ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ

Глава 1. ОТНОШЕНИЕ ДЕЛИМОСТИ В КОЛЬЦЕ ЦЕЛЫХ ЧИСЕЛ

§1. СВОЙСТВА ДЕЛИМОСТИ ЦЕЛЫХ ЧИСЕЛ. ПРОСТЫЕ И СОСТАВНЫЕ ЧИСЛА

Определение. Числа $a_1, a_2, \dots, a_n \in \mathbb{Z}$ называются ***взаимно простыми,*** если наибольший общий делитель $(a_1, a_2, \dots, a_n) = 1$. Числа $a_1, a_2, \dots, a_n \in \mathbb{Z}$ называются ***попарно взаимно простыми,*** если наибольший общий делитель $(a_i, a_j) = 1$ при $i \neq j$.

Если числа $a_1, a_2, \dots, a_n$ попарно взаимно просты, то они взаимно просты. Для двух чисел эти понятия совпадают.

Определение. Натуральное число $p \neq 1$, называется ***простым***, если оно имеет ровно два натуральных делителя (1 и p). Натуральное число n называется *составным*, если оно имеет более двух натуральных делителей.

Из определения следует, что любое составное число n можно представить в виде $n = ab$, где $1 < a \leq b < n$.

Для составления таблицы простых чисел, не превышающих натуральное число $n > 1$ можно использовать алгоритм, предложенный греческим математиком Эратосфеном. Он называется ***решетом Эратосфена*** и состоит в следующем:

- ✓ выписываем натуральные числа от 2 до n;
- ✓ так как 2 является первым простым числом, p_1, обводим его кружком и вычеркиваем из нашей последовательности натуральных чисел все числа, большие 2, которые делятся на 2 (все чётные числа, кроме $p_1 = 2$);
- ✓ следующее за $p_1 = 2$ невычеркнутое число является простым: $p_2 = 3$, обводим его кружком и вычёркиваем все числа, большие p_2 и делящиеся на p_2;
- ✓ следующее за p_2 невычеркнутое число является простым: $p_3 = 5$, обводим его кружком и вычёркиваем все числа, большие p_3 и делящиеся на p_3 и т.д.

…

- ✓ останавливаемся на простом числе p, которое не превышает $\sqrt{n}$: если вычеркнуты все числа, которые делятся на p и при этом $p^2 \geq n$, то процесс завершаем.

ТАБЛИЦА ПРОСТЫХ ЧИСЕЛ,
не превосходящих 1000

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997		

Некоторые знаменитые ***примеры*** простых чисел:

1) простое число называется *простым числом Ферма*, если оно имеет вид: $\boldsymbol{F_n = 2^{2^n} + 1}$, где $n \geq 0$; числа $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ являются простыми числами Ферма, однако число F_5 – составное число;

2) простое число называется *простым числом Мерсенна*, если оно имеет вид: $\boldsymbol{M_p = 2^p - 1}$, где p – простое число; числа $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$, M_{13}, M_{17}, M_{19}, M_{31}, M_{61} являются простыми числами Мерсенна.

Простые числа Ферма используются в теореме Гаусса о возможности построения правильного многоугольника с заданным числом сторон.

§2. КОНЕЧНЫЕ ЦЕПНЫЕ ДРОБИ. ПОДХОДЯЩИЕ ДРОБИ

Любое рациональное число можно представить в виде $\frac{a}{b}$, где $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Такое представление называют *обыкновенной дробью*. Наряду с этим, рациональное число можно представить в виде так называемой *конечной цепной дроби*. Это представление получается с помощью алгоритма Евклида.

Определение. Целой частью рационального числа α называется наибольшее целое число n, которое не превышает α, то есть: $n \le \alpha < n+1$. *Дробной частью* числа α называется разность $\alpha - [\alpha]$.

Обозначения: [α] – целая часть числа α; $\{\alpha\}$ – дробная часть числа α.

Вывод: $\alpha = [\alpha] + \{\alpha\}$, в частности, для рационального числа $\alpha = \frac{a}{b}$: $\frac{a}{b} = \left[\frac{a}{b}\right] + \left\{\frac{a}{b}\right\}$.

К конечной цепной дроби можно прийти, если записать рациональное число $\alpha = \frac{a}{b}$ в виде $\alpha = a_0 + \frac{1}{\alpha_1}$, где $a_0 = \left[\frac{a}{b}\right]$ – целая часть числа α, $0 < \frac{1}{\alpha_1} = \left\{\frac{a}{b}\right\} < 1$ (здесь $\frac{1}{\alpha_1} = \left\{\frac{a}{b}\right\}$ – дробная часть числа α). А затем записать в таком же виде α_1 и т.д.

Определение. Конечной цепной дробью называется выражение вида:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{s-1} + \cfrac{1}{a_s}}}}$$

где $a_0 \in \mathbb{Z}$, $a_1, a_2, \dots, a_s \in \mathbb{N}$, $a_s > 1$.

Числа $a_0, a_1, a_2, \dots, a_s$ называются *элементами* цепной дроби, а цепная дробь с этими элементами обозначается $[\boldsymbol{a_0};\ \boldsymbol{a_1}, \boldsymbol{a_2}, \dots, \boldsymbol{a_s}]$.

a_0 – целая часть числа $[a_0;\ a_1, a_2, \dots, a_s]$, а $\frac{1}{[a_1; a_2, \dots, a_s]}$ – дробная часть этого числа.

Применим алгоритм Евклида к числам a и b ($a \in \mathbb{Z}$, $b \in \mathbb{N}$):
$a = ba_0 + r_1,\ 0 < r_1 < b;$
$b = r_1a_1 + r_2,\ 0 < r_2 < r_1;$
…
$r_{s-2} = r_{s-1}a_{s-1} + r_s,\ 0 < r_s < r_{s-1};$
$r_{s-1} = r_sq_s$, где $q_i, r_i \in \mathbb{Z}$, $i = 1, 2, \dots, n.$
Тогда $\frac{a}{b}=[a_0;a_1,\dots,a_{s-1},a_s]$.

Теорема. Любое рациональное число можно представить в виде конечной цепной дроби и такое представление однозначно.

Определение. Рациональное число $\delta_k=[a_0;a_1,\dots,a_k]$ называется **-й подходящей дробью** ($0 \le k \le s$) конечной цепной дроби $[a_0;\ a_1,\ a_2, \dots, a_s]$.

Подходящая дробь δ_k может быть получена из подходящей дроби δ_{k-1} ($k \ge 1$) заменой величины a_{k-1} на величину $a_{k-1}+\frac{1}{a_k}$.

Всякая подходящая дробь δ_k есть рациональное число, следовательно, представима в виде обыкновенной дроби вида $\frac{P_k}{Q_k}$, где $P_k \in \mathbb{Z}$, $Q_k \in \mathbb{N}$ ($0 \le k \le s$).

Теорема. Если $[a_0;a_1,\dots,a_s]$ – конечная цепная дробь и даны две последовательности чисел P_0, P_1, …, P_s и Q_0, Q_1, …, Q_s, удовлетворяющие начальным условиям:
$P_0 = a_0,\ P_1 = a_1a_0 + 1,$
$Q_0 = 1,\ Q_1 = a_1,$
и рекуррентным соотношениям ($2 \le k \le s$):
$P_k = a_kP_{k-1} + P_{k-2},$
$Q_k = a_kQ_{k-1} + Q_{k-2},$
то $\delta_k=\frac{P_k}{Q_k}$ ($0 \le k \le s$).

Вычисление числителей и знаменателей подходящих дробей удобно выполнять по следующей схеме:

a_0	a_1	a_2	…	a_k	…	a_s
a_0	$a_1a_0 + 1$	$a_2P_1 + P_0$	…	$a_kP_{k-1} + P_{k-2}$	…	$a_sP_{s-1} + P_{s-2}$
1	a_1	$a_2Q_1 + Q_0$	…	$a_kQ_{k-1} + Q_{k-2}$	…	$a_sQ_{s-1} + Q_{s-2}$

Для вычисления P_k (Q_k) по данной схеме нужно число a_k, стоящее сверху, умножить на число P_{k-1} (Q_{k-1}), стоящее слева, и к произведению прибавить число P_{k-2} (Q_{k-2}), которое предшествует P_{k-1} (Q_{k-1}).

Свойства подходящих дробей:

1) числители и знаменатели двух соседних подходящих дробей связаны соотношением: $\boldsymbol{P_k Q_{k-1} - P_{k-1} Q_k = (-1)^{k-1}}$ $(k \geq 1)$;

2) подходящие дроби $\delta_k = \dfrac{P_k}{Q_k}$ несократимы;

3) $\delta_k - \delta_{k-1} = \dfrac{(-1)^{k-1}}{Q_k Q_{k-1}}$;

4) для конечной цепной дроби $[a_0; a_1, ..., a_s]$ подходящие дроби с чётными номерами $\delta_0, \delta_2, \delta_4, ...$ образуют возрастающую последовательность, а подходящие дроби $\delta_1, \delta_3, \delta_5, ...$ с нечётными номерами – убывающую последовательность чисел, причём всякая подходящая дробь с чётным номером меньше всякой подходящей дроби с нечётным номером: $\delta_0 < \delta_2 < \delta_4 < ... < \delta_s < ... < \delta_5 < \delta_3 < \delta_1$.

Конечные цепные дроби могут быть использованы для нахождения линейного представления НОД двух целых чисел:

Теорема. Пусть $d = \text{НОД}(a, b)$ и $\delta_{s-1} = \dfrac{P_{s-1}}{Q_{s-1}}$ – предпоследняя подходящая дробь разложения $\dfrac{a}{b}$ в конечную цепную дробь $[a_0;\ a_1,\ a_2, ..., a_s]$. Тогда:

$$\boldsymbol{d = (-1)^{s-1} a Q_{s-1} + (-1)^s b P_{s-1}}.$$

§3. КОЛЬЦО ЦЕЛЫХ ГАУССОВЫХ ЧИСЕЛ. ПРОСТЫЕ ГАУССОВЫ ЧИСЛА

Множество чисел вида $a+bi$, где $a,b\in\mathbb{Z}$, $i^2=-1$, называется *множеством целых гауссовых чисел*. Множество чисел вида $a+bi$, где $a,b\in\mathbb{Q}$, $i^2=-1$, называется *множеством рациональных гауссовых чисел.*

Так как множество целых гауссовых чисел является подмножеством множества комплексных чисел, то для целых гауссовых чисел справедливы некоторые определения и свойства комплексных чисел. В частности, на множестве целых гауссовых чисел определены операции сложения и умножения:

$(a+bi)+(\mathrm{c}+di)=(a+c)+(b+d)i;$

$(a+bi)\cdot(\mathrm{c}+di)=(ac-bd)+(ad+bc)i.$

Теорема. Множество целых гауссовых чисел с операциями сложения и умножения является коммутативным *кольцом* с единицей.

Обозначение. $\mathbb{Z}[\boldsymbol{i}]$ – кольцо целых гауссовых чисел.

