Глава I. Теория чисел

1. Теория делимости

Кольцо целых чисел. На множестве всех целых чисел $\mathbb{Z}$ определены две бинарные алгебраические операции – сложение и умножение. Как хорошо известно из школьного курса, эти операции обладают следующими свойствами:

(1) $a+(b+c)=(a+b)+c$ для любых $a,b,c\in\mathbb{Z}$ (ассоциативность сложения);
(2) $a+b=b+a$ для любых $a,b\in\mathbb{Z}$ (коммутативность сложения);
(3) существует такой элемент $0\in\mathbb{Z}$, что $0+a=a$ для любого $a\in\mathbb{Z}$;
(4) для любого $a\in\mathbb{Z}$ существует такой элемент $-a\in\mathbb{Z}$, что $a+(-a)=0$;
(5) $a(bc)=(ab)c$ для любых $a,b,c\in\mathbb{Z}$ (ассоциативность умножения);
(6) $ab=ba$ для любых $a,b\in\mathbb{Z}$ (коммутативность умножения);
(7) существует такой элемент $1\in\mathbb{Z}$, что $1\cdot a=a\cdot 1=a$ для любого $a\in\mathbb{Z}$;
(8) $a(b+c)=ab+ac$, $(a+b)c=ac+bc$ для любых $a,b,c\in\mathbb{Z}$ (дистрибутивность умножения относительно сложения).

Множество A, на котором заданы две бинарные операции – сложение и умножение, удовлетворяющие условиям $(1)-(4)$ и (8), называется кольцом. Кольцо A называется ассоциативным, если выполняется аксиома (5), коммутативным, если выполняется аксиома (6), кольцом с единицей, если выполняется аксиома (7). Таким образом, множество целых чисел $\mathbb{Z}$ – коммутативное ассоциативное кольцо с единицей. Обычно единица кольца обозначается цифрой 1; однако, иногда приходится указывать, единицей какого именно кольца A она является, и тогда мы используем обозначение 1_A.

Завершим этот пункт несколькими замечаниями об аксиомах кольца. Аксиомы (1)-(4) означают в точности, что относительно операции сложения кольцо является абелевой группой. Далее, в аксиому (8) включены два соотношения дистрибутивности, потому что кольцо не обязано быть коммутативным, а в некоммутативном кольце левая дистрибутивность не обязательно влечет правую дистрибутивность (правда, я затрудняюсь, какое из соотношений $a(b+c)=ab+ac$, $(a+b)c=ac+bc$ назвать левой, а какое правой дистрибутивностью). То же самое относится и к аксиоме (7): левая единица некоммутативного кольца не обязана быть правой единицей.

Области целостности. Конечно, свойства кольца целых чисел $\mathbb{Z}$ не ограничиваются только тем, что $\mathbb{Z}$ – коммутативное ассоциативное кольцо с 1. Отметим еще одно важное свойство: если произведение двух целых чисел равно 0, то хотя бы один из сомножителей равен 0. Поэтому естественно рассматривать класс колец, обладающих еще и этим свойством. Пусть A – коммутативное ассоциативное кольцо с 1; A называется кольцом без делителей 0 или, короче, областью целостности, если произведение двух элементов $a,b\in A$ может быть равным 0 только если хотя бы один из сомножителей равен 0. Иначе говоря, если A – область целостности, $a,b\in A$ и $ab=0$, то $a=0$ или $b=0$. Кольцо целых чисел $\mathbb{Z}$ – пример области целостности.

Важнейшим свойством областей целостности является возможность сокращения равенств на ненулевой множитель.

Предложение 1. *Пусть A – область целостности. Если $a,b,c\in A$, $ab=ac$ и $a\neq 0$, то $b=c$.*

Доказательство. Если $ab=ac$, то $a(b-c)=0$. Первый сомножитель a в этом произведении отличен от 0; поскольку A – область целостности, нулю равен второй сомножитель $b-c$. Итак, $b-c=0$, т.е. $b=c$.

Делимость. Хотя в этой главе мы будем иметь в виду только кольцо целых чисел, многие понятия и факты основаны лишь на том, что $\mathbb{Z}$ – коммутативное ассоциативное кольцо с 1, и лишь иногда нам потребуется еще, что $\mathbb{Z}$ – область целостности. Поэтому мы и будем их формулировать в этой более общей ситуации; это позволит в следующей главе применить результаты к другому коммутативному ассоциативному кольцу с 1 – кольцу многочленов.

Всюду дальше A – коммутативное ассоциативное кольцо с 1. Пусть $a, b \in A$; мы говорим, что a делится на b и пишем $a \div b$ (или иногда $b \mid a$), если существует такой элемент $c \in A$, что $a = bc$. В следующем предложении собраны основные свойства делимости.

Предложение 2. (1) $0 \div c$ *для всякого элемента* $c \in A$;

(2) *если* $a, b, c \in A$, $a \div c$, $b \div c$, *то* $(a \pm b) \div c$;
(3) *если* $a, x, c \in A$, $a \div c$, *то* $ax \div c$;
(4) $a \div 1$ *и* $a \div a$ *для любого* $a \in A$;
(5) *если* $a \in A$ *и* $a \div 0$, *то* $a = 0$;
(6) *если* $a, b, c \in A$, $a \div b$, $b \div c$, *то* $a \div c$.

Доказательство. (1). $0 = c \cdot 0$. (4). $a = 1 \cdot a$.

(2). Если $a \div c$, $b \div c$, то существуют $u, v \in A$, такие что $a = cu$, $b = cv$. Тогда $(a \pm b) = cu \pm cv = c(u \pm v)$; поскольку $u \pm v \in A$, это и значит, что $(a \pm b) \div c$.

(3). Если $a \div c$, $x \in A$, то существует элемент $u \in A$, такой что $a = cu$. Тогда $ax = (cu)x = c(ux)$; поскольку $ux \in A$, это и значит, что $ax \div c$.

(5). Если $a \div 0$, , то существует элемент $u \in A$, такой что $a = 0 \cdot u$. Итак, $a = 0 \cdot u = 0$.

(6). Если $a \div b$, $b \div c$, то существуют $u, v \in A$, такие что $a = bu$, $b = cv$. Тогда $a = (cv)u = c(vu)$; поскольку $vu \in A$, это и значит, что $a \div c$.

Сравнения. С понятием делимости тесно связано понятие сравнения по модулю. Пусть A – коммутативное ассоциативное кольцо с 1, и пусть $n \in A$. Мы говорим, что элементы $a, b \in A$ сравнимы по модулю n и пишем $a \equiv b \pmod{n}$, если $(a - b) \div n$.

Предложение 3. *Пусть* A *– коммутативное ассоциативное кольцо с 1, и пусть* $n \in A$.

(1) $a \equiv a \pmod{n}$ *для всякого* $a \in A$ *(рефлексивность сравнения);*
(2) *если* $a, b \in A$ *и* $a \equiv b \pmod{n}$, *то* $b \equiv a \pmod{n}$ *(симметричность сравнения);*
(3) *если* $a, b, c \in A$ *и* $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$, *то* $a \equiv c \pmod{n}$ *(транзитивность сравнения);*
(4) *если* $a, b, c, d \in A$ *и* $a \equiv c \pmod{n}$, $b \equiv d \pmod{n}$, *то* $(a \pm b) \equiv (c \pm d) \pmod{n}$, $ab \equiv cd \pmod{n}$;
(5) *если* $a, b, m \in A$ *и* $a \equiv b \pmod{n}$, *то* $am \equiv bm \pmod{nm}$;
(6) *если* A *– область целостности,* $a, b, m \in A$, $m \neq 0$ *и* $am \equiv bm \pmod{nm}$, *то* $a \equiv b \pmod{n}$
(7) *если* $a, b \in A$, $a \equiv b \pmod{n}$ *и* $n \div m$, *то* $a \equiv b \pmod{m}$.

Доказательство. (1) $a - a = 0 \div n$, а это и значит, что $a \equiv a \pmod{n}$.

(2) Если $a \equiv b \pmod{n}$, то $(a - b) \div n$; но тогда $(b - a) = (-1)(a - b) \div n$, т.е. $b \equiv a \pmod{n}$.

(3) Если $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$, то $(a - b) \div n$, $(b - c) \div n$; но тогда и $(a - c) = (a - b) + (b - c) \div n$, т.е. $a \equiv c \pmod{n}$.

(4) Если $a \equiv c \pmod{n}$, $b \equiv d \pmod{n}$, то $(a - c) \div n$, $(b - d) \div n$, и потому

$$(a \pm b) - (c \pm d) = (a - c) \pm (b - d) \div n,$$
$$ab - cd = ab - cb + cb - cd = (a - c)b + c(b - d) \div n,$$

а это и значит, что $(a \pm b) \equiv (c \pm d) \pmod{n}$, $ab \equiv cd \pmod{n}$.

