6.1. Основные понятия и определения

Приведем некоторые определения и свойства целых чисел, которые потребуются для формулировки двух главных теорем теории чисел.

6.1.1. Делимость целых чисел

Что общего между числами множества 9, 16, 23, 30, 37, 44 кроме того, что они все целые? Казалось бы ничего. Однако, если ввести операцию деления с остатком и интересоваться только целым положительным остатком от деления чисел этого множества на 7, то окажется, что все они будут иметь одинаковый остаток, равный 2. Эти числа эквивалентны по этому свойству. Тогда приведенную последовательность можно продолжить дальше: 51, 58, 65, 72, 79... Это множество чисел является бесконечным и счетным, все числа множества объединяет одно общее свойство: при делении на 7 они дают целый положительный остаток 2. Говорят, что эти числа a сравнимы по модулю 7. Такое свойство множества обозначают $a \equiv 2 \bmod 7$.

Можно рассмотреть другое множество чисел, например 3, 12, 21, 30, 39, 49,..., и убедиться в том, что при делении на число 9 все они дают остаток 3, т. е. общее свойство чисел a этого множества можно записать так: $a \equiv 3 \bmod 9$.

Произвольное целое число a единственным образом может быть представлено в виде $a = mt + r$, где $m > 0$ – целое положительное число (делитель), t – частное, r – остаток ($0 \le r < m$). Так, например, если $a = 17$, $m = 5$, то $17 = 5 \cdot 3 + 2$.

В дальнейшем мы будем использовать операцию деления и интересоваться только остатком, не обращая внимание на частное. Так, например, число 16 при делении на 11 дает остаток 5.

Наименьший положительный остаток от деления некоторого числа a на число m обычно называют наименьшим неотрицательным вычетом a по модулю m. Если m делит a нацело, то остаток $r = 0$. Например, наименьший неотрицательный вычет при делении числа 18 на 6 равен 0.

Пусть имеется два числа a и b. Будем говорить, что они сравнимы по модулю m, если при делении на m они дают одинаковый целый положительный остаток. Например, числа 8 и 15 при делении на 7 имеют одинаковый остаток 1, т. е. они сравнимы по модулю 7. Сравнение чисел будем обозначать так: $a \equiv b \bmod m$.

Сравнению $a \equiv 0 \bmod m$ удовлетворяют все числа a, которые делятся на m нацело или, как говорят, кратные m.

6.1.2. Свойства сравнений

От сравнения $a \equiv b \bmod m$ можно перейти к равенству. Сравнение $a \equiv b \bmod m$ справедливо, если выполняется следующее равенство: $a = b + m \cdot t$, где $\cdot$ – умножение, t – некоторое целое (положительное, отрицательное или 0).

Такая связь между сравнениями и равенствами позволяет распространить понятие сравнения не только на положительные, но и на отрицательные числа. Например, можем записать $12 \equiv 7 \equiv 2 \equiv -3 \equiv -8 \equiv -13 \ldots \bmod 5$.

Из связи между сравнениями и равенствами следуют правила эквивалентных преобразований сравнений.

a) Если $a \equiv b \bmod m$ и $b \equiv c \bmod m$, то $a \equiv c \bmod m$.

b) Если $a \equiv b \bmod m$ и $c \equiv d \bmod m$, то $a+b \equiv c+d \bmod m$. Это правило можно сформулировать и так: сравнения по одинаковому модулю можно почленно складывать.

c) Если $a \equiv b \bmod m$, то $a \equiv b+m \cdot t \bmod m$, так как справедливо сравнение $m \cdot t \equiv 0 \bmod m$, т. е. к любой части сравнения можно прибавить модуль, умноженный на любое целое.

d) Если $a \equiv b \bmod m$ и c – любое целое, взаимно простое с m, то $a \cdot c \equiv b \cdot c \bmod m$, т. е. обе части сравнения можно умножить на любое целое, если оно взаимно простое с модулем m.

e) Если $a \equiv b \bmod m$ и c – любое целое, взаимно простое с m, то $a/c \equiv b/c \bmod m$, т. е. обе части сравнения можно разделить на любое целое, если оно взаимно простое с модулем m.

Последнее свойство позволяет распространить понятия сравнения и на дробные числа. Так, например, если имеем сравнение $1/3 \equiv 16/15 \bmod 11$, то так как (15, 11) = 1, т. е. числа 15 и 11 взаимно просты, то обе части сравнения можно умножить на 15, и получим эквивалентное сравнение: $5 \equiv 16 \bmod 11$.