Кольцо целых гауссовых чисел обозначается $\mathbb{Z}[i]$, так как получается в результате присоединения к кольцу $\mathbb{Z}$ элемента i (является расширением кольца $\mathbb{Z}$ с помощью элемента i).

Геометрическая интерпретация: целые гауссовы числа образуют *целочисленную решётку* на комплексной плоскости: множество чисел комплексной плоскости с целочисленными координатами.

Каждому целому гауссову числу $\alpha=a+bi$ на комплексной плоскости соответствует вектор $\overrightarrow{OM}$ с началом в точке $O(0;0)$ и концом в точке $\mathrm{M}(a;b)$. Следовательно, модуль целого гауссова числа $\alpha=a+bi$ (как комплексного числа) равен $\sqrt{a^2+b^2}$. Для целых гауссовых удобнее пользоваться ***нормой***, то есть квадратом модуля: $\boldsymbol{N(\alpha)=a^2+b^2}$. Кроме нормы, каждому целому гауссову числу $\alpha=a+bi$ можно поставить в соответствие *сопряженное число*: $\bar{\alpha}=a-bi$.

Свойства нормы *целых гауссовых чисел:*

Для любого целого гауссова числа $\alpha=a+bi$ справедливо:

1) $N(\alpha)\in\mathbb{N}\cup\{0\}$, причём $N(\alpha)=0\Leftrightarrow\alpha=0$;

2) $N(-\alpha)=N(\alpha)$;

3) $N(\alpha)=\alpha\cdot\bar{\alpha}\in\mathbb{Z}$, поэтому для любого ненулевого гауссова числа α существует кратное ему целое число: $\alpha\bar{\alpha}=a^2+b^2\in\mathbb{Z}$: $(a^2+b^2)\ \vdots\ \alpha$.

Теорема (мультипликативность нормы). Для любых целых гауссовых чисел α, β справедливо: $\boldsymbol{N(\alpha\beta) = N(\alpha)N(\beta)}$.

Следствие. Если каждое из двух натуральных чисел может быть записано как сумма двух квадратов, то их произведение тоже.

Пример. $5 = 1^2 + 2^2; 13 = 2^2 + 3^2; 65 = 5 \cdot 13 = 1^2 + 8^2 = 4^2 + 7^2$.

Определение делимости целых чисел естественным образом распространяется на целые гауссовы числа:

Определение. Пусть $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$. Говорят, что целое гауссово число α ***делится*** на целое гауссово число β, если существует целое гауссово число γ, такое что $\alpha = \beta\gamma$.

Число α называется *делимым*, число β *– делителем*.

Обозначение: если α делится на β, то пишут $\alpha \vdots \beta$.

Определение. Число $\alpha \in \mathbb{Z}[i]$ называется ***делителем единицы*** (другое название: *обратимым*), если $\exists \beta \in \mathbb{Z}[i]$: $\alpha\,\beta = 1$.

Обозначение: ε.

Делителями единицы (обратимыми элементами) кольца $\mathbb{Z}[i]$ являются те элементы, норма которых равна 1, то есть $\boldsymbol{1, -1, i, -i}$.

Свойства делимости целых гауссовых чисел:

$\forall \alpha, \beta, \gamma \in \mathbb{Z}[i]$:

1) норма $N(\alpha) \vdots \alpha$;

2) $\alpha \vdots \beta \Leftrightarrow \bar{\alpha} \vdots \bar{\beta}$;

3) $\alpha \vdots \beta \Leftrightarrow \varepsilon_1\alpha \vdots \varepsilon_2\beta$, где $\varepsilon_1, \varepsilon_2 \in \{1, -1, i, -i\}$ (делители единицы);

4) $\alpha \vdots \beta \Rightarrow N(\alpha) \vdots N(\beta)$;

5) если $\alpha \vdots \beta$ и $\beta \vdots \gamma$, то $\alpha \vdots \gamma$;

6) если $\alpha \vdots \gamma$ и $\beta \vdots \gamma$, то $(\alpha + \beta) \vdots \gamma$;

7) если $\alpha \vdots \beta$ и $\beta \vdots \alpha$, то $\alpha = \varepsilon\beta$, где $\varepsilon \in \{1, -1, i, -i\}$ (делитель единицы).

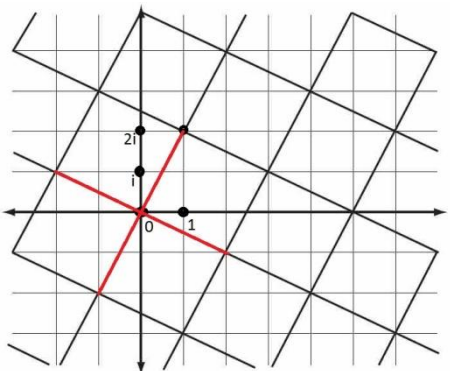
Следствие. Любое целое гауссово число α, не являющееся делителем 1, имеет как минимум, 8 делителей (эти делители называются *тривиальными*):

- $\boldsymbol{1, -1, i, -i}$ (4 делителя 1),
- $\boldsymbol{\alpha, -\alpha, i\alpha, -i\alpha}$ (4 произведения делителей 1 на α).

Определение. Два целых гауссовых числа называются ***ассоциированными***, если одно получается из другого умножением на делитель 1.

Геометрическая интерпретация: ассоциированные числа на комплексной плоскости отличаются друг от друга поворотом на угол, кратный $\frac{\pi}{2}$ (другими словами, отличаются на угол $\frac{k\pi}{2}$, $k \in \mathbb{Z}$).

Пример. Ассоциированными с числом $\alpha = 1 + 2i$ будут следующие числа: $-\alpha = -1 - 2i$, $i\alpha = -2 + i$, $-i\alpha = 2 - i$.



В кольце $\mathbb{Z}[i]$ возможно деление с остатком на ненулевое целое гауссово число, при котором остаток меньше делителя по норме: $\alpha = \beta\gamma + \rho$, где $N(\rho) < N(\beta)$.

Теорема (о делении с остатком в $\mathbb{Z}[i]$). Для любых целых гауссовых чисел α и β, $\beta \neq 0$, найдётся целое гауссово число γ такое, что $N(\alpha - \beta\gamma) < N(\beta)$.

В качестве $\gamma = m + ni$ можно взять одно из ближайших целых гауссовых чисел на комплексной плоскости к рациональному гауссову числу $\frac{\alpha}{\beta} = a + bi$, а именно, выбрать целые числа m и n из условий: $|a - m| \leq \frac{1}{2}$, $|b - n| \leq \frac{1}{2}$.

В $\mathbb{Z}[i]$, в отличие от $\mathbb{Z}$, деление с остатком неоднозначно. Например,
$7 + 2i = (3 - i)(2 + i) + i = (3 - i)(1 + i) + 3 = (3 - i)(2 + 2i) + (-1 - 2i)$.

Определение. Наибольшим общим делителем (***НОД***) двух целых гауссовых чисел α и β, хотя бы одно из которых ненулевое, называется такой их общий делитель, который делится на любой другой их общий делитель.

Наибольший общий делитель $\text{НОД}(\alpha, \beta)$ есть такой общий делитель α и β, у которого норма максимальна.

Определение. Наименьшим общим кратным (*НОК*) двух ненулевых целых гауссовых чисел α и β называется такое их общее кратное, которое делит любое их общее кратное.

Если известен некоторый *НОД*, то любое из трёх чисел, ассоциированных с ним, также будет *НОД*. В частности, если один из *НОД* — делитель единицы, то такими же будут и остальные три *НОД*.

Гауссовы числа взаимно просты тогда и только тогда, когда их *НОД* – делитель единицы.

Как и в множестве целых чисел, в множестве целых гауссовых чисел для нахождения НОД используют алгоритм Евклида:

$\alpha = \beta\gamma_1 + \rho_1,\ N(\rho_1) < N(\beta);$

$\beta = \rho_1\gamma_2 + \rho_2,\ N(\rho_2) < N(\rho_1);$

…

$\rho_{n-2} = \rho_{n-1}\gamma_n + \rho_n,\ N(\rho_n) < N(\rho_{n-1});$

$\rho_{n-1} = \rho_n\gamma_n,$

где $\gamma_i, \rho_i \in \mathbb{Z}[i],\ i = 1, 2, \dots, n.$

Алгоритм Евклида будет конечным, так как последовательность норм убывает: $N(\beta) > N(\rho_1) > N(\rho_2) > \dots$, а нормы – неотрицательные целые числа.

Теорема. *Наибольший общий делитель* целого гауссова числа α и ненулевого целого гауссова числа β, не делящего α, равен последнему ненулевому остатку алгоритма Евклида (ρ_n), записанного для этих чисел.

Теорема (о линейном представлении НОД в $\mathbb{Z}[i]$). Если НОД$(\alpha, \beta) = \delta$, то существуют такие целые гауссовы числа φ и ψ, что $\delta = \alpha\varphi + \beta\psi$.

Все целые гауссовы числа делятся на делители единицы, поэтому любое целое гауссово число, отличное от делителей единицы, имеет как минимум 8 делителей: 4 делителя единицы и 4 числа ассоциированных с самим числом (так называемые *тривиальные делители*).

Определение. Целое гауссово число π называется ***простым***, если оно не имеет других делителей, кроме тривиальных. Целое гауссово число α называется *составным*, если оно имеет другие делители, кроме тривиальных.

Делители единицы не считаются ни простыми, ни составными целыми гауссовыми числами.

Целое гауссово число является простым, если его нельзя представить в виде: $\pi = \alpha\beta$, где $N(\alpha) > 1$, $N(\beta) > 1$.

Примеры. $\mathbf{3}$ – простое целое гауссово число,
$\mathbf{1 + i}$ – простое целое гауссово число,
$\mathbf{5} = (2 + i)(2 - i) = (1 + 2i)(1 - 2i)$ – составное целое гауссово число.

Свойства простых целых гауссовых чисел:

1) если π – простое целое гауссово число, ε – делитель единицы, то $\varepsilon\pi$ – простое целое гауссово число;

2) целое гауссово число, сопряженное с простым целым гауссовым числом, само является простым целым гауссовым числом;

3) если произведение двух целых гауссовых чисел делится на простое целое гауссово число π, то хотя бы один из сомножителей делится на π;

4) любое простое целое гауссово число π является делителем ровно одного простого натурального числа p (существует такое простое число $p \in \mathbb{N}$, что $p \vdots \pi$);

5) простое число $p \in \mathbb{N}$ нельзя представить в виде произведения более чем двух целых гауссовых чисел, не являющихся делителями единицы.

Теорема (основная теорема арифметики целых гауссовых чисел). Любое ненулевое целое гауссово число, не являющееся делителем единицы, можно представить в виде произведения простых целых гауссовых чисел, причём это представление единственно с точностью до ассоциированности и порядка следования сомножителей.