(5) Если $a \equiv b \pmod{n}$, то $(a-b) \div n$, и существует элемент $c \in A$, такой что $a - b = nc$; но тогда $am - bm = (a-b)m = nmc \div nm$, т.е. $am \equiv bm \pmod{nm}$.

(6) Если $am \equiv bm \pmod{nm}$, то $am - bm \div nm$, и существует элемент $c \in A$, такой что $a-b)m = am-bm = ncm$. Но A – область целостности, и поэтому можно сократить обе части последнего равенства на элемент $m \neq 0$; тогда получаем, что $a - b = nc \div n$, т.е. $a \equiv b \pmod{n}$.

(7) Если $a \equiv b \pmod{n}$, то $(a-b) \div n$; если к тому же $n \div m$, то $(a-b) \div m$, и $a \equiv b \pmod{m}$

Ассоциированные элементы. Элементы $a, b \in A$ называются ассоциированными, если $a \div b$, $b \div a$. Для записи того, что a и b ассоциированы, мы применяем обозначение $a \sim b$.

Предложение 4. (1) *$a \sim a$ для всякого элемента $a \in A$;*

(2) *если $a, b \in A$, $a \sim b$, то $b \sim a$;*
(3) *если $a, b, c \in A$, $a \sim b$, $b \sim c$, то $a \sim c$;*
(4) *если $a \sim a'$, $b \sim b'$, $a \div b$, то $a' \div b'$;*
(5) *если $a \in A$ и $a \sim 0$, то $a = 0$.*

Доказательство. Все утверждения очевидным образом следуют из соответствующих утверждений предложения 1.

В кольце целых чисел $\mathbb{Z}$ числа a, b ассоциированы тогда и только тогда, когда $a = \pm b$. Отметим, что для каждого числа $a \in \mathbb{Z}$ найдется единственное ассоциированное с ним неотрицательное число.

Делители 1. Элемент $\varepsilon \in A$ называется делителем 1, или обратимым элементом кольца A, если $1 \div \varepsilon$. Поскольку ε, как и любой элемент из A, делится на 1, мы заключаем, что делитель единицы – это то же самое, что элемент, ассоциированный с 1. В кольце $\mathbb{Z}$ единственными делителями 1 являются числа 1 и -1; в других кольцах делителей 1 может быть больше.

Если ε – делитель 1, то существует элемент $x \in A$, такой что $1 = \varepsilon x$. Он единствен: если $1 = \varepsilon y$, то $y = y \cdot 1 = y(\varepsilon x) = (y\varepsilon)x = 1 \cdot x = x$. Единственный элемент x, такой что $1 = \varepsilon x$, называется обратным к ε элементом и обозначается ε^{-1}. Отсюда происходит второе название делителей единицы – обратимые элементы, т.е. такие элементы, для которых есть обратный элемент.

Предложение 5. (1) *1 – делитель 1;*

(2) *если ε, δ – делители 1, то $\varepsilon\delta$ – делитель 1, причем $(\varepsilon\delta)^{-1} = \varepsilon^{-1}\delta^{-1}$;*
(3) *если ε – делитель 1, то ε^{-1} – тоже делитель 1, причем $(\varepsilon^{-1})^{-1} = \varepsilon$;*
(4) *если a – любой элемент из A, а ε – делитель 1, то $a \sim a\varepsilon$;*
(5) *обратно, если A – область целостности, и элементы $a, b \in A$ ассоциированы, то существуют такие делители 1 ε, δ, что $a = b\varepsilon$, $b = a\delta$.*

Доказательство. Утверждение 1 очевидно. Если ε, δ – делители 1, то

$$1 = (\varepsilon\delta)(\varepsilon^{-1}\delta^{-1}) \div (\varepsilon\delta),$$

и $\varepsilon^{-1}\delta^{-1}$ – обратный к $\varepsilon\delta$ элемент. Точно так же, если ε – делитель 1, то $1 = \varepsilon^{-1}\varepsilon \div \varepsilon^{-1}$, и ε – обратный к ε^{-1} элемент. Пусть теперь ε – делитель 1 и $a \in A$; тогда $a\varepsilon \div a$, $a = a\varepsilon\varepsilon^{-1} \div a\varepsilon$, т.е. a и $a\varepsilon$ ассоциированы.

Наконец, докажем (5). Утверждение тривиально, если $a = 0$. Пусть $a \neq 0$, $a \sim b$; тогда $a \div b$, $b \div a$, а это значит, что существуют такие элементы $\varepsilon, \delta \in A$, что $a = b\varepsilon$, $b = a\delta$. Подставляя одно из этих равенств в другое, получаем: $a \cdot 1 = a = b\varepsilon = a\delta\varepsilon$. Сократив на $a \neq 0$ (а это возможно, потому что A – область целостности), получаем, что $1 = \delta\varepsilon$, т.е. что ε и δ – делители 1.

2. Идеалы и делимость

Идеалы кольца. Подмножество I коммутативного кольца с 1 называется идеалом кольца, если выполняются следующие три условия:

(1) $0 \in I$;
(2) если $a, b \in I$, то $a \pm b \in I$;
(3) если $a \in I$, а x – любой элемент из A, то $ax \in I$.

Замечание. *На самом деле идеалы определяются в произвольных кольцах, не обязательно коммутативных и с 1; однако, в общем случае определение идеала и некоторые утверждения об идеалах становятся чуть-чуть сложнее.*

Свойства делимости (1)-(3) из предложения 1.2 показывают, что для любого $c \in A$ множество всех элементов из A, делящихся на c, является идеалом кольца A. Немного усложнив этот пример, укажем еще одну конструкцию для построения идеалов.

Пусть $a_1, \ldots, a_n$ – произвольные элементы кольца A. Через $(a_1, \ldots, a_n)$ обозначим множество всех элементов вида $x_1a_1 + \cdots + x_na_n$, где коэффициенты $x_1, \ldots, x_n$ независимо друг от друга пробегают все кольцо A.

Предложение 1. *Для любых элементов $a_1, \ldots, a_n \in A$ множество $(a_1, \ldots, a_n)$ является идеалом кольца A.*

Доказательство. Надо проверить, что множество $(a_1, \ldots, a_n)$ удовлетворяет условиям (1)-(3) определения идеала.

(1). $0 = 0 \cdot a_1 + \cdots + 0 \cdot a_n \in (a_1, \ldots, a_n)$;

(2). Пусть $a = x_1a_1 + \cdots + x_na_n$, $b = y_1a_1 + \cdots + y_na_n$ – любые элементы из $(a_1, \ldots, a_n)$ (здесь $x_1, y_1, \ldots, x_n, y_n$ – какие-то элементы из A). Тогда

$$a \pm b = (x_1a_1 + \cdots + x_na_n) \pm (y_1a_1 + \cdots + y_na_n) = \\ = (x_1 \pm y_1)a_1 + \cdots + (x_n \pm y_n)a_n \in (a_1, \ldots, a_n).$$

(3). Пусть $a = x_1a_1 + \cdots + x_na_n \in (a_1, \ldots, a_n)$, и пусть $x \in A$. Тогда

$$ax = (x_1a_1 + \cdots + x_na_n)x = (x_1x)a_1 + \cdots + (x_nx)a_n \in (a_1, \ldots, a_n).$$

Предложение доказано.

Идеал $(a_1, \ldots, a_n)$ называется идеалом, порожденным элементами $a_1, \ldots, a_n \in A$. Идеал (c), порожденный единственным элементом $c \in A$, называется главным идеалом кольца A, порожденным c. Главный идеал (c) состоит из всех элементов вида cx, $x \in A$, т.е. из всех элементов кольца A, делящихся на c.

Основные определения теории делимости красиво формулируются в терминах идеалов. Например, $a \div b$ тогда и только тогда, когда $(a) \subseteq (b)$; $a \sim b$ тогда и только тогда, когда $(a) = (b)$; ε – делитель 1 тогда и только тогда, когда $(\varepsilon) = (1) = A$. Доказательства этих фактов очень просты, и мы их опускаем.

Отметим, что некоторые из доказанных выше свойств делимости, и так совершенно тривиальные, становятся еще нагляднее, если их переформулировать в терминах идеалов. Например, утверждение (6) предложения 1.2 о том, что если $a \div b$, $b \div c$, то $a \div c$, приобретает следующий вид: если $(a) \subseteq (b)$, $(b) \subseteq (c)$, то $(a) \subseteq (c)$.

