(19)=18.** Из этого следует, что в каждой строке таблицы умещается целое число периодов соответствующих последовательностей.

В) Некоторые последовательности имеют длину **18**. В таком случае говорят, что целое число ***а*** *генерирует* (своими степенями) ***множество всех ненулевых вычетов по модулю 19***. Любое из таких целых чисел называют **первообразным корнем по модулю 19** (см. определение выше)**.**

Если ***a*** является первообразным корнем ***n***, его степени

$$a, a^2, a^{\phi(n)}$$

оказываются ***различными по модулю n*** и *взаимно простыми с* ***n***.

В частности, для простого числа ***p***, если ***a*** является первообразным корнем ***p***, то

$$a, a^2, a^{p-1}$$

оказываются различными по модулю ***p***.

*Для простого числа 19 его первообразными корнями являются числа*

*2, 3, 10, 13, 14 и 15.*

**Целыми числами с первообразными корнями** будут только числа

**2**, **4**, $p^a$ и $2p^a$ ,

где ***p*** - любое *нечетное простое* число.

## *Дискретные логарифмы*

Известно, что любое целое число ***b*** можно представить в форме

$$b \equiv r \bmod p \text{ , где } 1 \le r \le (p-1)$$

в **классах вычетов**.

*Отсюда вытекает*, что для любого целого числа ***b*** и любого первообразного корня ***a*** простого числа ***p*** можно найти ровно один показатель степени ***i***, для которого

$$b \equiv a^i \bmod p, \quad \text{где } 1 \le i \le (p-1).$$

Значение этого показателя называют

**индексом числа *b* по модулю *p* при основании *a*.**

Записывается это значение как $ind_{a,p}(b)$.

Свойства индексов чисел

$ind_{a,p}(1) = 0$ , **поскольку** $a^0 \bmod p = 1 \bmod p = 1$,

$ind_{a,p}(a) = 1$, **поскольку** $a^1 \bmod p = a$ ,

$ind_{a,p}(xy) = [ind_{a,p}(x) + ind_{a,p}(y)] \bmod \phi(p)$,

$ind_{a,p}(y^r) = [r \times ind\ a,p\ (y)] \bmod \phi(p)$.

Из-за аналогии между обычными логарифмами и индексами последние называют

**дискретными логарифмами**.

***Однозначно*** дискретные логарифмы по модулю ***n*** при основании ***a*** определяются, только когда ***a*** является **первообразным корнем *n*.**

Таблицы дискретных логарифмов **по модулю 19**

(**а**) Дискретные логарифмы по модулю 19 **при основании 2**

| $b$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $ind_{2,19}(b)$ | 18 | 1 | 13 | 2 | 16 | 14 | 6 | 3 | 8 | 17 | 12 | 15 | 5 | 7 | 11 | 4 | 10 | 9 |

(**б**) Дискретные логарифмы по модулю 19 **при основании 3**

| $b$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $ind_{3,19}(b)$ | 18 | 7 | 1 | 14 | 4 | 8 | 6 | 3 | 2 | 11 | 12 | 15 | 17 | 13 | 5 | 10 | 16 | 9 |

(**в**) Дискретные логарифмы по модулю 19 **при основании 10**

| $b$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $ind_{10,19}(b)$ | 18 | 17 | 5 | 16 | 2 | 4 | 12 | 15 | 10 | 1 | 6 | 3 | 13 | 11 | 7 | 14 | 8 | 9 |

(**г**) Дискретные логарифмы по модулю 19 **при основании 13**

| $b$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $ind_{13,19}(b)$ | 18 | 11 | 17 | 4 | 14 | 10 | 12 | 15 | 16 | 7 | 6 | 3 | 1 | 5 | 13 | 8 | 2 | 9 |

(**д**) Дискретные логарифмы по модулю 19 **при основании 14**

| $b$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $ind_{14,19}(b)$ | 18 | 13 | 7 | 8 | 10 | 2 | 6 | 3 | 14 | 5 | 12 | 15 | 11 | 1 | 17 | 16 | 14 | 9 |

(**е**) Дискретные логарифмы по модулю 19 **при основании 15**

| $b$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $ind_{15,19}(b)$ | 18 | 5 | 11 | 10 | 8 | 16 | 12 | 15 | 4 | 13 | 6 | 3 | 7 | 17 | 1 | 2 | 12 | 9 |