Любое ненулевое целое гауссово число α представляется в виде:
$\alpha = \varepsilon\pi_1^{k_1}\pi_2^{k_2} \ldots \pi_n^{k_n}$, где $\varepsilon \in \{1, -1, i, -i\}$, $\pi_1, \pi_2, \ldots, \pi_n$ – различные (т.е. неассоциированные) простые целые гауссовы числа, $\pi_1, \pi_2, \ldots, \pi_n \in \mathbb{N}$.

Теорема. Простые числа вида $p = 4k + 3$, $k \in \mathbb{N}$, и ассоциированные с ними являются простыми целыми гауссовыми числами.

Теорема. Если норма целого гауссова числа α есть простое (натуральное) число, то α – простое целое гауссово число.

Теорема. Простые (натуральные) числа вида $p = 4k + 1$, $k \in \mathbb{N}$, раскладываются в произведение двух простых сопряженных целых гауссовых чисел.

§4. ДИОФАНТОВЫ УРАВНЕНИЯ

Определение. Линейным диофантовым уравнением *(ЛДУ)* относительно переменных x и y называется уравнение вида:

$ax + by = c$, где $a, b, c \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, НОД$(a, b) = 1$, (1)

для которого необходимо найти *только целые решения* (пары целых чисел, удовлетворяющих уравнению).

Теорема. Пусть (x_0, y_0) – какое-нибудь частное решение *ЛДУ* (1), тогда его общее решение задается формулами: $x = x_0 - bt$, $y = y_0 + at$, $t \in \mathbb{Z}$.

Общее решение неоднородного *ЛДУ* есть сумма:

- ✓ общего решения соответствующего однородного уравнения;
- ✓ некоторого (любого) частного решения неоднородного *ЛДУ*.

Рассмотрим диофантово уравнение второй степени с тремя неизвестными:

$\boldsymbol{x^2 + y^2 = z^2}$ (уравнение Ферма). (2)

Геометрически решение этого уравнения в целых числах можно интерпретировать как нахождение всех прямоугольных треугольников, у которых катеты x, y, и гипотенуза z выражаются целыми числами.

Общие делители двух из величин x, y, z в уравнении (2) должны быть делителями третьей и могут быть сокращены. Поэтому можно ограничиться рассмотрением взаимно простых значений неизвестных.

Теорема. Формулы:

$x = uv$, $y = \frac{u^2 - v^2}{2}$, $z = \frac{u^2 + v^2}{2}$,

при нечётных взаимно простых u и v $(v < u)$ дают все свободные от общих делителей тройки натуральных чисел x, y, z (т. наз. *пифагоровы тройки*), которые удовлетворяют уравнению (2).

Пример. Для начальных значений u и v получаем следующие равенства:

$v = 1, u = 3$: $x = 3, y = 4, z = 5$; $\boldsymbol{3^2 + 4^2 = 5^2}$;

$v = 1, u = 5$: $x = 5, y = 12, z = 13$; $\boldsymbol{5^2 + 12^2 = 13^2}$;

$v = 3, u = 5$: $x = 15, y = 8, z = 17$; $\boldsymbol{15^2 + 8^2 = 17^2}$.

Последняя теорема Ферма утверждает, что никакие три положительных целых числа a, b и c не могут удовлетворять уравнению $\boldsymbol{x^n + y^n = z^n}$, где $n \geq 3$.

Эта теорема является естественным продолжением пифагоровых троек, для которых $n = 2$. Французский математик Пьер де Ферма записал

формулировку этой теоремы на полях одной из книг по математике в 1637 г. Он утверждал, что нашёл метод доказательства этой теоремы, но однако никому не удавалось его обнаружить (для $n = 2$ Ферма оставил доказательство).

Почти триста пятьдесят лет спустя, в процессе доказательства истинности одной важной гипотезы в теории эллиптических кривых, сэр Эндрю Уайлс (институт Исаака Ньютона в Кембридже) объявил, что нашёл доказательство последней теоремы Ферма. Окончательный вариант доказательства был принят в 1995 г.

Диофантово уравнение второй степени с двумя неизвестными:

$\boldsymbol{x^2 - dy^2 = 1}$, (уравнение Пелля), (3)

где d – целое положительное число, не являющееся полным квадратом ($\sqrt{d}$ – иррациональное число).

Определение. Фундаментальным решением уравнения Пелля называется решение (x_1, y_1), в котором натуральные числа x_1 и y_1, принимают свои наименьшие значения.

Пример. Для уравнения $x^2 - 2y^2 = 1$ фундаментальным решением будет пара (3, 2).

Теорема. Любое решение диофантова уравнения (3) имеет вид $(\pm x_n, \pm y_n)$, где:

$$x_n = \frac{1}{2}\left[\left(x_1 + \sqrt{d}\,y_1\right)^n + \left(x_1 - \sqrt{d}\,y_1\right)^n\right],$$

$$y_n = \frac{1}{2\sqrt{2}}\left[\left(x_1 + \sqrt{d}\,y_1\right)^n - \left(x_1 - \sqrt{d}\,y_1\right)^n\right],$$

(x_1, y_1) – фундаментальное решение.

Пример. Для уравнения $x^2 - 2y^2 = 1$ фундаментальным решением будет пара (3, 2). Поэтому формулы принимают вид:

$$x_n = \frac{1}{2}\left[\left(3+2\sqrt{2}\right)^n + \left(3-2\sqrt{2}\right)^n\right],$$

$$y_n = \frac{1}{2\sqrt{2}}\left[\left(3+2\sqrt{2}\right)^n - \left(3-2\sqrt{2}\right)^n\right].$$

В частности, следующая пара, которая является решением:

$$x_2 = \frac{1}{2}\left[\left(3+2\sqrt{2}\right)^2 + \left(3-2\sqrt{2}\right)^2\right] = \frac{1}{2}\left[\left(9+12\sqrt{2}+8\right) + \left(9-12\sqrt{2}+8\right)\right] = 17,$$

$$y_2 = \frac{1}{2\sqrt{2}}\left[\left(3+2\sqrt{2}\right)^n - \left(3-2\sqrt{2}\right)^n\right] = \frac{1}{2\sqrt{2}}\left[\left(9+12\sqrt{2}+8\right) - \left(9-12\sqrt{2}+8\right)\right] = 12.$$

Рассмотрим уравнение более общего вида:

$x^2 - dy^2 = c,$ (4)

где d – целое положительное число, $\sqrt{d}$ – иррациональное число, $c \in \mathbb{Z}$.

Теорема. Если уравнение (4) имеет хотя бы одно решение, то оно имеет бесконечное множество решений.

Решение уравнений второй степени с двумя неизвестными общего вида $Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$, где $A, B, C, D, E, F \in \mathbb{Z}$, сводится с помощью замен переменных к уравнению вида (4).

Некоторые ***методы решения*** нелинейных диофантовых уравнений.

1. Метод разложения на множители:

1) уравнение, с помощью группировки слагаемых и вынесения общих множителей, приводится к виду, когда в левой части уравнения стоит произведение сомножителей, содержащих неизвестные, а в правой части стоит некоторое число;

2) на следующем шаге рассматриваются все делители числа в правой части;

3) далее проводится исследование, в которых каждый сомножитель, стоящий в левой части приравнивается к соответствующему делителю числа, стоящего в правой части.

2. Метод испытания остатков:

исследуются всевозможные остатки левой и правой части от деления на некоторое фиксированное натуральное число.

§5. ЧИСЛОВЫЕ ФУНКЦИИ

Определение. Комплекснозначная функция $f(n)$ называется ***числовой функцией*** (или *арифметической функцией*), если значение $f(n)$ определено для любого натурального числа n.

Известными числовыми функциями являются функции целая часть числа и дробная часть числа.

Определение. Функция ***целая часть*** действительного числа x, обозначаемая $[x]$, есть наибольшее целое число m, не превосходящее x, т.е. $m \le x < m+1$. Функция ***дробная часть*** действительного числа x, обозначаемая $\{x\}$, определяется как $\{x\} = x - [x]$.

Примеры. $[2{,}8] = 2,\ [-3] = -3,\ [-2{,}2] = -3.$
$\{2{,}8\} = 0{,}8,\ \{-3\} = 0, \{-2{,}2\} = 0{,}8.$

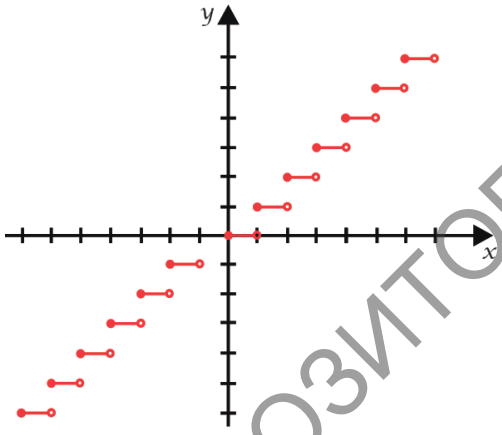


График функции $f(x) = [x]$.

Свойства функции $[x]$:

1) $|\{n \in \mathbb{N} : n \le x,\ n \vdots d\}| = \left[\frac{x}{d}\right]$ для любого положительного действительного числа x и любого натурального числа d;

2) $\left[\frac{[x]}{d}\right] = \left[\frac{x}{d}\right]$ для любого положительного действительного числа x и любого натурального числа d;

3) наибольший показатель α, с которым простое число p входит в каноническое разложение числа $n!$, находится по формуле: $\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^k}\right]$, где k такое число, что $p^k \le n < p^{k+1}$.

Рассмотрим функцию $\tau(n) = \sum_{n:d} 1$, дающую ***число*** натуральных ***делителей*** натурального числа n, и функцию $\sigma(n) = \sum_{n:d} d$, дающую ***сумму*** натуральных ***делителей*** натурального числа n.

Пример. $\tau(6) = 4,\ \sigma(6) = 12.$

Теорема. Если $n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot \ldots \cdot {p_k}^{\alpha_k}$ – каноническое разложение, то:
$\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_k + 1) = \prod_{j=1}^{k}(\alpha_j + 1)$;
$\sigma(n) = \prod_{j=1}^{k}\left(\frac{{p_j}^{\alpha_j+1}-1}{p_j-1}\right)$.

Определение. Числовая функция $\theta(n)$ называется ***мультипликативной***, если $\theta(1) = 1$ и $\theta(m \cdot n) = \theta(m) \cdot \theta(n)$ для любых взаимно простых m и n.

Пример. Функция $\theta(n) = n^2$ – мультипликативная, так как $\theta(1) = 1$ и $\theta(m \cdot n) = (m \cdot n)^2 = m^2 \cdot n^2 = \theta(m) \cdot \theta(n)$.