3. Идеалы кольца целых чисел $\mathbb{Z}$

Аксиома индукции. Множество целых чисел не только является коммутативным ассоциативным кольцом с 1; мы еще можем сравнивать целые числа друг с другом. Если $a, b \in \mathbb{Z}$, то одно из чисел a, b не больше другого, т.е. выполняется одно из соотношений $a \leq b$ или $b \leq a$. При этом если $a \leq b$ и $b \leq a$, то $b = a$. Свойства

неравенств для целых чисел хорошо известны из школьного курса; поэтому мы не повторяем их здесь.

Целые числа, большие 0, называются натуральными числами; множество всех натуральных чисел обозначают через $\mathbb{N}$. Часто удобно присоединить к множеству натуральных чисел 0; для обозначения этого расширенного множества натуральных чисел, состоящего из всех неотрицательных целых чисел, используется символ $\mathbb{N}_0$. Напомним, что если $a \in \mathbb{Z}$, то ровно одно из чисел a, $-a$ принадлежит $\mathbb{N}_0$; оно называется абсолютной величиной, или модулем, числа a, и обозначается $|a|$. Свойства абсолютной величины тоже хорошо известны и не приводятся здесь.

Множество натуральных чисел обладает еще одним важным свойством, которое наглядно очевидно, но которое при строгом построении теории натуральных чисел приходится включать в число аксиом.

Аксиома индукции. *Всякое непустое подмножество множества $\mathbb{N}_0$ содержит наименьший элемент. Иначе говоря, если $X \subseteq \mathbb{N}_0$, $X \neq \emptyset$, то существует элемент $x_0 \in X$, такой что для всякого $x \in X$ будет $x_0 \leq x$.*

Следствие. *Если $X \subseteq \mathbb{N}_0$, причем некоторое число $a \in \mathbb{N}_0$ принадлежит X, и из того, что число $n \in \mathbb{N}_0$ принадлежит X следует, что $n+1 \in X$, то X содержит все числа, большие или равные a.*

Доказательство. Если это не так, то множество $Y = \{y \in \mathbb{N}_0 \,|\, y \geq a, y \notin X\}$ непусто. По аксиоме индукции, в Y есть наименьшее число y_0. При этом $y_0 \neq a$, так как по условию $a \in X$. Следовательно, $y_0 > a$, и потому $y_0 - 1 \geq a$. Значит, $y_0 - 1 \in X$, так как y_0 – наименьшее число, большее или равное a и не принадлежащее X. Но тогда по условию число $y_0 = (y_0 - 1) + 1$ принадлежит X. Мы пришли к противоречию, которое и доказывает наше утверждение.

Доказанное следствие лежит в основе метода доказательства, известного как метод математической индукции. Пусть $P(n)$ – некоторое утверждение, зависящее от параметра $n \in \mathbb{N}_0$. Предположим, что нам удалось доказать, что верно утверждение $P(a)$ (база индукции), и что из верности утверждения $P(n)$ следует верность утверждения $P(n+1)$ (индукционный переход). Тогда $P(n)$ верно для любого $n \geq a$. Действительно, множество тех $n \in \mathbb{N}_0$, для которых утверждение $P(n)$ верно, удовлетворяет требованиям предыдущего следствия.

Деление с остатком для целых чисел. Не всегда одно целое число можно разделить не другое, оставаясь в рамках кольца целых чисел. В какой-то степени неудобства, связанные с невозможностью деления, возмещаются наличием другой операции, называемой делением с остатком.

Теорема 1 (о делении с остатком). *Пусть $a, b \in \mathbb{Z}$, причем $b \neq 0$. Тогда существуют единственные целые числа q, r, такие что $a = bq + r$, $0 \leq r < |\,b\,|$. Число q называется неполным частным, а число r – остатком от деления a на b.*

Доказательство. Сначала докажем единственность. Пусть $a = bq + r = bq' + r'$, где $0 \leq r, r' < |\,b\,|$. Не умаляя общности, мы можем считать, что $r \leq r'$. Тогда $0 \leq r' - r \leq r' < |\,b\,|$ и $r' - r = b(q - q') \div |\,b\,|$; это возможно только тогда, когда $r' - r = 0$, т.е. $r' = r$. Но тогда $b(q - q') = r' - r = 0$, и, поскольку $b \neq 0$, получается, что $q - q' = 0$, т.е. $q - q'$.

Перейдем к доказательству существования неполного частного и остатка. Пусть сначала $a \geq 0$, $b > 0$. Рассмотрим множество Y чисел вида $a - bx$, где x пробегает множество $\mathbb{Z}$. Пересечение $Y \cap \mathbb{N}_0$ содержится в $\mathbb{N}_0$ и непусто, так как $a \in Y \cap \mathbb{N}_0$. Пусть r – наименьший элемент этого пересечения; поскольку $r \in Y$, существует $q \in \mathbb{Z}$, такое что $r = a - bq$. Если $r \geq b$, то элемент $r_1 = r - b = a - b(q+1)$

принадлежит Y; кроме того, $0 \le r_1 < r$, и потому $r_1 \in Y \cap \mathbb{N}_0$, причем $r_1 < r$, что противоречит минимальности r. Следовательно, $r < b$, и $a = bq + r$, $0 \le r < b$.

Теперь положим, что $a < 0$, $b > 0$; тогда $-a > 0$, и по уже доказанному существуют $q', r' \in \mathbb{Z}$, такие что $-a = bq' + r'$, $0 \le r' < b$. Если $r' = 0$, положим $q = -q'$, $r = 0$; если же $r' > 0$, то положим $q = -q' - 1$, $r = b - r'$. В обоих случаях $a = bq + r$, $0 \le r < b$.

Наконец, пусть $b < 0$; тогда $-b > 0$. По уже доказанному, существуют такие $q', r \in \mathbb{Z}$, что $a = (-b)q' + r$, $0 \le r < -b = |\, b \,|$. Положим $q = -q'$; тогда $a = bq + r$, $0 \le r < |\, b \,|$.

Идеалы кольца $\mathbb{Z}$. Следующая теорема является основной для теории делимости в кольце $\mathbb{Z}$.

Теорема 2. *Всякий идеал кольца целых чисел $\mathbb{Z}$ главный.*

Доказательство. Пусть I – идеал кольца $\mathbb{Z}$. Число 0 всегда принадлежит идеалу. Если идеал I состоит только из 0, то $I = (0)$, и все доказано. Пусть в I есть ненулевой элемент a; тогда $-a$ тоже принадлежит идеалу I. Одно из чисел a, $-a$ положительно. Таким образом, множество I_+ натуральных чисел, принадлежащих идеалу I, непусто. По аксиоме индукции, в множестве I_+ есть наименьший элемент c. Покажем, что $I = (c)$, чем и завершим доказательство теоремы.

Любой элемент $a \in (c)$ имеет вид $a = cx$, где $x \in \mathbb{Z}$; но $c \in I$, и потому $a = cx \in I$. Итак, $(c) \subseteq I$. Обратно, пусть $b \in I$; разделим b с остатком на c: $b = cq + r$, где $q, r \in \mathbb{Z}, 0 \le r < c$. Если $r > 0$, то $r = b - cq$ принадлежит идеалу I, так как b и c оба принадлежат I; следовательно, $r < c$ – натуральное число, принадлежащее I, а это противоречит тому, что наименьшим натуральным числом в I является число c. Итак, $r = 0$, и $b = cq \in (c)$. Таким образом, доказано и обратное включение $I \subseteq (c)$.

4. Наибольший общий делитель

Кольца главных идеалов. Мы по-прежнему основное внимание уделяем кольцу целых чисел. Однако, в рассуждениях мы все еще используем сравнительно мало специфических свойств целых чисел, так что результаты на самом деле остаются справедливыми и в более общей ситуации.

До сих пор наша теория строилась для произвольных коммутативных ассоциативных колец с 1. Теперь мы наложим на рассматриваемые кольца еще одно ограничение: мы будем считать, что все идеалы кольца главные. Теорема 2 показывает, что кольцо целых чисел $\mathbb{Z}$ удовлетворяет этому условию.

Наибольший общий делитель. Пусть A – коммутативное ассоциативное кольцо с 1, и пусть $a_1, \ldots, a_n \in A$. Элемент $d \in A$ называется наибольшим общим делителем a_1, ... , a_n, если выполняются условия:

a). $a_1 \div d, a_2 \div d, \ldots, a_n \div d$;

b). если $\delta \in A$ и $a_1 \div \delta, a_2 \div \delta, \ldots, a_n \div \delta$, то $d \div \delta$.

Иными словами, наибольший общий делитель a_1, ... , a_n – это такой общий делитель a_1, ... , a_n, который делится на любой их общий делитель.