6.1.3. Решение сравнений

Из приведенных правил эквивалентных преобразований сравнений следуют общие приемы решения сравнений. Пусть требуется решить сравнение $27 - 13 \cdot 5 \equiv 10 \cdot X \bmod 7$ относительно неизвестного X. Можно показать, что если в сравнении имеется арифметическое выражение, то любой член его можно заменить остатком от деления на модуль (в общем случае – на любое сравнимое с ним число). Так как $27 \equiv 6 \bmod 7$, $13 \equiv -1 \bmod 7$ и $10 \equiv 3 \bmod 7$, то исходное сравнение можно представить в виде $6 - (-1) \cdot 5 \equiv 3 \cdot X \bmod 7$.

Далее вычисляем $11 \equiv 3 \cdot X \bmod 7$, $18 \equiv 3 \cdot X \bmod 7$, $6 \equiv X \bmod 7$, откуда одно из решений сравнения – $X = 6$. Общее решение $X = 6 + t \cdot 7$.

Упражнения.

Найти общие решения следующих сравнений:

a) $8 \equiv 3X \bmod 11$;

b) $25 \equiv 15\ X \bmod 17$;

c) $3(24-18)/5 \equiv 7X \bmod 19$;

d) $8^{125} - 6^{29} \equiv 5X \bmod 7$;

e) $$\frac{(75 \cdot 1824 + 33 \cdot 2083)}{37 \cdot 21^6} \equiv 23^3\, X \bmod 19;$$

f) $$\frac{36 \cdot 10^{112} + 81 \cdot 12^{58}}{41 \cdot 9^{10}} \equiv 21^6 X \bmod 11.$$

6.1.4. Наименьшее общее кратное и наибольший общий делитель

Пусть имеется n целых чисел: $a_1, a_2, a_3, \ldots, a_n$. Общим кратным этих чисел называется целое число, которое делится нацело на каждое из этих чисел. Наименьшее из этих общих кратных называется наименьшим общим кратным чисел $a_1, a_2, a_3, \ldots, a_n$ и обозначается НОК ($a_1, a_2, a_3, \ldots, a_n$) или $[a_1, a_2, a_3, \ldots, a_n]$.

Пусть имеется n целых чисел $a_1, a_2, a_3, \ldots, a_n$. Общим делителем этих чисел называется число, которое нацело делит каждое их этих чисел. Сре-

ди делителей имеется наибольшее число, которое называется наибольшим общим делителем – НОД $(a_1, a_2, a_3, ..., a_n)$ или $(a_1, a_2, a_3, ..., a_n)$.

6.1.5. Простые числа. Разложение на простые сомножители. Каноническая форма числа

Число, которое не имеет никаких делителей, кроме 1 и самого себя, называется простым числом. Примеры простых чисел: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

Любое число N может быть представлено в виде произведения степеней простых чисел (каноническое представление числа). Такое представление единственно (с точностью до перестановки сомножителей). Так, число $600 = 2^3 3^1 5^2$.

Для представления числа N в канонической форме можно использовать следующий алгоритм. Число N делим на наименьшее простое число 2 до тех пор, пока оно делится нацело, затем на 3, на 5 и т. д.

Например, $N = 10500$. $10500 : 2 = 5250$; $5250 : 2 = 2625$. Это число больше не делится на 2 нацело. Делим его на 3. $2625 : 3 = 875$. Это число на 3 нацело не делится. Делим его на 5. $875 : 5 = 175$. Еще раз делим на 5. $175 : 5 = 35$. Еще раз делим на 5. $35 : 5 = 7$. Число 7 – простое число, поэтому окончательно имеем в канонической форме: $10\,500 = 2^2 3^1 5^3 7^1$.

6.1.6. Определение НОК И НОД чисел

Для произвольного целого числа a и произвольного целого положительного числа b существуют такие числа t и r, что $a = bt + r$, где $0 \le r < b$. Причем такое представление единственное.

Можно показать, что если $b|a$ (b делит a нацело), то $(a, b) = b$, и если $a = bt + r$, то $(a, b) = (b, r)$.

Для нахождения наибольшего общего делителя двух чисел a и b известен алгоритм Евклида: пусть $a \ge b$. Рассмотрим следующую последовательность равенств:

$$a = bt_1 + r_2,\ 0 < r_2 < b;$$
$$b = r_2 t_2 + r_3,\ 0 < r_3 < r_2;$$
$$r_2 = r_3 t_3 + r_4,\ 0 < r_4 < r_3 \ ...$$
$$r_{n-1} = r_n t_n + r_{n+1},\ 0 = r_{n+1}.$$

Поскольку $a \ge b > r_2 > r_3 > ... \ge 0$, то алгоритм имеет конечное число шагов. Согласно вышеприведенным свойствам, $(a, b) = (b, r_2) = (r_2, r_3) = ... = r_n$. Таким образом, наибольший общий делитель чисел a и b равен последнему ненулевому остатку в последовательности равенств, т. е. r_n. А наименьшее общее кратное a и b равно $[a, b] = ab/(a, b)$.

Упражнения.