Свойства мультипликативных функций:

1) если $\theta_1(n)$ и $\theta_2(n)$ – мультипликативные функции, то функция $\theta(n) = \theta_1(n) \cdot \theta_2(n)$ – мультипликативная функция, т. е. произведение мультипликативных функций есть мультипликативная функция;

2) если $\theta(n)$ – мультипликативная функция и $n_1, n_2, \ldots, n_k$ – попарно взаимно простые числа, то $\theta(n_1 \cdot n_2 \cdot \ldots \cdot n_k) = \theta(n_1) \cdot \theta(n_2) \cdot \ldots \cdot \theta(n_k)$;

3) мультипликативная функция полностью определяется её значениями на степенях простых чисел: если $n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot \ldots \cdot {p_k}^{\alpha_k}$ – каноническое разложение и $\theta(n)$ – мультипликативная функция, то $\theta(n) = \theta({p_1}^{\alpha_1}) \cdot \theta({p_2}^{\alpha_2}) \cdot \ldots \cdot \theta({p_k}^{\alpha_k})$;

4) функции $\tau(n)$ и $\sigma(n)$ являются мультипликативными функциями.

Определение. Делители числа n за исключением самого n называются *собственными делителями* числа n. Их сумма равна $\sigma(n) - n$.

Определение. Если для двух натуральных чисел сумма собственных делителей каждого из них равна второму числу, то такие числа называются ***дружественными***. Для таких чисел: $\sigma(a) - a = b$, а $\sigma(b) - b = a$, следовательно, $\sigma(a) = \sigma(b) = a + b$.

Определение. Натуральное число называется ***совершенным,*** если оно равно сумме своих собственных делителей (или дружественно само себе). Это значит, что: $\sigma(n) - n = n$ или $\sigma(n) = 2n$.

Определение дружественных и совершенных чисел имеется уже в «Началах» Евклида. Древним грекам были известны дружественные числа 220 и 284, а также совершенные числа $6, 28, 496, 8128$.

Теорема (Евклид). Если число n имеет вид $n = 2^{k-1}(2^k - 1)$, где $k > 1$ натуральное число, а $2^k - 1$ – простое, то число n – *совершенное*.

Эйлер доказал, что достаточное условие Евклида для чётных совершенных чисел является так же необходимым. Количество чётных совершенных чисел, очевидно, совпадет с количеством простых чисел Мерсенна $M_k = 2^k - 1$.

Определение. Для натурального числа n ***функция Эйлера*** $\varphi(n)$ определяется как число натуральных чисел, не превосходящих n и *взаимно простых* с n.

Примеры. $\varphi(1) = 1$; $\varphi(6) = 2$; $\varphi(8) = 4$, т.к. ровно четыре натуральных числа не превосходят 8 и являются взаимно простыми с 8 (это числа 1, 3, 5, 7).

Свойства функции Эйлера:

1) $\varphi(p) = p - 1$ для любого простого p;

2) $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ для любого простого p и любого натурального α.

Определение. Функция Мёбиуса $\mu(n)$ определена для всех натуральных чисел n и принимает значения из множества $\{-1, 0, 1\}$ в зависимости от разложения n на простые множители: $\mu(n) = 1$, если n – свободное от квадратов число с чётным числом простых делителей; $\mu(n) = -1$, если n – свободное от квадратов число с нечётным числом простых делителей; $\mu(n) = 0$, если n не является свободным от квадратов числом, т.е.

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ (-1)^s, & \text{если } n = p_1 \cdot p_2 \cdot \ldots \cdot p_s, \\ 0, & \text{если } \exists p: n \vdots p^2, \end{cases}$$

где $p_1, p_2, \ldots, p_s$ – попарно различные простые числа, p – простое число.

Примеры.

$\mu(6) = 1$, т.к. $6 = 2 \cdot 3$ – свободное от квадратов число, имеющее два простых делителя;

$\mu(70) = -1$, т.к. $70 = 2 \cdot 5 \cdot 7$ – свободное от квадратов число, имеющее три простых делителя;

$\mu(50) = 0$, т.к. $50 = 2 \cdot 5^2$ делится на квадрат простого числа 5, и, следовательно, не является числом свободным от квадратов.

Свойства функции Мёбиуса:

1) функция Мебиуса является мультипликативной;

2) $\sum_{n:d} \mu(d) = 1$, если $n = 1$; и $\sum_{n:d} \mu(d) = 0$, если $n > 1$.

Глава 2. ОТНОШЕНИЕ СРАВНИМОСТИ В КОЛЬЦЕ ЦЕЛЫХ ЧИСЕЛ

§1. СРАВНЕНИЯ И ИХ ОСНОВНЫЕ СВОЙСТВА

Определение. Два целых числа a и b называются ***сравнимыми*** по модулю m ($m \in \mathbb{N}$, $m \geq 2$), если a и b имеют *одинаковые остатки* при делении на m.

Два целых числа a и b сравнимы по модулю m, если *разность* чисел a и b *делится* на m: $(a - b) \vdots m$ (эквивалентное определение).

Обозначение. $a \equiv b (\mathrm{mod}\ m)$.

Пример. $-27 \equiv 15 (\mathrm{mod}\ 7)$, т.к. $-27 = 7 \cdot (-4) + 1$ и $15 = 7 \cdot 2 + 1$ (числа –27 и 15 имеют одинаковые остатки при делении на 7). С другой стороны, (–27) – 15= – 42 и $(-42) \vdots 7$ (разность чисел –27 и 15 делится на7).

Свойства отношения сравнимости:

1) отношение сравнимости $\equiv$ является отношением эквивалентности на множестве целых чисел:

$a \equiv a(mod\ m)$ (рефлективность),

$a \equiv b(mod\ m) \Rightarrow b \equiv a(mod\ m)$ (симметричность),

$a \equiv b (\mathrm{mod}\ m)$ и $b \equiv c (\mathrm{mod}\ m) \Rightarrow a \equiv c (\mathrm{mod}\ m)$ (транзитивность);

2) $a \equiv b (\mathrm{mod}\ m) \Leftrightarrow \exists\, t \in \mathbb{Z} : a = b + mt$ (критерий сравнимости);

3) сравнения по одинаковому модулю можно почленно складывать и умножать;

4) обе части сравнения можно возвести в одну и ту же степень;

5) слагаемое, стоящее в какой-либо части сравнения, можно переносить в другую часть, изменив его знак на противоположный;

6) к любой части сравнения можно добавить число, кратное модулю;

7) обе части сравнения можно умножить на одно и то же целое число;

8) обе части сравнения и его модуль можно умножить на одно и то же натуральное число или разделить на их общий делитель;

9) обе части сравнения можно разделить на их общий делитель, взаимно простой с модулем;

10) если число a сравнимо с числом b по нескольким разным модулям, то a сравнимо с b и по модулю, равному наименьшему общему кратному этих модулей.

§2. ПОЛНАЯ И ПРИВЕДЕННАЯ СИСТЕМЫ ВЫЧЕТОВ

Отношение сравнимости чисел по модулю m рефлексивно, симметрично и транзитивно, т.е. является отношением эквивалентности на множестве $\mathbb{Z}$ и разбивает множество $\mathbb{Z}$ на классы сравнимых между собой по модулю m чисел.

Определение. Множество всех целых чисел, сравнимых с данным числом a по модулю m, называется ***классом вычетов*** (числа a) по модулю m.

Обозначения: $\overline{a}_m = \{k \in \mathbb{Z} \mid k \equiv a\ (mod\ m)\}$ или просто $\overline{a}$, когда из контекста понятно, по какому модулю рассматривается класс вычетов.

Пример. Для модуля $m = 5$ класс вычетов: $\overline{3} = \{k \in \mathbb{Z} \mid k \equiv 3\ (\mathrm{mod}\ 5)\} =$
$= \{\ldots, 3 - 5 \cdot 3, 3 - 5 \cdot 2,\ 3 - 5,\ 3,\ 3 + 5, 3 + 5 \cdot 2,\ 3 + 5 \cdot 3, \ldots\} =$
$\{\ldots, -12, -7, -2,\ 3,\ 8,\ 13,\ 18, \ldots\}$.

Свойства классов вычетов:

1) $\overline{a} = \{a + mt \mid\ t \in \mathbb{Z}\}$;
2) $\overline{a} = \overline{b} \Leftrightarrow a \equiv b(\mathrm{mod}\ m)$;
3) число классов вычетов по модулю m равно m;
4) все числа одного класса вычетов по модулю m имеют с модулем m один и тот же наибольший общий делитель: если $k \in \overline{a}$, то $НОД(k, m) = НОД(a, m)$;
5) число классов вычетов по модулю m, взаимно простых с m, равно $\varphi(m)$.

Сложение и умножение на множестве $\mathbb{Z}_m = {}^{\mathbb{Z}}/_{m\mathbb{Z}} = \{\overline{0},\ \overline{1},\ \overline{2}, \ldots, \overline{m-1}\}$ всех ***классов вычетов*** по модулю m определяются следующим образом:

$\overline{a} + \overline{b} = \overline{a + b}$,
$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

В этом случае $\mathbb{Z}_m$ превращается в *коммутативное кольцо с единицей,* содержащее m элементов (называется ***кольцом классов вычетов***).

Если p – простое число, то множество $\mathbb{Z}_p$ образует поле.

Теорема. Мультипликативная группа кольца $\mathbb{Z}_m$ (обозначается $\mathbb{Z}_m^*$) состоит из классов вычетов, взаимно простых с модулем m и порядок этой группы $|\mathbb{Z}_m^*| = \varphi(m)$.

Определение. Полной системой вычетов по модулю m (*обозначение:* ПСВ_m) называется система чисел, взятых по одному из каждого класса вычетов по модулю m. ***Приведенной системой вычетов*** по модулю m (*обозначение:* ПрСВ_m) называется система чисел, взятых по одному из каждого класса вычетов по модулю m, взаимно простых с модулем m.

Примеры.

$\text{ПСВ}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ (система наименьших неотрицательных вычетов);

$\text{ПСВ}_7 = \{-3, -2, -1, 0, 1, 2, 3\}$ (система абсолютно наименьших вычетов);

а также $\text{ПСВ}_7 = \{-17, -9, 13, 14, -20, 9, -4\}$;

$\text{ПрСВ}_7 = \{1, 2, 3, 4, 5, 6\}$; а также $\text{ПрСВ}_7 = \{-3, -2, -1, 1, 2, 3\}$ и

$\text{ПрСВ}_7 = \{-17, -9, 13, \ -20, 9, -4\}$;

$\text{ПСВ}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $\text{ПрСВ}_{10} = \{1, 3, 7, 9\}$ (ПрСВ_m можно выделить из полной системы наименьших неотрицательных вычетов отбором вычетов взаимно простых с m).

Свойства полной и приведенной систем вычетов:

1) $|\text{ПСВ}_\text{m}| = \text{m}$;

2) $|\text{ПрСВ}_\text{m}| = \varphi(\text{m})$, где $\varphi(\text{m})$ – функция Эйлера (это следует из определения ПрСВ_m).

Теорема (*признак* $\text{ПСВ}_{\boldsymbol{m}}$ – полной системы вычетов по модулю m). Система m *попарно несравнимых* целых чисел по модулю m чисел образует полную систему вычетов по модулю m.