Естественно возникают вопросы: всегда ли существует наибольший общий делитель? если наибольший общий делитель существует, то единствен ли он? как найти наибольший общий делитель? Мы ответим здесь на первые два вопроса; ответ на третий вопрос для кольца целых чисел будет дан в следующем пункте.

Теорема 1. *Пусть A – коммутативное ассоциативное кольцо с 1, и пусть $a_1, \ldots, a_n \in A$.*

(1) Если d, d' – два наибольших общих делителя элементов $a_1, \ldots, a_n$, то d и d' ассоциированы, т.е. $(d) = (d')$.

(2) Если все идеалы кольца A главные, то наибольший общий делитель элементов $a_1, \ldots, a_n$ существует. Более того, элемент $d \in A$ является наибольшим общим делителем a_1, ... , a_n тогда и только тогда, когда $(d) = (a_1, \ldots, a_n)$.

(3) Если все идеалы кольца A главные, и d – наибольший общий делитель элементов $a_1, ..., a_n \in A$, то существуют такие элементы $x_1, \ldots, x_n \in A$, что $d = x_1a_1 + \cdots + x_na_n$.

(4) Если все идеалы кольца A главные, и d – наибольший общий делитель элементов $a, b \in A$, то существует такой элемент $x \in A$, что $xa \equiv d \pmod b$.

Доказательство. Утверждение (1) очевидно: наибольший общий делитель d делится на другой общий делитель d', а наибольший общий делитель d' делится на другой общий делитель d. Утверждение (3) тривиально следует из утверждения (2): если d – наибольший общий делитель элементов $a_1, \ldots, a_n$, то $d \in (d) = (a_1, \ldots, a_n)$, а идеал $(a_1, \ldots, a_n)$ состоит по определению из элементов вида $x_1a_1 + \cdots + x_na_n$, где $x_1, \ldots, x_n \in A$. Далее, утверждение (4) по существу совпадает с утверждением (3) для $n = 2$: если d – – наибольший общий делитель элементов $a, b \in A$, то существуют такие $x, y \in A$, что $xa + yb = d$, т.е. $xa = d - yb \equiv d \pmod b$. Остается, таким образом, доказать утверждение (2).

Поскольку все идеалы кольца A главные, существует элемент $d \in A$, такой что $(d) = (a_1, \ldots, a_n)$; покажем, что d – наибольший общий делитель элементов $a_1, \ldots, a_n$. В самом деле, для любого i, $1 \le i \le n$, элемент a_i принадлежит идеалу $(a_1, \ldots, a_n) = (d)$; но идеал (d) состоит из элементов, делящихся на d, и потому $a_i \div d$. Итак, d – общий делитель $a_1, \ldots, a_n$. Пусть теперь δ – какой-то общий делитель $a_1, \ldots, a_n$. Элемент d принадлежит идеалу $(d) = (a_1, \ldots, a_n)$, а идеал $(a_1, \ldots, a_n)$ состоит по определению из элементов вида $x_1a_1 + \cdots + x_na_n$, где $x_1, \ldots, x_n \in A$. Итак, существуют $x_1, \ldots, x_n \in A$, такие что $d = x_1a_1 + \cdots + x_na_n$; поскольку $a_1 \div \delta$, ... , $a_n \div \delta$, мы получаем, что и элемент $d = x_1a_1 + \cdots + x_na_n$ делится на δ. Итак, d – наибольший общий делитель элементов $a_1, \ldots, a_n$.

Мы доказали, таким образом, что если все идеалы кольца A главные, то существует наибольший общий делитель d элементов $a_1, \ldots, a_n$, причем если $(d) = (a_1, \ldots, a_n)$, то d – наибольший общий делитель $a_1, \ldots, a_n$. Обратно, если d' – любой наибольший общий делитель $a_1, \ldots, a_n$, то по утверждению (1) доказываемой теоремы имеем: $(d') = (d) = (a_1, \ldots, a_n)$. Теорема полностью доказана.

В математической литературе принято записывать тот факт, что d является наибольшим общим делителем $a_1, \ldots, a_n$ следующим образом: $(a_1, \ldots, a_n) = d$. Однако, мне кажется, что это не совсем корректно, потому что наибольший общий делитель определен не однозначно, и правильнее было бы писать $(a_1, \ldots, a_n) = (d)$, что мы и будем делать.

Алгорифм Евклида. Способ, позволяющий вычислить наибольший общий делитель двух целых чисел, был открыт еще в древности. В настоящее время он известен под названием "алгорифм Евклида".

Основан алгорифм Евклида на следующих двух простых утверждениях.

(1) *Если $a, b \in \mathbb{Z}$, $b \neq 0$ и r – остаток от деления a на b, то $(a, b) = (b, r)$.*

(2) *Если $a \in \mathbb{Z}$, то $(a, 0) = (a)$.*

Доказательство. (1). По определению остатка, существует такое целое число q, что $a = bq + r$; тогда $r = a - bq$. Имеем включения, которые доказывают (1):

$$(a,b)=\{ax+by \mid x,y\in\mathbb{Z}\}=\{(bq+r)x+by \mid x,y\in\mathbb{Z}\}=\{b(qx+y)+rx \mid x,y\in\mathbb{Z}\} \subseteq (b,r),$$

$$(b,r)=\{bx+ry \mid x,y\in\mathbb{Z}\}=\{bx+(a-bq)y \mid x,y\in\mathbb{Z}\}=\{ay+b(x-qy) \mid x,y\in\mathbb{Z}\} \subseteq (a,b).$$

(2). Совсем очевидно: $(a, 0) = \{ax + 0 \cdot y \mid x, y \in \mathbb{Z}\} = \{ax \mid x \in \mathbb{Z}\} = (a)$.

Теперь мы можем описать алгорифм Евклида. Пусть $a, b \in \mathbb{Z}$, причем $b \neq 0$. Строим последовательность целых чисел $a_0, a_1, a_2, \ldots$ следующим образом:

1. Полагаем $a_0 = a$, $a_1 = b$.

2. Пусть $a_0, a_1, \ldots, a_n$ уже построены ($n \geq 1$). Если $a_n \neq 0$, то полагаем a_{n+1} равным остатку от деления a_{n-1} на a_n; если же $a_n = 0$, то полагаем $d = a_{n-1}$ и останавливаем построение.

Покажем, что эта процедура обязательно остановится и что выданное ею число d является наибольшим общим делителем a и b. Поскольку при $n > 1$ каждое число a_n является остатком от деления на предыдущее число, справедливы неравенства: $a_2, a_3, \cdots \geq 0, \quad a_2 > a_3 > \ldots$. Но убывающая последовательность положительных целых чисел не может быть бесконечной, и поэтому обязательно найдется такой номер $n > 1$, что $a_{n-1} \neq 0$, $a_n = 0$. Тогда по построению $d = a_{n-1}$; вспоминая, что каждое a_{i+1} – это остаток от деления a_{n-1} на a_n, и используя доказанные выше утверждения (1), (2), мы получаем:

$$(a, b) = (a_0, a_1) = (a_1, a_2) = \cdots = (a_{n-1}, a_n) = (a_{n-1}, 0) = (d, 0) = (d).$$

Таким образом, d – наибольший общий делитель a и b.

Заметим, что алгорифм Евклида не только находит наибольший общий делитель чисел a и b, но и позволяет представить его в виде $au + bv$, где $u, v \in \mathbb{Z}$. Для этого последовательно представим все числа a_i в виде $a_i = au_i + bv_i$. Имеем: $a_0 = a \cdot 1 + b \cdot 0$, $a_1 = a \cdot 0 + b \cdot 1$. По построению $a_{i-1} = q_i a_i + a_{i+1}$, где q_i – неполное частное от деления a_{i-1} на a_i; если уже найдены линейные представления $a_{i-1} = au_{i-1} + bv_{i-1}$, $a_i = au_i + bv_i$, то

$$a_{i+1} = a_{i-1} - q_i a_i = a(u_{i-1} - q_i u_i) + b(v_{i-1} - qv_i),$$

так что в качестве u_{i+1}, v_{i+1} можно взять числа $u_{i-1} - q_i u_i$, $v_{i-1} - qv_i$. Поскольку $d = a_{n-1}$, мы и получим искомое линейное представление наибольшего общего делителя $d = au_{n-1} + bv_{n-1}$.