Используя алгоритм Евклида, найти НОК и НОД чисел:

а) 575 и 155;

β) 840 и 188650;

с) 4851 и 29106;

d) 975 и 616.

Если два числа N_1 и N_2 представлены в канонической форме соответственно: $N_1 = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$, $N_2 = p_1^{m_1} p_2^{m_2} \dots p_s^{m_s}$, то

$$\text{НОК}\left(N_1, N_2\right) = p_1^{\min(n_1, m_1)} p_2^{\min(n_2, m_2)} p_s^{\min(n_s, m_s)};$$

$$\text{НОД}\ \left(N_1, N_2\right) = p_1^{\min(n_1, m_1)} p_2^{\min(n_2, m_2)} p_s^{\min(n_s, m_s)}.$$

Если в каноническом представлении одного из чисел отсутствует какой-либо простой сомножитель, его можно ввести в нулевой степени. Например, для чисел $N_1 = 2^3 5^2 7^1$ и $N_2 = 3^1 5^1 11^2$, прежде чем находить НОК и НОД, требуется их привести к одинаковой форме, т. е. сделать так, чтобы в каноническом представлении обоих чисел присутствовали бы одинаковые простые числа в соответствующих степенях, а именно: $N_1 = 2^3 3^0 5^2 7^1 11^0$; $N_2 = 2^0 3^1 5^1 7^0 11^2$. Тогда НОК ($N_1$, N_2) = $= 2^3 3^1 5^2 7^1 11^2 = 508200$, НОД ($N_1$, N_2) = $2^0 3^0 5^1 7^0 11^0 = 5$.

Упражнения.

Найти НОК и НОД для пар чисел:

а) $N_1 = 440$; $N_2 = 6050$;

β) $N_1 = 234$; $N_2 = 4125$;

с) $N_1 = 66550$; $N_2 = 40131$;

d) $N_1 = 388$; $N_2 = 1647$.

Приведенный алгоритм легко обобщается на произвольное количество чисел, для которых требуется определить НОК и НОД.

Упражнения.

Найти НОК и НОД для следующих наборов чисел:

а) $N_1 = 60$; $N_2 = 350$; $N_3 = 495$;

β) $N_1 = 265$; $N_2 = 104$; $N_3 = 93$;

с) $N_1 = 2100$; $N_2 = 630$; $N_3 = 5880$; $N_4 = 9450$;

d) $N_1 = 700$; $N_2 = 495$; $N_3 = 104$;

е) $N_1 = 103$; $N_2 = 260$; $N_3 = 121$.

6.1.7. Функция Эйлера для натурального числа φ(m)

Функция Эйлера $\varphi(m)$ определяется для всех целых чисел m как количество чисел ряда 1, 2, 3, ..., m взаимно простых с m. Так, $\varphi(1) = 1$ (по определению), $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$ и т. д. Легко показать, что для $m = p$ (простых чисел) $\varphi(p) = p-1$. Для $m = p^n$ функция

Эйлера $\varphi(p^n) = p^{n-1}(p-1)$. Для произвольного числа m, представленного в канонической форме $m = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$, функция Эйлера определяется следующим образом: $\varphi(m) = m(1-1/p_1)(1-1/p_2)\dots(1-1/p_s)$.

Например: $\varphi(11) = 10$; $\varphi(9) = 6$; $\varphi(18) = 6$.

Упражнения.

Вычислить функцию Эйлера $\varphi(m)$ для чисел m = 7, 12, 15, 17, 23, 24, 25, 28, 37, 54, 64.

6.1.8. Сравнимость чисел и классы вычетов

Выпишем все числа от 1 до 8 и вычеркнем все числа не взаимно простые с 8. Количество оставшихся чисел равно $\varphi(m = 8) = 4$, а сами эти числа (1, 3, 5, 7). Множество этих чисел обладает свойством замкнутости относительно операции умножения по модулю $m = 8$. Действительно, перемножая любые пары чисел из множества (1, 3, 5, 7) и находя наименьший положительный остаток по модулю $m = 8$, будем получать всегда одно из этих же чисел. Каждое из этих чисел порождает бесконечный счетный класс чисел: $1+8\cdot t$; $3+8\cdot t$; $5+8\cdot t$; $7+8\cdot t$, где t – любое целое.

Более того, множество классов с порождающими элементами в виде этих чисел обладает свойством замкнутости, а именно: при любых целых t произведение представителей классов ($1+8\cdot t$; $3+8\cdot t$; $5+8\cdot t$; $7+8\cdot t$) дает в результате представителя одного из этих же классов.

Можно показать, что классы вычетов, получаемые в соответствии с функцией Эйлера, всегда образуют абелеву группу по умножению. А это, в частности, означает, что для любого представителя из этих классов можно найти обратный элемент из представителей этих же классов.

Упражнения.