Свойство. Если $\{\text{x}_1, \ \text{x}_2, \dots, \text{x}_\text{m}\} = \text{ПСВ}_\text{m}$, то $\{\text{ax}_1 + \text{b}, \ \text{ax}_2 + \text{b}, \dots, \text{ax}_\text{m} + \text{b}\} = \text{ПСВ}_\text{m}$ для любого целого b и любого целого a, взаимно простого с m.

Все числа фиксированного класса вычетов по модулю m имеют один и тот же НОД с модулем m.

Теорема (*признак* $\text{ПрСВ}_{\boldsymbol{m}}$ – приведенной системы вычетов по модулю m). Система из $\varphi(m)$ чисел *несравнимых* между собой по модулю m и *взаимно простых* с модулем m образуют приведенную систему вычетов по модулю m.

Свойство. Если $\{\text{x}_1, \ \text{x}_2, \dots, \text{x}_{\varphi(\text{m})}\} = \text{ПрСВ}_\text{m}$, то $\{\text{ax}_1, \ \text{ax}_2, \dots, \text{ax}_{\varphi(\text{m})}\} = \text{ПрСВ}_\text{m}$ для любого целого a, взаимно простого с m.

Теорема. Функция Эйлера является ***мультипликативной,*** т.е. если натуральные числа a и b взаимно просты, то $\boldsymbol{\varphi(ab) = \varphi(a)\varphi(b)}$.

Теорема (формула для вычисления функции Эйлера).

Если $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ – каноническое разложение натурального числа n, то $\boldsymbol{\varphi(n) = p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_s^{\alpha_s - 1}(p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_s - 1)}$.

Другая запись этой же формулы: $\boldsymbol{\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_s}\right)}$.

Теорема (тождество Гаусса). $\sum_{n:d} \varphi(d) = n$.

§3. МАЛАЯ ТЕОРЕМА ФЕРМА И ТЕОРЕМА ЭЙЛЕРА

Теорема Эйлера. $\boldsymbol{a^{\varphi(m)} \equiv 1 (mod\ m)}$ для любого целого числа a, *взаимно простого* с m.

Малая теорема Ферма. $\boldsymbol{a^{p-1} \equiv 1 (mod\ p)}$ для любого простого числа p и любого целого числа a, *взаимно простого* с p.

Следствие. $a^p \equiv a (\mathrm{mod}\ p)$ для любого простого числа p и любого целого числа a.

Теорема Вильсона. $(p-1)! + 1 \equiv 0 (\mathrm{mod}\ p)$ для любого простого числа p.

§4. ЛИНЕЙНЫЕ СРАВНЕНИЯ И СИСТЕМЫ СРАВНЕНИЙ

Определение. Линейным сравнением (другое название: *сравнение первой степени*) называется сравнение вида $\boldsymbol{ax \equiv b (mod\ m)}$, где $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, $a \not\equiv 0 (mod\ m)$.

Если $ac \equiv b(mod\ m)$ для некоторого $c \in \mathbb{Z}$, то $ax \equiv b(mod\ m)$ для любого $x \equiv c(mod\ m)$. В этом случае говорят, что класс вычетов $\overline{c}_m = \{x \in \mathbb{Z} \mid x \equiv c(mod\ m)\}$ является ***решением*** сравнения $ax \equiv b(mod\ m)$.

Теорема (*о линейных сравнениях*). Линейное сравнение $ax \equiv b(mod\ m)$ имеет:

- ✓ единственное решение, если НОД$(a, m) = 1$;
- ✓ ровно d решений, если НОД$(a, m) = d$ и $b \vdots d$;
- ✓ не имеет решений в остальных случаях (если НОД$(a, m) = d$ и b не делится d).

При этом единственное решение $x \equiv c(mod\ m)$ для случая НОД$(a, m) = 1$ может быть найдено различными способами.

Способы решения линейных сравнений:

1) ***перебор*** представителей всех классов вычетов по модулю m до первого подходящего класса (этот способ применим для малых значений m);

2) ***преобразование коэффициентов:*** рассматриваются последовательно сравнения $ax \equiv b(mod\ m)$, $ax \equiv b + m(mod\ m)$, $ax \equiv b + 2m(mod\ m)$, …, $ax \equiv b + km(mod\ m)$, … с целью получения в правой части числа $b + km$, которое делится на a, тогда искомое решение принимает вид:

$$x \equiv \frac{km+b}{a} (\mathrm{mod}\, m);$$

3) использование теоремы Эйлера: так как $a^{\varphi(m)} \equiv 1(mod\ m)$, то искомое решение принимает вид: $\boldsymbol{x \equiv a^{\varphi(m)-1} b (mod\ m)}$;

4) использование свойств подходящих дробей: искомое решение имеет вид $x \equiv (-1)^s P_{s-1} b(mod\ m)$, где P_{s-1} – числитель предпоследней подходящей дроби при разложении $\frac{m}{a}$ в конечную цепную дробь.

Линейные сравнения и линейные диофантовы уравнения с двумя неизвестными: нахождение частного решения.

Рассмотрим линейное диофантово уравнение $ax + by = c$, НОД$(a, b) = 1$.

Это уравнение разрешимо в целых числах (т.к. a и b взаимно просты). Следовательно, $(c - ax) \vdots b$ (делится). Перейдём к сравнению $ax \equiv c(mod\ b)$. Пусть x_0 –решение последнего сравнения (этому сравнению будут удовлетворять также числа $x_0 - bt,\ t \in \mathbb{Z}$). Тогда $\left(x_0,\ \frac{c-ax_0}{b} \right)$ – частное решение линейного диофантова уравнения $ax + by = c$, НОД$(a, b) = 1$. Его общим решением будет $\left(x_0 - bt,\ \frac{c-ax_0}{b} + at \right)$, $t \in \mathbb{Z}$.

Рассмотрим систему линейных сравнений от одной неизвестной с попарно взаимно простыми модулями $m_1,\ m_2,\ \ldots,\ m_k$ (т. е. НОД$(m_i, m_j) = 1$ при $i \neq j$):

$$\begin{cases} a_1x \equiv b_1(mod\ m_1) \\ a_2x \equiv b_2(mod\ m_2) \\ \quad \ldots\ldots \\ a_kx \equiv b_k(mod\ m_k) \end{cases}.$$

Решением этой системы сравнений является класс вычетов, который удовлетворяет каждому сравнению системы. Если какое-то сравнение не имеет решений, то вся система несовместна. Каждое из этих сравнений можно решить отдельно и получить систему линейных сравнений, эквивалентную исходной системе:

$$\begin{cases} x \equiv b_1(mod\ m_1) \\ x \equiv b_2(mod\ m_2) \\ \quad \ldots \\ x \equiv b_k(mod\ m_k) \end{cases}.$$

Система такого вида выражает условие ***старинной китайской задачи:*** найти число, которое при делении на m_1 дает остаток b_1,при делении на m_2 дает остаток b_2 ,…, при делении на m_k дает остаток b_k.

Китайская теорема об остатках. Система линейных сравнений

$$\begin{cases} x \equiv b_1(mod\ m_1) \\ x \equiv b_2(mod\ m_2) \\ \quad \ldots \\ x \equiv b_k(mod\ m_k) \end{cases}$$

с попарно взаимно простыми модулями $m_1, m_2,\ldots, m_k$ имеет единственное решение по модулю $M = m_1\ m_2\ \ldots m_k$ и это решение имеет вид:

$x \equiv M_1M_1'b_1 + M_2M_2'b_2 + \cdots + M_kM_k'b_k\ (modM)$, где $M_i = \frac{M}{m_i}$, M_i' – решение сравнения $M_iM_i' \equiv 1\ (mod\ m_i),\ 1 \leq i \leq k$.

§5. ПЕРВООБРАЗНЫЕ КОРНИ И ИНДЕКСЫ

Определение. Для данного натурального числа m и данного целого числа a, взаимно простого с m, ***порядком*** (другое название: *показателем*) числа a по модулю m называется наименьшее натуральное число k такое, что $a^k \equiv 1(mod\ m)$.

Обозначение: $P_m(a)$ (или просто $P(a)$, если из контекста понятно по какому модулю рассматривается порядок).

Определение. Целое число g называется ***первообразным корнем*** по модулю m, если $P_m(g) = \varphi(m)$.

Примеры: 1) $\boldsymbol{P_5(3) = 4}$, так как $3^4 \equiv 1(mod\ 5)$, но $3^1 \not\equiv 1(mod\ 5)$, $3^2 \not\equiv 1(mod\ 5)$, $3^3 \not\equiv 1(mod\ 5)$; 2) $\boldsymbol{P_5(4) = 2}$, так как $4^2 \equiv 1(mod\ 5)$ но $4^1 \not\equiv 1(mod\ 5)$. Функция Эйлера $\varphi(5) = 4$, поэтому число 3 является первообразным корнем по модулю 5, а число 4 не является первообразным корнем по модулю 5; 3) число **2** является *первообразным корнем по модулю* 11, так как $2^{10} \equiv 1(mod\ 11)$, но $2^k \not\equiv 1(mod\ 11)$ для $k \in \{1, 2, \dots, 9\}$; 4) число **2** является *первообразным корнем по модулю* 37, так как $2^{36} \equiv 1(mod\ 37)$, но $2^k \not\equiv 1(mod\ 36)$ для $k \in \{1, 2, \dots, 35\}$; 5) по модулю 8 не существует первообразных корней (существуют только числа порядков 1 и 2), т.е. не по любому модулю существуют первообразные корни.

Теорема. По простому модулю p существует первообразный корень.

Теорема. По модулям $\boldsymbol{2, 4, p^\alpha, 2p^\alpha,}$ где p – нечётное простое число, $\alpha \in \mathbb{N}$, и только по этим модулям, существуют первообразные корни.

Теорема. Для каждого нечётного простого p существует $\varphi(p-1)$ классов первообразных корней по модулю p.

Свойства порядков *(показателей):*

1) если одно число классов вычетов по модулю m имеет порядок k, то и все числа этого класса имеют порядок k по модулю m: $\boldsymbol{a \equiv b(mod\ m) \Rightarrow P_m(a) = P_m(b)}$ (поэтому мы можем называть число k порядком класса вычетов $\overline{a}_m$ и обозначать $\boldsymbol{P_m(\overline{a})}$);

2) если $P_m(a) = k$ и $a^n \equiv 1(mod\ m)$, то $n \vdots k$;

3) $\varphi(m) \vdots P_m(a)$ (порядок числа a по модулю m является делителем $\varphi(m)$);

4) если $P_m(a) = k$, то $a^{k_1} \equiv a^{k_2}(mod\ m) \Leftrightarrow k_1 \equiv k_2(mod\ k)$ (критерий сравнимости степеней);

5) если $P_m(a) = k$, то числа $a^0, a^1, a^2 \dots a^{k-1}$ попарно несравнимы по модулю m (принадлежат различным классам вычетов по модулю m);

6) для первообразного корня g по модулю m числа $g^0,\ g^1,\ g^2, \dots, g^{\varphi(m)-1}$ образуют приведенную систему вычетов по модулю m (ПрСВ_m);

7) $P_m(a^s) = \dfrac{P_m(a)}{НОД(s,\ P_m(a))}$;

8) если $P_m(a) = kl$, то $P_m(a^k) = l$ (связь между порядком числа и порядком его степени);

9) если $P_m(a_1) = k_1$, $P_m(a_2) = k_2$ и $\text{НОД}(k_1, k_2) = 1$ (взаимно простые числа), то $P_m(a_1 a_2) = k_1 k_2$.