Взаимно простые элементы. Мы возвращаемся к рассмотрению произвольных коммутативных ассоциативных колец с 1, в которых все идеалы главные. Элементы $a_1, \ldots, a_n$ кольца A называются взаимно простыми в совокупности, если 1 является их наибольшим общим делителем. Подчеркнем: было бы не совсем точно сказать, что элементы взаимно просты в совокупности, если их наибольший общий делитель равен 1, потому что, например, -1 тоже будет наибольшим общим делителем этих элементов. Тот факт, что элементы $a_1, \ldots, a_n$ взаимно просты в совокупности, равносилен соотношению $(a_1, \ldots, a_n) = (1)$, которое мы и будем использовать для обозначения этого факта (в отличие от обычно применяющегося в литературе обозначения $(a_1, \ldots, a_n) = 1$).

Для двух элементов $a, b \in A$ вместо того, чтобы говорить, что они взаимно просты в совокупности, мы будем говорить, что они взаимно просты, опуская слова "в совокупности".

Основные свойства взаимной простоты собраны в следующем утверждении.

Предложение 1. *Пусть A – коммутативное ассоциативное кольцо с 1, в котором все идеалы главные.*

(1) *Элементы $a_1, \ldots, a_n \in A$ взаимно просты в совокупности тогда и только тогда, когда существуют элементы $x_1, \ldots, x_n \in A$, такие что $x_1 a_1 + \cdots + x_n a_n = 1$.*

(2) *Элементы $a, b \in A$ взаимно просты тогда и только тогда, когда существует элемент $x \in A$, такой что $xa \equiv 1 \pmod{b}$.*

(3) *Если $a, b, c \in A$, $ab \div c$ и элементы a и c взаимно просты, то $b \div c$.*

(4) *Если $a, b, c \in A$, $(a, c) = (1)$, $(b, c) = (1)$, то $(ab, c) = 1$.*

(5) *Если $a_1, \ldots, a_n, b \in A$ и каждый из элементов a_i, $(1 \leq i \leq n)$, взаимно прост с b, то их произведение $a_1 \ldots a_n$ тоже взаимно просто с b.*

(6) *Если* $a_1, \dots, a_n$; $b_1, \dots, b_m \in A$, *и каждый из элементов* $a_1, \dots, a_n$ *взаимно прост с каждым из элементов* $b_1, \dots, b_m$, *то их произведения* $a_1 \dots a_n$ *и* $b_1 \dots b_m$ *взаимно просты.*

(7) *Если* $a, b, c \in A$, $a \div b$, $a \div c$ *и* b *и* c *взаимно просты, то* $a \div bc$.

(8) *Если* $a, b_1, \dots, b_n \in A$, $a \div b_i$ *для всех* i, $1 \le i \le n$, *и элементы* $b_1, \dots, b_n$ *попарно взаимно просты (т.е.* $(b_i, b_j) = (1)$ *для всех* $i \ne j$, $1 \le i, j \le n$*), то* $a \div (b_1 \dots b_n)$.

Доказательство. (1). Если 1 – наибольший общий делитель $a_1, \dots, a_n$, то по теореме 1, (3) существуют элементы $x_1, \dots, x_n \in A$, такие что $x_1a_1 + \dots + x_na_n = 1$. Обратно, если d – наибольший общий делитель $a_1, \dots, a_n$ и $x_1a_1 + \dots + x_na_n = 1$ для некоторых $x_1, \dots, x_n \in A$, то $1 = x_1a_1 + \dots + x_na_n \div d$, т.е. d – делитель 1. Но тогда $1 \sim d$ – тоже наибольший общий делитель $a_1, \dots, a_n$.

(2) Если 1 – наибольший общий делитель $a, b \in A$, то по теореме 1, (4) существует элемент $x \in A$, такой что $xa \equiv 1 \pmod b$. Обратно, если d – наибольший общий делитель a и b, и существует элемент $x \in A$, такой что $xa \equiv 1 \pmod b$, то существует и элемент $y \in A$, такой что $xa - 1 = by$, т.е. $1 = xa + (-y)b$; но тогда a и b взаимно просты по утверждению (1).

(3) Элементы a и c взаимно просты; поэтому по свойству (2) существует такой элемент $x \in A$, что $xa \equiv 1 \pmod c$. Умножая обе части этого сравнения на b и учитывая, что $ab \div c$, т.е. $ab \equiv 0 \pmod c$, получаем, что $b \equiv xab \equiv 0 \pmod c$, и $b \div c$.

(4) Если $(a, c) = (1)$, $(b, c) = (1)$, то по свойству (2) существуют такие $x, y \in A$, что $xa \equiv 1 \pmod c$, $yb \equiv 1 \pmod c$. Перемножив эти сравнения, получим: $(xy)(ab) \equiv 1 \pmod c$. Опять используя свойство (2) (но уже в другую сторону!), получаем, что ab и c взаимно просты.

(5) Индукция по n. При $n = 1$ утверждение бессодержательно, при $n = 2$ оно совпадает со свойством (4). Пусть $n > 2$ и уже доказано, что $(a_1 \dots a_{n-1}, b) = (1)$; тогда, опять по свойству (3), элементы $(a_1 \dots a_{n-1})a_n = a_1 \dots a_{n-1}a_n$ и b взаимно просты.

(6) По свойству (4), каждый из элементов b_1, ... , b_m взаимно прост с произведением $a_1 \dots a_n$; опять используя свойство (4), находим, что произведение $b_1 \dots b_m$ взаимно просто с $a_1 \dots a_n$.

(7) Поскольку $a \div b$, $a \div c$, существуют $u, v \in A$, такие что $a = bu = cv$. Далее, b и c взаимно просты, и потому существуют $x, y \in A$, такие что $1 = bx + cy$. Умножив последнее равенство на a, получаем:

$$a = abx + acy = (cv)bx + (bu)cy = (bc)(vx + uy) \div bc.$$

(8) Индукция по n; при $n = 2$ утверждение совпадает со свойством (7). Пусть $n > 2$ и пусть уже доказано, что a делится на $b_1 \dots b_{n-1}$. По свойству (5) элементы $b_1 \dots b_{n-1}$ и b_n взаимно просты. Поскольку a делится и на $b_1 \dots b_{n-1}$, и на b_n, по свойству (7) a делится и на $(b_1 \dots b_{n-1})b_n = b_1 \dots b_{n-1}b_n$.

Китайская теорема об остатках.

Теорема 2. *Пусть* A *– коммутативное ассоциативное кольцо с 1, в котором все идеалы главные, и пусть элементы* $n_1, \dots, n_r \in A$ *попарно взаимно просты. Тогда:*

(1) *для произвольных элементов* $a_1, \dots, a_r \in A$ *найдется такой элемент* $x \in A$, *что,* $x \equiv a_1 \pmod{n_1}, \dots, x \equiv a_r \pmod{n_r}$;

(2) *всякие два таких элемента сравнимы по модулю* $n_1 \cdots n_r$, *и наоборот, всякий элемент* $y \in A$, *сравнимый по модулю* $n_1 \cdots n_r$ *с элементом* x, *удовлетворяющим требованиям пункта* (1), *тоже удовлетворяет этим требованиям.*

Доказательство. (1). Утверждение бессодержательно, если $r = 1$. Пусть $r \geq 2$. Для $1 \leq i \leq r$ обозначим через N_i произведение всех элементов $n_1, \ldots, n_r$, кроме n_i. Поскольку элемент n_i взаимно прост с каждым элементом n_j, $j \neq i$, он взаимно прост и с их произведением N_i, и поэтому существует такой элемент $q_i \in A$, что $q_i N_i \equiv 1 \pmod{n_i}$. Положим $x = a_1 q_1 N_1 + \cdots + a_i q_i N_i + \cdots + a_r q_r N_r$. При $i \neq j$ элемент n_i входит в N_j в качестве сомножителя, и потому $N_j \equiv 0 \pmod{n_i}$; следовательно, для любого i, $1 \leq i \leq r$,

$$x = a_1 q_1 N_1 + \cdots + a_i q_i N_i + \cdots + a_r q_r N_r \equiv a_i (q_i N_i) \equiv a_i \cdot 1 = a_i \pmod{n_i}.$$

(2). Пусть $x, y \in A$, и пусть $x \equiv a_1 \pmod{n_1}, \ldots, x \equiv a_r \pmod{n_r}$; тогда для выполнения сравнений $y \equiv a_1 \pmod{n_1}, \ldots, y \equiv a_r \pmod{n_r}$ необходимо и достаточно, чтобы разность $y - x$ была сравнима с 0 по каждому из модулей $n_1, \ldots, n_r$, т.е. чтобы эта разность делилась на каждый из элементов $n_1, \ldots, n_r$. Поскольку по условию теоремы элементы $n_1, \ldots, n_r$ попарно взаимно просты, предыдущее условие по предложению 1, (8) равносильно тому, что $y - x$ делится на $n_1 \cdots n_r$, т.е. $y \equiv x \pmod{n_1 \cdots n_r}$.