Постройте абелевы группы классов, порождаемые числами 10, 12, 15, 18, 21, 24, 25, 27, 28.

6.1.9. Теоремы Ферма и Эйлера

Теорема Ферма.

Существует мнение, что Ферма не публиковал свои научные труды, а формулировал свои знаменитые теоремы либо в письмах к знакомым математикам, либо на полях рукописей. Так, на полях одной из рукописей Ферма написал, что если p – простое число и $(a, p) = 1$, то $a^{p-1} \equiv 1 \bmod p$.

Пусть $p = 23$, $a = 18$. Очевидно, что (23, 18) = 1, следовательно, $18^{22} \equiv 1 \bmod 23$. Проверить этот результат несложно. Для этого заметим, что $18 \equiv -5 \bmod 23$, поэтому можно написать эквивалентное сравнение: $(-5)^{22} \equiv 1 \bmod 23$ или $5^{22} \equiv 1 \bmod 23$. Последнее сравнение можно представить в виде $(5^2)^{11} \equiv 1 \bmod 23$, и так как $25 \equiv 2 \bmod 23$, то

$2^{11} \equiv 1 \bmod 23$. Полученное сравнение элементарно проверяется: $2048 \equiv 1 \bmod 23$.

Теорема Эйлера.

Если $m > 1$ и $(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \bmod m$. Эта теорема обобщает теорему Ферма, так как при $m = p$, $\varphi(m = p) = p - 1$.

Пусть $m = 18$, $a = 5$. Очевидно, что $(5, 18) = 1$.

Функция Эйлера $\varphi(m = 18) = 6$. Поэтому $5^6 \equiv 1 \bmod 18$. Это сравнение проверяется достаточно просто: $5^2 \equiv 7 \bmod 18$, следовательно, $((5^2))^3 \equiv 7^3 = 343 \equiv 1 \bmod 18$.

Упражнения.

На основании теорем Ферма и Эйлера доказать справедливость сравнений:

a) $2^{36} \equiv 3^{36} \equiv \ldots \equiv 36^{36} \equiv 1 \bmod 37$;

b) $2^{100} \equiv 3^{100} \equiv \ldots \equiv 100^{100} \equiv 1 \bmod 101$;

c) $2^8 \equiv 4^8 \equiv 7^8 \equiv 8^8 \equiv 11^8 \equiv 13^8 \equiv 14^8 \equiv 1 \bmod 15$.

6.1.10. Показатели чисел по модулю и примитивные корни

Пусть $(a, m) = 1$. Рассмотрим бесконечную последовательность степеней числа a: $a^0 = 1$, a^1, a^2, a^3, ... В соответствии с теоремой Эйлера существует целое положительное число s, такое, что

$$a^s \equiv 1 \bmod m. \qquad (6.1)$$

В самой теореме $s = \varphi(m)$. Могут существовать и другие целые положительные числа s, удовлетворяющие этому сравнению. Наименьшее из них обозначается $\boldsymbol{e}$ и называется показателем числа a по модулю m. Иногда $\boldsymbol{e}$ называют порядком числа a по модулю m.

Набор степеней числа a вида a^0, a^1, a^2, a^3, ..., a^{e-1} попарно несравнимы между собой по модулю m. Докажем это. Пусть, например, при некоторых n_1 и n_2 выполняется сравнение $a^{n_1} \equiv a^{n_2} \bmod m$, где для определенности $n_1 < n_2 < \boldsymbol{e}$. Умножим обе части сравнения на a^{e-n_2}, тогда получим $a^{(e+n_1-n_2)} \equiv 1 \bmod m$. Но поскольку $n_1 < n_2$, то в левой части сравнения степень числа a меньше $\boldsymbol{e}$, что противоречит тому, что $\boldsymbol{e}$ – наименьшее число, удовлетворяющее сравнению (6.1). Если найдется некоторое k, такое, что $a^k \equiv 1 \bmod m$, то $\boldsymbol{e}$ является делителем k. Очевидно, что всегда e является делителем $\varphi(m)$.

Пример.

Возьмем $m = 45$, $a = 2$, $(45, 2) = 1$. Функция Эйлера $\varphi(45) = 24$, следовательно, $2^{24} \equiv 1 \bmod 45$. Число 24 представляется в канонической форме в виде $24 = 2^3 3$, т. е. имеет 8 разных делителей: 1, 2, 3, 4, 6, 8, 12, 24. Проверка показывает, что наименьшее число $e = 12$, так как $2^{12} \equiv 1 \bmod 45$.

Если показатель $\boldsymbol{e}$ числа a по модулю m равен $\varphi(m)$, то a называют примитивным элементом по модулю m.

Пример. По каким модулям число $a = 2$ является примитивным элементом? $m = \mathbf{3}, \mathbf{5}, 7, \mathbf{9}, \mathbf{11}, 15, 17, \mathbf{19}$.