Следствие (обобщение свойства 9). Если $P_m(a_1) = k_1$, $P_m(a_2) = k_2$, …, $P_m(a_s) = k_s$ и числа $k_1, k_2, \dots, k_s$ попарно взаимно простые, то $P_m(a_1 a_2 \dots a_s) = k_1 k_2 \dots k_2$.

Пример. Числа $2^0,\ 2^1,\ 2^2, \dots, 2^9$ образуют приведенную систему вычетов по модулю 11 (ПрСВ_{11}).

Определение. Пусть g – первообразный корень по простому модулю p (первообразный корень по простому модулю всегда существует). Целое число $k \geq 0$ называется ***индексом*** числа a по модулю p и основанию (первообразному корню) g, если $g^k \equiv a (mod\ p)$.

Обозначение. Для краткости при фиксированном модуле p это записывается в виде $k = \boldsymbol{ind_g a}$, а если фиксировано также и основание g, то еще короче: $k = ind\ a$.

Согласно определению, $g^{ind_g a} \equiv a (mod\ p)$.

Обобщение. Поскольку первообразные корни существуют только по модулям $2, 4, p^\alpha, 2p^\alpha$, где p – нечётное простое число, $\alpha \in \mathbb{N}$, то и понятие индекса можно определить только по модулю из указанного списка. В частности, мы всегда можем говорить об индексах по простому модулю p.

Если $a_1 \in \overline{a}_p$, то из $g^s \equiv a (mod\ p)$ следует также $g^s \equiv a_1 (mod\ m)$, т.е. индекс числа a по модулю p и основанию g является также индексом и всех чисел из класса вычетов $\overline{a}_p$.

Если g – первообразный корень по модулю p, то числа $g^0, g^1, g^2, \dots, g^{p-2}$ образуют приведенную систему вычетов по модулю p (ПрСВ_p). Если число a взаимно просто с p, то в последовательности $g^0, g^1, g^2, \dots, g^{p-2}$ существует некоторое число g^s такое, что $g^s \equiv a(mod\, p)$ (принадлежит тому же классу вычетов, что и a). Если $g^{s_1} \equiv a(mod\, p)$, то $g^s \equiv g^{s_1}(mod\, p)$, следовательно, $s \equiv s_1(mod\ (p-1))$, т.е. любое число a, взаимно простое с p, имеет бесконечное множество индексов по модулю p и основанию (первообразному корню) g. Обычно из всех возможных значений индекса числа a по основанию g берут наименьшее и в качестве индекса указывают одно из чисел: $0, 1, 2, \dots, p-2$. Существует ***биекция*** между приведенной системой положительных вычетов по простому модулю p ($\text{ПрСВ}_p = \{1, 2, \dots, p-1\}$) и полной системой неотрицательных вычетов по модулю $(p-1)$ ($\text{ПСВ}_{p-1} = \{0, 1, 2, \dots, p-2\}$).

Свойства индексов по простому модулю p:

1) $ind_g 1 \equiv 0\ (mod\ (p-1))$;

2) $ind_g g \equiv 1\ (mod\ (p-1))$;

3) $a \equiv b(mod\, p) \Leftrightarrow\ ind_g a \equiv ind_g b\ (mod\ (p-1))$;

4) $ind_g(ab) \equiv ind_g a + ind_g b(mod\ (p-1))$;

5) $ind\ a^n \equiv \text{n ind a}(\text{mod}\ (\text{p}-1))$для любого $n \in \mathbb{N}$;

6) $ind_g \frac{b}{a} \equiv ind_g b - ind_g a\ (\text{mod}\ (p-1))$;

7) если g, g_1 – два первообразных корня по модулю p и числа a и p взаимно просты, то $ind_g a \equiv ind_{g_1} a \cdot ind_{g_1} g(mod\ (p-1))$ (*формула перехода* от основания g_1 к основанию g).

Следствие (обобщение свойства 4). $ind_g(a_1 \dots a_n) \equiv ind_g a_1 + \dots + ind_g a_n(mod\ (p-1))$.

Очевидно, что понятие индекса аналогично понятию логарифма. Для практических целей (решения задач) составлены таблицы индексов, по которым можно находить индекс по числу или число по индексу.

Таблицы индексов для простых модулей p содержат индексы чисел от 1 до $p-1$ (ПрСВ_p). Для каждого такого числа и всех сравнимых с ним по модулю p в таблице указывается индекс, представляющий собой одно из чисел: $0, 1, \dots, p-2$ (ПСВ_{p-1}).

Пример 1. Составим ***таблицу индексов*** по модулю 11, используя первообразный корень 2. Получаем последовательно: $2^0 \equiv 1(mod\ 11)$, $2^1 \equiv 2(mod\ 11)$, $2^2 \equiv 4(mod\ 11)$, $2^3 \equiv 8(mod\ 11)$, $2^4 \equiv 5(mod\ 11)$, $2^0 \equiv 10(mod\ 11)$, $2^6 \equiv 9(mod\ 11)$, $2^7 \equiv 7(mod\ 11)$, $\mathbf{2^8 \equiv 3(mod\ 11)}$, $2^9 \equiv 6(mod\ 11)$. Следовательно, $ind\ 1 = 0$, $ind\ 2 = 1$, $\boldsymbol{ind\ 3 = 8}$, $ind\ 4 = 2$, $ind\ 5 = 4$, $ind\ 6 = 9$, $ind\ 7 = 7$, $ind\ 8 = 3$, $ind\ 9 = 6$ (все индексы рассматриваются по основанию 2). Таблица индексов по модулю 11 имеет вид:

Таблица для нахождения по данному числу соответствующего ему индекса $(p = 11, g = 2)$

N	0	1	2	3	4	5	6	7	**8**	9
0		0	1	8	2	4	9	7	**3**	6
1	*5*									

Таблица для нахождения по данному индексу соответствующего ему числа $(p = 11, g = 2)$

Ind	0	1	2	**3**	4	5	6	7	8	9
0		0	1	**8**	2	4	9	7	3	6

В учебниках можно встретить таблицы индексов, составленные по различным первообразным корням для одного и того же простого числа. Это не влияет на результаты вычислений.

Пример 2. Составим ***таблицу индексов*** по модулю 37, используя первообразный корень 2. Получаем последовательно:

$2^0 \equiv 1\ (mod\ 37)$
$2^1 \equiv 2\ (mod\ 37)$
$2^2 \equiv 4\ (mod\ 37)$
$2^3 \equiv 8\ (mod\ 37)$
$2^4 \equiv 16\ (mod\ 37)$
$2^5 \equiv 32\ (mod\ 37)$
$2^6 \equiv 27\ (mod\ 37)$
$2^7 \equiv 17\ (mod\ 37)$
$2^8 \equiv 34\ (mod\ 37)$
$2^9 \equiv 31\ (mod\ 37)$
$2^{10} \equiv 25\ (mod\ 37)$
$2^{11} \equiv 13\ (mod\ 37)$
$2^{12} \equiv 26\ (mod\ 37)$
$2^{13} \equiv 15\ (mod\ 37)$
$2^{14} \equiv 30\ (mod\ 37)$
$2^{15} \equiv 23\ (mod\ 37)$
$2^{16} \equiv 9\ (mod\ 37)$
$2^{17} \equiv 18\ (mod\ 37)$
$2^{18} \equiv 36\ (mod\ 37)$
$2^{19} \equiv 35\ (mod\ 37)$
$2^{20} \equiv 33\ (mod\ 37)$
$2^{21} \equiv 29\ (mod\ 37)$
$2^{22} \equiv 21\ (mod\ 37)$
$2^{23} \equiv 5\ (mod\ 37)$
$2^{24} \equiv 10\ (mod\ 37)$
$2^{25} \equiv 20\ (mod\ 37)$
$2^{26} \equiv 3\ (mod\ 37)$
$2^{27} \equiv 6\ (mod\ 37)$
$2^{28} \equiv 12\ (mod\ 37)$
$2^{29} \equiv 24\ (mod\ 37)$
$2^{30} \equiv 11\ (mod\ 37)$
$2^{31} \equiv 22\ (mod\ 37)$
$2^{32} \equiv 7\ (mod\ 37)$
$2^{33} \equiv 14\ (mod\ 37)$
$2^{34} \equiv 28\ (mod\ 37)$
$2^{35} \equiv 19\ (mod\ 37)$

Таблица для нахождения по данному числу соответствующего ему индекса $(p = 37,\ g = 2)$

N	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
0		*0*	*1*	*26*	*2*	*23*	*27*	*32*	*3*	*16*
1	*24*	*30*	*28*	*11*	*33*	*13*	*4*	*7*	*17*	*35*
2	*25*	*22*	*31*	*15*	*29*	*10*	*12*	*6*	*34*	*21*
3	*14*	*9*	*5*	*20*	*8*	*19*	*18*			

Таблица для нахождения по данному индексу соответствующего ему числа $(p = 37,\ g = 2)$

Ind	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
0	*1*	*2*	*4*	*8*	*16*	*32*	*27*	*17*	*34*	*31*
1	*25*	*13*	*26*	*15*	*30*	*23*	*9*	*18*	*36*	*35*
2	*33*	*29*	*21*	*5*	*10*	*20*	*3*	*6*	*12*	*24*
3	*11*	*22*	*7*	*14*	*28*	*19*				

§6. КВАДРАТИЧНЫЕ ВЫЧЕТЫ И СИМВОЛ ЛЕЖАНДРА

Определение. Сравнение вида

$$\boldsymbol{ax^n \equiv b(mod\ p)},\ (1)$$

где a и p взаимно просты $(a \not\equiv 0(mod\ p))$, $n \in \mathbb{N}$, p – простое число, называется ***двучленным сравнением*** -ой степени с одной переменной x по простому модулю p.

Проиндексируем обе части сравнения по модулю p и некоторому первообразному корню (основанию) g: $ind_g a + n\, ind_g x \equiv ind_g b(mod\ (p-1))$ или

$$\boldsymbol{n\ ind_g x \equiv ind_g b - ind_g a\ (mod\ (p-1))}.\ (2)$$

Таким образом, решение двучленного сравнения -ой степени сводится к решению сравнения первой степени.

Если $НОД(n, p-1) = d$ и разность $(ind_g b - ind_g a) \vdots d$, то сравнение (2), а следовательно, и сравнение (1) имеет d решений. Если же $(ind_g b - ind_g a)$ не делится на d, то сравнение (2), а следовательно, и сравнение (1) не имеет решений.