5. Простые элементы

Простые элементы. Всякий элемент $a \in A$ может быть разложен в произведение двух сомножителей, один из которых ε является делителем 1 в кольце A, а другой $a' = \varepsilon^{-1} a$ ассоциирован с a. Такие разложения элемента a в произведение двух сомножителей называются тривиальными. Ненулевой элемент $p \in A$ называется простым (или неприводимым), если p – не делитель 1, и всякое разложение p в произведение двух сомножителей является тривиальным, т.е. один из сомножителей разложения ассоциирован с p, а другой – делитель 1. Полезно сформулировать и отрицание этого определения: если ненулевой элемент $a \in A$ не является ни делителем 1, ни простым (неприводимым) элементом, то существует его представление в виде $a = bc$, где $b, c \in k$ и оба сомножителя – не делители 1. [1]

Из определения простого элемента сразу следует, что всякий его делитель или асоциирован с ним, или является делителем 1.

Предложение 1. *Пусть A – область главных идеалов.*

(1) Пусть $p \neq 0$ – простой элемент A и пусть $a \in A$. Тогда или a делится на p, или a взаимно просто с p.

(2) Пусть $a_1, \ldots, a_n$ – элементы из A, $p \neq 0$ – простой элемент A, и пусть $a_1 \ldots a_n$ делится на p. Тогда хотя бы один из сомножителей $a_1, \ldots, a_n$ делится на p.

(3) Если p, q – ненулевые простые элементы A и $p \div q$, то $p \sim q$, или, что то же, $(p) = (q)$.

(4) Если p – ненулевой простой элемент A и $q \sim p$, то q – тоже простой элемент A.

(5) Пусть $p_1, \ldots, p_n; q_1, \ldots, q_m$ – ненулевые простые элементы кольца A. Если $p_1 \ldots p_n \div q_1 \ldots q_m$, то $m \leq n$ и существует такая подстановка σ множества $\{1, \ldots, n\}$, что $p_{\sigma(1)} \sim q_1, \ldots, p_{\sigma(m)} \sim q_m$.

(6) Пусть $p_1, \ldots, p_n; q_1, \ldots, q_m$ – ненулевые простые элементы кольца A. Если $p_1 \ldots p_n \sim q_1 \ldots q_m$, то $m = n$ и существует такая подстановка σ множества $\{1, \ldots, n\}$, что $p_{\sigma(1)} \sim q_1, \ldots, p_{\sigma(n)} \sim q_n$.

---

[1] На самом деле дано определение неприводимого элемента. В общем случае простые элементы определяются иначе; в частности, в области целостности 0 является простым элементом. Однако, для ненулевых элементов области главных идеалов понятия простоты и неприводимости совпадают. Мы предпочли здесь термин "простой", потому что прежде всего имеем в виду целые числа, а для них принято говорить о простых, а не неприводимых, числах. Мы вернемся к обсуждению этих вопросов в одной из следующих глав.

Доказательство. (1) Пусть $d \in A$ является наибольшим общим делителем a и p. Тогда $p \div d$; следовательно, d, как и любой делитель простого элемента p, ассоциирован с p или является делителем 1. В первом случае a делится на ассоциированный с d элемент p, во втором $1 \sim d$ – тоже наибольший общий делитель a и p, и потому элементы a, p взаимно просты.

(2) Если ни один из элементов $a_1, \ldots, a_n$ не делится на p, то, по свойству (1), все они взаимно просты с p. Но тогда и их произведение взаимно просто с p, а это невозможно, ибо в этом случае наибольший общий делитель 1 элементов $a_1 \ldots a_n$, p делился бы на их общий делитель p, и простой элемент p был бы делителем 1.

(3) Поскольку q – делитель простого элемента p, q ассоциирован с p или q – делитель 1. Но вторая возможность отпадает, так как простой элемент q по определению не может быть делителем 1.

(4) Очевидно.

(5) Это самое главное утверждение нашего предложения. Будем доказывать его индукцией по m. Случай $m = 0$ бессодержателен. Пусть $m \geq 1$ и для меньших значений этого параметра утверждение уже доказано. Элемент $p_1 \ldots p_n$ делится на элемент $q_1 \ldots q_m$, который в свою очередь делится на q_1. Тогда по свойству (2) найдется сомножитель p_i $(1 \leq i \leq n)$, который делится на q_1; по свойству (3) $p_i \sim q_1$. Если $i \neq 1$, положим $p'_1 = p_i$, $p'_i = p_1$, $p'_j = p_j$ при $j \neq 1, i$; если же $i = 1$, то положим $p'_j = p_j$ для всех j. В обоих случаях $p'_1 \sim q_1$, и потому $q_1 \div p'_1$, т.е. существует $\varepsilon \in A$, для которого $q_1 = \varepsilon p'_1$. Мы имеем:

$$p'_1 p'_2 \ldots p'_n \div q_1 q_2 \ldots q_m = p'_1 \varepsilon q_2 \ldots q_m \div p'_1 q_2 \ldots q_m.$$

Поэтому существует элемент $x \in A$, такой что $p'_1 p'_2 \ldots p'_n = p'_1 q_2 \ldots q_m x$; сократив обе части этого равенства на $p'_1 \neq 0$ (это можно делать, потому что A – область целостности), получим, что $p'_2 \ldots p'_n = q_2 \ldots q_m x \div q_2 \ldots q_m$. К полученному соотношению можно применить предположение индукции, согласно которому количество сомножителей в произведении $p'_2 \ldots p'_n$ не меньше количества сомножителей в произведении $q_2 \ldots q_m$, т.е. $n - 1 \geq m - 1$, и, кроме того, существует подстановка

$$\begin{pmatrix} 2 & 3 & \ldots & n \\ j_2 & j_3 & \ldots & j_n \end{pmatrix},$$

такая что $p'_{j_2} \sim q_2,\ p'_{j_3} \sim q_3,\ \ldots, p'_{j_m} \sim q_m$. Положим

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & j_2 & j_3 & \ldots & j_n \end{pmatrix} \quad \text{или} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & j_2 & j_3 & \ldots & j_n \end{pmatrix} (1, i)$$

в зависимости от того, равен или нет 1 индекс i, для которого $p'_1 = p_i$. Мы получаем требуемый результат: $n \geq m$, потому что $n - 1 \geq m - 1$, и $p_{\sigma(1)} \sim q_1$, $p_{\sigma(2)} \sim q_2$, ... , $p_{\sigma(m)} \sim q_m$.

(6) Это утверждение – простое следствие из утверждения (5); надо лишь заметить, что не только $p_1 \ldots p_n$ делится на $q_1 \ldots q_m$, но и наоборот, $q_1 \ldots q_m$ делится на $p_1 \ldots p_n$, а потому справедливы оба неравенства $n \geq m$, $m \geq n$.

6. Основная теорема арифметики для целых чисел

Особенности теории делимости для целых чисел. Для целых чисел теория делимости чуть-чуть проще, чем в общем случае. Прежде всего, в $\mathbb{Z}$ "почти нет"делителей 1: их только 2 – это число 1 и число -1. Далее, ассоциированными с числом $a \in \mathbb{Z}$ являются только числа $\pm a$; таким образом, для каждого числа из $\mathbb{Z}$ существует одно и только одно ассоциированное с ним неотрицательное число. Отметим еще, что произведение неотрицательных чисел неотрицательно. Множество простых ненулевых элементов кольца $\mathbb{Z}$ состоит из двух классов – положительных простых элементов 2, 3, 5, 7, 11, ... , которые, собственно, и называются простыми числами, и отрицательных простых элементов -2, -3, -5 и т.д.

Основная теорема арифметики.

Теорема 1. *Всякое целое число $a \in \mathbb{Z}$, отличное от 0, может быть представлено в виде произведения $a = \varepsilon p_1 \dots p_n$, где $\varepsilon = \pm 1$, $n \geq 0$, $p_1, \dots, p_n$ – положительные простые числа. Это представление единственно с точностью до порядка сомножителей: если есть другое представление $a = \delta q_1 \dots q_m$, где $\delta = \pm 1$, $m \geq 0$, $q_1, \dots, q_m$ – положительные простые числа, то $\varepsilon = \delta$, $m = n$ и существует подстановка $\sigma \in S_n$, такая что $q_1 = p_{\sigma(1)}, \dots, q_n = p_{\sigma(n)}$.*

Доказательство. Единственность по существу уже доказана. Если

$$a = \varepsilon p_1 \dots p_n = \delta q_1 \dots q_m,$$

где $\varepsilon, \delta = \pm 1$, а p_i, q_j – положительные простые числа, то $p_1 \dots p_n \sim q_1 \dots q_m$, и по предложению 8, (6) $m = n$ и существует такая подстановка σ множества $\{1, \dots, n\}$, что $p_{\sigma(1)} \sim q_1$, ... , $p_{\sigma(n)} \sim q_n$. Но положительные целые числа ассоциированы лишь тогда, когда они совпадают, поэтому $q_1 = p_{\sigma(1)}, \dots, q_n = p_{\sigma(n)}$. Остается заметить, что если $a > 0$, то $\varepsilon = \delta = 1$, а если $a < 0$, то $\varepsilon = \delta = -1$.