Умножив обе части сравнения (1) на такое число m, что $am \equiv 1(mod\ p)$, получим сравнение $x^n \equiv c(mod\ p)$, где $c = mb$.

Определение. Целое число a, взаимно простое с простым числом p, называется *вычетом степени* n по модулю p, если сравнение

$$\boldsymbol{x^n \equiv a(mod\ p)}\ (3)$$

имеет решения. В противном случае a называется *невычетом* степени n по модулю p.

При $НОД(a, p) = 1$ и $НОД(n, p-1) = d$ сравнение $x^n \equiv a(mod\ p)$ имеет d решений, если $ind\ a \vdots d$, и не имеет решений, если $ind\ a$ не делится на d.

Теорема. Сравнение (3) имеет решение тогда и только тогда, когда $a^{\frac{p-1}{d}} \equiv 1(mod\ p)$, где $d = НОД(n, p-1)$.

Следствие 1. Число a является вычетом *степени* n по модулю p тогда и только тогда, когда справедливо сравнение: $a^{\frac{p-1}{d}} \equiv 1(mod\ p)$, где $d = НОД(n, p-1)$.

Следствие 2. По простому модулю p существует $\frac{p-1}{d}$ классов вычетов -ой степени по модулю p, где $d = НОД(n, p-1)$,

Определение. Показательным двучленным сравнением называется сравнение вида $ac^x \equiv b(mod\ p)$, где p – простое число, $a \not\equiv 0(mod\ p)$, $c \not\equiv 0(mod\ p)$.

Проиндексировав показательное сравнение $ac^x \equiv b(mod\ p)$ по модулю p и некоторому первообразному корню (основанию) g, получим сравнение первой степени (линейное сравнение): $x\ ind_g c \equiv\ ind_g b - ind_g a\ (mod\ (p-1))$. Решив это сравнение, найдём x.

Определение. Число a называется ***квадратичным вычетом*** по модулю p, если сравнение $\boldsymbol{x^2 \equiv a(mod\ p)}$, где p – нечётное простое число, имеет решение. Число a называется *квадратичным невычетом* по модулю p, если сравнение $x^2 \equiv a(mod\ p)$ не имеет решений.

Примеры. Число 2 является квадратичным *вычетом* по модулю 7, так как сравнение $x^2 \equiv 2(mod\ 7)$ разрешимо: $4^2 \equiv 2(mod\ 7)$. Число 3 является квадратичным *невычетом* по модулю 7, так как сравнение $x^2 \equiv 3(mod\ 7)$ решений не имеет (в этом можно убедиться последовательным перебором полной системы вычетов по модулю 7).

Теорема. Если a – квадратичный вычет по модулю p, то сравнение $x^2 \equiv a(mod\ p)$ имеет ровно два решения.

Теорема. Если a является квадратичным вычетом по модулю p и имеет место сравнение $b \equiv a(mod\ p)$, тогда b также является квадратичным вычетом по модулю p.

Теорема. По простому модулю $p > 2$ существует ровно $\frac{p-1}{2}$ классов квадратичных вычетов и $\frac{p-1}{2}$ классов квадратичных невычетов. Причём всякий квадратичный вычет сравним с одним из чисел $1^2, 2^2, \ldots \left(\frac{p-1}{2}\right)^2$.

Другими словами, приведенная система вычетов по простому модулю $p > 2$: $-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2}$ состоит из $\frac{p-1}{2}$ квадратичных вычетов, сравнимых с числами $1^2, 2^2, \ldots \left(\frac{p-1}{2}\right)^2$ и $\frac{p-1}{2}$ квадратичных невычетов, т.е. квадратичных вычетов и невычетов поровну. Количество квадратичных вычетов модулю p равно количеству квадратичных невычетов по модулю p и равно $\frac{p-1}{2}$.

Теорема (критерий Эйлера). Число a, взаимно простое с p (p – нечётное простое число), является квадратичным вычетом по модулю p тогда и только тогда, когда справедливо сравнение:

$a^{\frac{p-1}{2}} \equiv 1(mod\ p)$.

Число a, взаимно простое с p, является квадратичным невычетом по модулю p тогда и только тогда, когда справедливо сравнение

$a^{\frac{p-1}{2}} \equiv -1(mod\ p)$.

Примеры. 1. Выясним, разрешимо ли квадратичное сравнение $x^2 \equiv 3(mod\ 7)$?

Решение. Для этого выясним, будет ли число $a = 3$ квадратичным вычетом по модулю $p = 7$. Так как $3^{\frac{7-1}{2}} = 3^3 \equiv -1(mod\ 7)$, то отсюда следует, что 3 – квадратичный невычет по модулю 7, поэтому сравнение $x^2 \equiv 3(mod\ 7)$ неразрешимо.

2. Выясним, разрешимо ли квадратичное сравнение $x^2 \equiv 5(mod\ 7)$?

Решение. $5^{\frac{7-1}{2}} = 5^3 \equiv -1\ (\mathrm{mod}\ 7)$, поэтому 5 – квадратичный невычет по модулю 7, поэтому сравнение $x^2 \equiv 5(mod\ 7)$ неразрешимо.

3. Выясним, разрешимо ли квадратичное сравнение $x^2 \equiv 2(mod\ 7)$?

Решение. Теперь выясним, будет ли число $a = 2$ квадратичным вычетом по модулю $p = 7$. Так как $2^3 \equiv 1(mod\ 7)$, то отсюда следует, что 2 – квадратичный вычет по модулю 7 и сравнение $x^2 \equiv 2(mod\ 7)$ разрешимо (имеет два решения).

При изучении сравнений 2-ой степени удобно пользоваться так называемым символом Лежандра. Введение этого символа значительно облегчает вычисления и упрощает запись многих результатов.

Обозначение. $\left(\frac{a}{p}\right)$ – символ Лежандра для числа a по простому модулю $p > 2$.

Определение. Пусть p – простое нечётное число, a не кратно p. Тогда символ Лежандра $\left(\frac{a}{p}\right)$ определяется следующим образом:

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

Другими словами, $\left(\frac{a}{p}\right) = 1$, если сравнение $\boldsymbol{x^2 \equiv a(mod\ p)}$ разрешимо (имеет два решения), и $\left(\frac{a}{p}\right) = -1$, если сравнение $x^2 \equiv a(mod\ p)$ не имеет решений. Таким образом, с помощью символа Лежандра легко можно выяснить, сколько решений имеет сравнение $x^2 \equiv a(mod\ p)$, где p – нечётное простое число.

Примеры. 1) $\left(\frac{3}{11}\right) = 1$, так как сравнение $x^2 \equiv 3(mod\ 11)$ имеет два решения: $x \equiv \pm 5(mod\ 11)$; 2) $\left(\frac{5}{7}\right) = -1$, так как сравнение $x^2 \equiv 5(mod\ 7)$ не имеет решений.

Свойства символа Лежандра:

1) если $b \equiv a(mod\ p)$, то $\left(\frac{b}{p}\right) = \left(\frac{a}{p}\right)$;

2) $\left(\frac{\boldsymbol{a^2}}{\boldsymbol{p}}\right) = \mathbf{1}$, в частности, $\left(\frac{1}{p}\right) = 1$;

3) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ (mod\ p)$ (*критерий Эйлера*);

4) $\left(\frac{\boldsymbol{ab}}{\boldsymbol{p}}\right) = \left(\frac{\boldsymbol{a}}{\boldsymbol{p}}\right)\left(\frac{\boldsymbol{b}}{\boldsymbol{p}}\right)$**;**

5) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, т.е. $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{если } p \equiv 1(mod\ 4); \\ -1, & \text{если } p \equiv 3(mod\ 4); \end{cases}$

6) $\left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}$ т.е.

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{если } p \equiv 1(mod\ 8) \text{ или } p \equiv 7(mod\ 8); \\ -1, & \text{если } p \equiv 3(mod\ 8) \text{ или } p \equiv 5(mod\ 8); \end{cases}$$

7) для различных нечётных простых чисел p и q имеет место равенство: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ (*квадратичный закон взаимности*).

Следствие (обобщение свойства 4). $\left(\frac{a_1 a_2 \ldots a_n}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right) \ldots \left(\frac{a_n}{p}\right)$.

Следствие (свойства 7). $\left(\frac{\boldsymbol{q}}{\boldsymbol{p}}\right) = (\boldsymbol{-1})^{\frac{\boldsymbol{p-1}}{\boldsymbol{2}}\cdot\frac{\boldsymbol{q-1}}{\boldsymbol{2}}}\left(\frac{\boldsymbol{p}}{\boldsymbol{q}}\right)$ (эта формула получается после домножения левой и правой частей равенства на $\left(\frac{p}{q}\right)$ с учётом того, что $\left(\frac{p}{q}\right) = 1$ или (-1)).

Перечисленные свойства символа Лежандра позволяют вычислять $\left(\frac{a}{p}\right)$, а следовательно, определять, имеет ли решения сравнение $x^2 \equiv a(mod\ p)$.

Примеры. 1. Имеет ли решения сравнение $x^2 \equiv 68(mod\ 113)$?

Решение. 113 – простое число, $68 = 2^2 \cdot 17$. Последовательно находим: $\left(\frac{68}{113}\right) = \left(\frac{2}{113}\right)^2 \left(\frac{17}{113}\right) = \left(\frac{17}{113}\right) = \left(\frac{113}{17}\right)$ (использовали квадратичный закон взаимности). Имеет место сравнение $113 \equiv 11(mod\ 17)$, поэтому $\left(\frac{113}{17}\right) = \left(\frac{11}{17}\right)$. Продолжаем вычисления, используя свойства символа Лежандра: $\left(\frac{11}{17}\right) = \left(\frac{17}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = -\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) = \left(\frac{2}{3}\right) = -1$, поэтому сравнение $x^2 \equiv 68(mod\ 113)$ не имеет решений.

2. Имеет ли решения сравнение $x^2 \equiv 310(mod\ 521)$?

Решение. 521 – простое число, $310 = 2 \cdot 5 \cdot 31$. Вычисляем соответствующий символ Лежандра:

$$\left(\frac{310}{521}\right) = \left(\frac{2}{521}\right)\left(\frac{5}{521}\right)\left(\frac{31}{521}\right) = \left(\frac{521}{5}\right)\left(\frac{521}{31}\right) = \left(\frac{1}{5}\right)\left(\frac{25}{31}\right) = \left(\frac{5^2}{31}\right) = 1,$$

поэтому сравнение $x^2 \equiv 310(mod\ 521)$ имеет решения (и их два).