Теперь покажем существование разложения. Сначала индукцией докажем, что всякое целое положительное a раскладывается в произведение положительных простых чисел. Для $a = 1$ утверждение верно: 1 является произведением 0 простых сомножителей. Пусть $a > 1$ и для всех положительных целых чисел $b < a$ существование разложения уже доказано. Если $a = p$ – простое число, то $a = p$ и есть нужное представление (здесь количество простых сомножителей равно 1). Пусть теперь число a не простое; тогда у него существует нетривиальный делитель b, который можно считать положительным, потому что вместе с b число $-b$ тоже является нетривиальным делителем a. Поскольку $a \div b$, существует $c \in \mathbb{Z}$, для которого $a = bc$; при этом вместе с a и b число c положительно. Заметим, что $b \neq 1$, так как нетривиальный делитель b не является делителем 1, и $c \neq 1$, поскольку в противном случае $b = a$ ассоциировано с a, и потому является тривиальным делителем a. Но тогда $b > 1$, $c > 1$, а значит, $b < a$, $c < a$. Поэтому мы можем применить к b и c предположение индукции: существуют положительные простые числа $p_1, \dots, p_m; p_{m+1}, \dots, p_n$, такие что $b = p_1 \dots p_m$, $c = p_{m+1} \dots p_n$. Но тогда $a = bc = p_1 \dots p_m p_{m+1} \dots p_n$, а это и есть нужное разложение.

Осталось доказать существование разложения для случая, когда $a < 0$. Но тогда $-a > 0$, и по уже доказанному существуют число $n \geq 0$ и положительные простые числа $p_1, \dots, p_n$, такие что $-a = p_1 \dots p_n$. Значит, $a = (-1) p_1 \dots p_n$, а это и есть нужное разложение.

О множестве простых чисел. Основная теорема арифметики показывает, что относительно умножения множество целых чисел устроено сравнительно просто. Однако, для полноты картины хотелось бы выяснить, как умножение связано со сложением. Точнее говоря, любое натуральное число получается сложением нескольких единиц, и хотелось бы знать, по какому закону среди этих сумм распределены простые числа. Но оказывается, что этот вопрос чрезвычайно труден; им занимались многие выдающиеся математики, получившие первоклассные результаты, но все они – лишь незначительное приближение к пониманию природы простых чисел. В этом пункте мы отметим лишь два элементарных свойства простых чисел, известных с древности.

Теорема 2. *Множество простых чисел бесконечно.*

Доказательство. Предположим, что это не так. Тогда существует лишь конечное множество положительных простых чисел. Пусть $p_1, p_2, \dots, p_N$ – все простые натуральные числа. По основной теореме арифметики число $p_1 p_2 \dots p_N + 1$ раскладывается в произведение простых чисел:

$$p_1 p_2 \dots p_N + 1 = q_1 q_2 \dots q_m.$$

Но простое число q_1 не может совпадать ни с одним из чисел p_1, p_2,..., p_N: если $q_1 = p_i$, то

$$1 = q_1 q_2 \dots q_m - p_1 \dots p_i \dots p_N = p_i q_2 \dots q_m - p_1 \dots p_i \dots p_N \div p_i,$$

что невозможно, так как простое число p_i не является делителем 1. Итак, предположив, что $p_1, p_2, \dots, p_N$ – все простые числа, мы нашли еще по крайней мере одно простое число q_1, не входящее в это множество. Значит, предположение о конечности множества простых чисел было неверно.

Если посмотреть на несколько первых простых чисел

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101,$$

то может возникнуть впечатление, что пробелы между соседними простыми числами не слишком велики. Однако, легко показать, что они могут быть сколь угодно большими.

Теорема 3. *Для любого натурального числа N существует такое натуральное число a, что все N последовательных чисел $a+1, a+2, \dots, a+N$ не простые.*

Доказательство. Мы явно укажем это число. Положим

$$a = (N+1)! + 1 = 1 \cdot 2 \cdot 3 \cdot \dots \cdot N \cdot (N+1) + 1;$$

тогда для любого i, $1 \le i \le N$ число

$$a + i = 1 \cdot 2 \cdot \dots \cdot (i+1) \cdot \dots \cdot (N+1) + (i+1)$$

делится на $i+1$. Но $a + i > N + 1 \ge i + 1$, а $i + 1 > 1$; поэтому число $a + i$ не простое.

7. Кольца вычетов

Сравнение как отношение эквивалентности. Пусть A – коммутативное ассоциативное кольцо с 1, и пусть $n \in A$. Мы определили выше понятие сравнения по модулю n. Напомним некоторые из основных свойств сравнений

(1) $a \equiv a \pmod{n}$ *для всякого* $a \in A$ *(рефлексивность сравнения);*
(2) *если* $a, b \in A$ *и* $a \equiv b \pmod{n}$, *то* $b \equiv a \pmod{n}$ *(симметричность сравнения);*
(3) *если* $a, b, c \in A$ *и* $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$, *то* $a \equiv c \pmod{n}$ *(транзитивность сравнения);*
(4) *если* $a, b, c, d \in A$ *и* $a \equiv c \pmod{n}$, $b \equiv d \pmod{n}$, *то* $(a \pm b) \equiv (c \pm d) \pmod{n}$, $ab \equiv cd \pmod{n}$.

Отношения между элементами множества, обладающие свойствами (1)-(3) (т.е. рефлексивные, симметричные и транзитивные отношения) играют в математике очень важную роль (а если вдуматься, то и не только в математике, а во всей научной деятельности). Такие отношения называются отношениями эквивалентности. Таким образом, первые три пункта предыдущего предложения утверждают, что сравнение по данному модулю является отношением эквивалентности на A. Последний пункт утверждает, что действия на A хорошо согласуются со сравнениями. В такой ситуации мы будем говорить, что алгебраические операции на A (в данном случае сложение и умножение) устойчивы относительно эквивалентности.

Классы вычетов. Пусть опять A – коммутативное ассоциативное кольцо с 1, и пусть $n \in A$. Для любого элемента $a \in A$ будем обозначать через $[a]_n$ множество всех таких элементов $x \in A$, что $a \equiv x \pmod{n}$. Это множество называется классом вычетов по модулю n, определенным элементом a. Иногда, когда ясно, о каком модуле идет речь, мы будем опускать его в обозначениях и писать $[a]$ вместо $[a]_n$. Еще раз подчеркнем, что класс вычетов – это подмножество A.

Лемма. *Элемент $b \in A$ принадлежит классу вычетов $[a]_n$ тогда и только тогда, когда $[a]_n = [b]_n$.*

Доказательство. Пусть $[a]_n = [b]_n$. Поскольку $b \equiv b \pmod{n}$, элемент b принадлежит классу $[b]_n = [a]_n$.

Обратно, пусть $b \in [a]_n$; тогда, по определению, $a \equiv b \pmod{n}$. Если $x \in [b]_n$, то $b \equiv x \pmod{n}$, и по транзитивности $a \equiv x \pmod{n}$, т.е. $x \in [a]_n$; таким образом, $[b]_n \subseteq [a]_n$. Пусть, наоборот, $x \in [a]_n$. Тогда $a \equiv x \pmod{n}$; кроме того, из соотношения $a \equiv b \pmod{n}$ следует из-за симметричности сравнений, что $b \equiv a \pmod{n}$. Снова пользуясь транзитивностью, получаем: $b \equiv x \pmod{n}$, т.е. $x \in [b]_n$, и доказано включение $[a]_n \subseteq [b]_n$. Сопоставляя полученные включения $[b]_n \subseteq [a]_n$, $[a]_n \subseteq [b]_n$, находим, что $[a]_n = [b]_n$.

Предложение 1. *Пусть A – коммутативное ассоциативное кольцо с 1, и пусть $n \in A$. Любые два класса вычетов по модулю n или не пересекаются, или совпадают.*

Доказательство. Если пересечение классов вычетов $[a]_n$ и $[b]_n$ непусто, то существует элемент $c \in A$, такой что $c \in [a]_n$ и $c \in [b]_n$. Но тогда по лемме $[a]_n = [c]_n$ и $[b]_n = [c]_n$, т.е. $[a]_n = [b]_n$.