§7. АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ ТЕОРИИ СРАВНЕНИЙ

Для записи натуральных чисел обычно применяется *десятичная система счисления.* В этой системе счисления используется десять цифр: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Вместо десятичной системы счисления можно рассматривать g*-ичную систему счисления*, где $g \in \mathbb{N}$ и $g > 1$. В этом случае натуральное число записывается в виде: $a = a_n \cdot g^n + a_{n-1} \cdot g^{n-1} + \ ... + a_1 \cdot g + a_0$, где $0 \leq a_n < g$. Число g называется *основанием* системы счисления, а сумма степеней основания с коэффициентами, которые могут принимать значения от 0 до $g-1$, $\sum_{i=o}^{n} a_i \cdot g^i$, называется представлением числа a в системе счисления с основанием g (в -ичной системе счисления). Числа $a_n,\ a_{n-1},\ \ldots a_1,\ a_0$ – *цифры*, изображающие число a.

В случае $g = 2$ получаем *двоичную* систему счисления с цифрами 0, 1; при $g = 8$ – *восьмиричную* с цифрами 0, 1, …, 7; при $g = 16$ – *шестнадцатиричную* с цифрами 0, 1, …, 9, A, B, C, D, E, F (цифры A, B, C, D, E, F обозначают соответственно числа 10, 11, 12, 13, 14, 15, 16). В процессе решения задач иногда приходится переводить числа из одной системы счисления в другую.

Обозначение: $a = \sum_{i=o}^{n} a_i \cdot g^i = \overline{a_n\ a_{n-1}\ \ldots a_1\ a_0}_{(g)}$.

Черта сверху означает, что имеется в виду упорядоченная последовательность цифр, а не произведение чисел.

Теорема. Любое натуральное число единственным образом записывается в g -ичной системе счисления.

Применим некоторые из рассмотренных свойств сравнений для обращения обыкновенной дроби в десятичную.

Обыкновенные дроби – это числа вида $\frac{a}{b}$, где a и b – натуральные числа. Десятичная дробь – это другая форма записи дроби.

Определение. ***Десятичной дробью*** называется последовательность целых чисел $a_0, a_1, a_2, \ldots$, где $a_1, a_2, \ldots$ – цифры десятичной системы счисления, которая записывается в виде $\boldsymbol{a_0, a_1 a_2 \ldots}$, причём *цифра* 9 *не повторяется* бесконечное число раз подряд, т.е. для любого индекса i существует индекс $j > i$ такой, что $a_j \neq 9$ (этим устраняется неоднозначность типа $1 = 1{,}000\ldots$ и $1 = 0{,}999\ldots$). Целое число a_0 называется *целой частью* десятичной дроби. Дробь, имеющая бесконечное число знаков после запятой, называется *бесконечной* десятичной дробью (в противном случае дробь называется *конечной* десятичной дробью).

Определение. Десятичная дробь называется ***периодической,*** если существуют такие целые числа s $(s \geq 0)$ и t $(t > 0)$, что для любого индекса $i \in \mathbb{N}$ выполняется равенство $a_{s+t+i} = a_{s+i}$. Наименьшее s называется числом цифр в предпериоде (число знаков до периода), а наименьшее t – числом цифр в периоде. Повторяющаяся группа цифр $a_{s+1}a_{s+2}\ \ldots a_{s+t}$ называется периодом, а сама дробь записывается в виде $\boldsymbol{a_0, a_1a_2\ \ldots a_s(a_{s+1}a_{s+2}\ \ldots a_{s+t})}$ (периодическую дробь условились записывать конечным числом цифр: выписывают цифры до периода, а затем в скобках записывают период; наличие скобок и указывает, что дробь является бесконечной периодической).

Другими словами, периодическая дробь – бесконечная десятичная дробь, в которой, начиная с некоторого десятичного знака, повторяется некоторая группа цифр (период). Минимальная повторяющаяся группа цифр после запятой в десятичной записи числа называется *периодом*, число цифр в периоде называется длиной периода, а бесконечная десятичная дробь, имеющая период, называется *периодической*.

Период периодической бесконечной десятичной дроби может быть сколько угодно большим.

Примеры. $\frac{1}{33} = 0,(03)$;
$\frac{1}{39} = 0,(025641)$;
$\frac{1}{51} = 0,(0196078431372549)$;
$\frac{1}{1150} = 0{,}00(0869565217391304347826)$.

Определение. Бесконечная периодическая десятичная дробь называется *чистой периодической,* если период начинается сразу после запятой, и *смешанной периодической,* если между целой частью и периодом находится группа цифр, предпериод (число цифр в предпериоде $s \geq 1$).

Примеры. $0{,}75$ – конечная десятичная дробь;
$0,(6)$- чистая периодическая десятичная дробь;
$0{,}8(3)$ смешанная периодическая десятичная дробь.

Теорема. Любое рациональное число может быть представлено в виде конечной десятичной дроби или бесконечной десятичной дроби — чистой периодической или смешанной периодической.

Любое иррациональное число есть непериодическая бесконечная десятичная дробь.

Теорема 1. Несократимая обыкновенная дробь $\frac{a}{b}$ обращается в *конечную десятичную дробь* (представима в виде конечной десятичной дроби) тогда и только тогда, когда в каноническое разложение её знаменателя входят лишь простые числа 2 и 5.

Следствие. Несократимая обыкновенная дробь $\frac{a}{b}$ обращается в бесконечную десятичную дробь тогда и только тогда, когда каноническое разложение её знаменателя содержит хотя бы одно простое число, отличное от 2 и 5.

Теорема 2. Несократимая обыкновенная дробь $\frac{a}{b}$, знаменатель которой взаимно прост с 10, обращается в *чистую периодическую дробь*, длина периода которой равна $P_b(10)$ (порядку 10 по модулю b).

Теорема 3. Пусть $\frac{a}{b}$ – несократимая обыкновенная дробь, $b = 2^{\alpha}5^{\beta}b_1$, где α, β – целые неотрицательные числа, хотя бы одно из которых отлично от нуля, НОД $(b_1, 10) = 1$, $b_1 \neq 1$ (т.е. в каноническое разложение b входит 2 или 5, а также хотя бы одно число, отличное от 2 и 5). Тогда $\frac{a}{b}$ обращается в *смешанную периодическую дробь*, у которой длина предпериода $t = \max\{\alpha, \beta\}$, а длина периода равна $P_{b_1}(10)$.

Примеры. $\frac{3}{4} = 0{,}75$ – конечная десятичная дробь;

$\frac{2}{3}$=0,(6)- чистая периодическая десятичная дробь;

$\frac{5}{6} = 0{,}8(3)$ смешанная периодическая десятичная дробь.

Рассмотрим *обратную задачу:* найти обыкновенную дробь, равную данной периодической десятичной дроби ***(обращение периодической дроби в обыкновенную).***

Правило 1. Чтобы записать *чистую периодическую дробь* в виде обыкновенной, нужно период дроби записать в числителе, а в знаменателе записать столько девяток, сколько цифр в периоде.

Примеры. $0,(8) = \frac{8}{9}$; $0,(123) = \frac{123}{999} = \frac{41}{333}$.

Правило 2. Чтобы записать *смешанную периодическую дробь* в виде обыкновенной, нужно от числа, записанного десятичными знаками до второго периода, отнять число, записанное десятичными знаками до первого периода, и записать полученную разность в числителе. В знаменателе же записать столько девяток, сколько цифр в периоде (длина периода) и столько нулей, сколько цифр в предпериоде.

Примеры. $0{,}11(7) = \frac{117-11}{900} = \frac{106}{900} = \frac{53}{450}$; $2{,}154(31) = \frac{215431-2154}{99000} = \frac{213277}{99000}$.

Рассмотрим применение теории сравнений к выводу некоторых признаков делимости.

Любое натуральное число a в десятичной системе счисления можно записать в виде: $a = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, где $0 \le a_i \le 9$ (цифры числа a, причём $a_k \neq 0$). Обозначим через r_i – абсолютно наименьший *вычет* числа 10^i по некоторому фиксированному модулю m. Составим число $\boldsymbol{R_m = a_k r_k + a_{k-1} r_{k-1} + \cdots + a_1 r_1 + a_0}$**.** Тогда, по свойству сравнений: $a \equiv R_m \,(mod\, m)$. Это сравнение и выражает общий *признак делимости Паскаля* (другое название: признак равноостаточности Паскаля).

Теорема (*общий признак делимости Паскаля*). Натуральное число a делится на натуральное число m тогда и только тогда, когда $R_m \vdots m$.

Другими словами, остатки от деления на m у чисел a и R_m совпадают (поэтому другое название признака: *признак равноостаточности Паскаля*).

Из общего признака делимости Паскаля следуют различные частные признаки делимости (для отдельных значений a). Рассмотрим некоторые из них, наиболее часто используемые на практике.

Примеры.

Признак делимости на $\mathbf{2}$ $(m = 2)$.

$10 \equiv 0 \,(mod\, 2)$, $10^i \equiv 0 \,(mod\, 2)$, $1 \le i \le k$. Поэтому $r_i = 0$, $1 \le i \le k$, и $R_2 = a_0$. Следовательно, согласно теореме, натуральное число $a = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$ $(0 \le a_i \le 9)$ делится на 2 тогда и только тогда, когда a_0 делится на 2, т.е. натуральное число a делится на 2 тогда и только тогда, когда его последняя цифра a_0 делится на 2 (последняя цифра чётная): $\boldsymbol{a \vdots 2 \Leftrightarrow a_0 \vdots 2.}$

Признак делимости на $\mathbf{3}$ $(m = 3)$.

$R_3 = a_k + a_{k-1} + \cdots \ldots + a_0$, так как $10^i \equiv 1 \,(mod\, 3)$, $1 \le i \le k$. Следовательно, согласно теореме, $\boldsymbol{a \vdots 3 \Leftrightarrow (a_k + a_{k-1} + \ \ldots + a_0) \vdots 3}$ (сумма его цифр делится на 3).

Признак делимости на $\mathbf{9}$ $(m = 9)$.

$R_9 = a_k + a_{k-1} + \ \ldots + a_0$, так как $10^i \equiv 1 \,(mod\, 9)$, $1 \le i \le k$. Следовательно, согласно теореме, $\boldsymbol{a \vdots 9 \Leftrightarrow (a_k + a_{k-1} + \ \ldots + a_0) \vdots 9}$ (сумма его цифр делится на 9).

Признак делимости на $\mathbf{11}$ ($m = 11$).

$R_{11} = (-1)^k a_k + (-1)^{k-1} a_{k-1} + \ ... \ + a_2 - a_1 + a_0$, так как $10^i \equiv -1 \ (mod \ 11)$, если i – нечётное; $10^i \equiv -1 \ (mod \ 11)$, если i – чётное, $1 \leq i \leq k$. Следовательно, согласно теореме, $\boldsymbol{a \vdots 11} \Leftrightarrow (\boldsymbol{(-1)^k a_k + (-1)^{k-1} a_{k-1} + \ ... \ + a_2 - a_1 + a_0}) \vdots \boldsymbol{11}$ (разность между суммой цифр, стоящих на чётных местах и суммой цифр, стоящих на нечётных местах, делится на 11.

Теорема (*признак делимости на составное число*). Если $\text{НОД}(a, b) = 1$ (взаимно просты), то число $n \vdots ab$ тогда и только тогда, когда $n \vdots a$ и $n \vdots b$.