Кольцо классов вычетов. Пусть A – коммутативное ассоциативное кольцо с 1, и пусть $n \in A$. Обозначим через $A/(n)$ множество всех таких подмножеств A, которые являются классами вычетов по модулю n. Таким образом, множество $X \subseteq A$ является элементом $A/(n)$ если и только если существует элемент $a \in A$, такой что $X = [a]_n$. Конечно, этот элемент a, вообще говоря, не единственный; подойдет любой элемент из множества X.

Для того, чтобы сделать это определение более понятным, опишем явно множество классов вычетов для случая $A = \mathbb{Z}$.

Предложение 2. *Пусть $n \in \mathbb{Z}$, $n > 0$. Тогда множество классов вычетов $\mathbb{Z}/(n)$ состоит из n классов $[0]_n$, $[1]_n$, ... , $[n-1]_n$.*

Доказательство. Пусть $a \in \mathbb{Z}$, и пусть r – остаток от деления a на n. Тогда $a - r = nq \div n$, где q – неполное частное, и потому $a \equiv r \pmod{n}$. Следовательно, $r \in [a]_n$, и потому по лемме $[a]_n = [r]_n$. Остается заметить, что $0 \le r < n$, т.е. что $[a]_n = [r]_n$ – один из классов $[0]_n$, $[1]_n$, ... , $[n-1]_n$, и что эти классы попарно различны, ибо при $0 \le i, j < n$, $i \ne j$ разность $i - j$ не делится на n.

Определим теперь на множестве классов вычетов $A/(n)$ две алгебраические операции – сложение и умножение. Пусть $\alpha, \beta \in A/(n)$. Напомним, что α и β – подмножества A. Выберем в них какие-то элементы $a \in \alpha \subseteq A$, $b \in \beta \subseteq A$, так что $\alpha = [a]_n$, $\beta = [b]_n$, и положим $\alpha + \beta = [a+b]_n$, $\alpha\beta = [ab]_n$. На первый взгляд эти определения некорректны, так как зависят от выбора представителей в классах α, β. Однако, если $a' \in \alpha$, $b' \in \beta$ – другие представители тех же классов, то $a' \equiv a \pmod{n}$, $b' \equiv b \pmod{n}$, и по утверждению (4) предложения 9 будет $a'+b' \equiv a+b \pmod{n}$, $a'b' \equiv ab \pmod{n}$, так что $[a'+b']_n = [a+b]_n$, $[a'b']_n = [ab]_n$, т.е. определенные нами сумма и произведение классов α, β не зависят от выбора представителей в классах.

Определения суммы и произведения классов удобно использовать в следующей форме: $[a]_n + [b]_n = [a+b]_n$, $[a]_n[b]_n = [ab]_n$.

Теорема 1. *Пусть A – коммутативное ассоциативное кольцо с 1, и пусть $n \in A$. Тогда множество классов вычетов $A/(n)$ является относительно только что определенных операций сложения и умножения коммутативным ассоциативным кольцом с 1.*

Доказательство. Надо проверить, что выполняются аксиомы коммутативного ассоциативного кольца с 1. Напомним эти аксиомы.

(1) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ для любых $\alpha, \beta, \gamma \in A/(n)$ (ассоциативность сложения);
(2) $\alpha + \beta = \beta + \alpha$ для любых $\alpha, \beta \in A/(n)$ (коммутативность сложения);
(3) существует такой элемент $\bar{0} \in A/(n)$, что $\bar{0} + \alpha = \alpha$ для любого $\alpha \in A/(n)$;
(4) для любого $\alpha \in A/(n)$ существует такой элемент $-\alpha \in A/(n)$, что $\alpha + (-\alpha) = \bar{0}$;
(5) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ для любых $\alpha, \beta, \gamma \in A/(n)$ (ассоциативность умножения);
(6) $\alpha\beta = \beta\alpha$ для любых $\alpha, \beta \in A/(n)$ (коммутативность умножения);
(7) существует такой элемент $\bar{1} \in A/(n)$, что $\bar{1} \cdot \alpha = \alpha$ для любого $\alpha \in A/(n)$;
(8) $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ для любых $\alpha, \beta, \gamma \in A/(n)$ (дистрибутивность умножения относительно сложения).

Пусть $a \in \alpha$, $b \in \beta$, $c \in \gamma$ – какие-то представители классов α, β, γ, так что $\alpha = [a]$, $\beta = [b]$, $\gamma = [c]$. Обозначим через $\bar{0}$, $\bar{1}$, $-\alpha$ классы $[0]$, $[1]$, $[-a]$. Проверим, что соотношения (1)-(8) выполняются.

(1). Пользуясь тем, что в кольце A выполняется соотношение $a + (b + c) = (a + b) + c$, получаем:

$$\alpha + (\beta + \gamma) = [a] + ([b] + [c]) = [a] + [b + c] = [a + (b + c)] = [(a + b) + c] =$$
$$= [a + b] + [c] = ([a] + [b]) + [c] = (\alpha + \beta) + \gamma.$$

(2). Пользуясь тем, что в кольце A выполняется соотношение $a + b = b + a$, получаем: $\alpha + \beta = [a] + [b] = [a + b] = [b + a] = [b] + [a] = \beta + \alpha$.

(3). Пользуясь тем, что в кольце A выполняется соотношение $0 + a = a$, получаем: $\bar{0} + \alpha = [0] + [a] = [0 + a] = [a] = \alpha$.

(4). Пользуясь тем, что в кольце A выполняется соотношение $a + (-a) = 0$, получаем: $\alpha + (-\alpha) = [a] + [-a] = [a + (-a)] = [0] = \bar{0}$.

(5). Пользуясь тем, что в кольце A выполняется соотношение $a(bc) = (ab)c$, получаем: $\alpha(\beta\gamma) = [a]([b][c]) = [a][bc] = [a(bc)] = [(ab)c] = [ab][c] = ([a][b])[c] = (\alpha\beta)\gamma$.

(6). Пользуясь тем, что в кольце A выполняется соотношение $ab = ba$, получаем: $\alpha\beta = [a][b] = [ab] = [ba] = [b][a] = \beta\alpha$.

(7). Пользуясь тем, что в кольце A выполняется соотношение $1 \cdot a = a$, получаем: $\bar{1} \cdot \alpha = [1][a] = [1 \cdot a] = [a] = \alpha$.

(8). Пользуясь тем, что в кольце A выполняется соотношение $a(b+c) = ab+ac$, получаем:

$$\alpha(\beta + \gamma) = [a]([b] + [c]) = [a][b + c] = [a(b + c)] = [ab + ac] = [ab] + [ac] =$$
$$= [a][b] + [a][c] = \alpha\beta + \alpha\gamma.$$

Кольцо $\mathbb{Z}/(n)$. Как мы видели, кольцо $\mathbb{Z}/(n)$ состоит из n элементов

$$[0]_n, [1]_n, [2]_n, \ldots, [n - 1]_n.$$

Для того чтобы сложить или перемножить два таких элемента $[i]_n$, $[j]_n$, надо сложить или перемножить определяющие их целые числа i, j, а затем получившийся результат заменить на его остаток от деления на n; класс этого остатка и будет результатом соответствующего действия. Например, $[6]_{11} + [7]_{11} = [2]_{11}$, $[6]_{11} \cdot [7]_{11} = [9]_{11}$, потому что остатки от деления чисел $6 + 7 = 13$, $6 \cdot 7 = 42$ на 11 равны соответственно 2 и 9.

В качестве примера приведем таблицы сложения и умножения для кольца $\mathbb{Z}/(6)$. В левом вертикальном ряду каждой из этих таблиц указаны все возможные значения элемента $\alpha \in \mathbb{Z}/(6)$, а в верхнем горизонтальном ряду – значения элемента $\beta \in \mathbb{Z}/(6)$. На пересечении соответствующих рядов в первой таблице указано значение суммы $\alpha+\beta$, а во второй таблице – значение произведения $\alpha\beta$.

$\alpha+\beta$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$\alpha\times\beta$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Глядя на эти таблицы, мы можем заметить, что сложение и умножение коммутативны – обе таблицы симметричны относительно диагонали. Далее, сразу видно, что есть нулевой элемент, прибавление которого к любому элементу не меняет этот последний элемент, и, аналогично, есть единичный элемент для умножения. То, что в каждой строке таблицы сложения есть [0], показывает, что для каждого элемента α есть противоположный элемент $-\alpha$. Конечно, ассоциативность сложения и умножения и дистрибутивность в этих таблицах так наглядно не проявляются.

Глядя на таблицу умножения для $\mathbb{Z}/(6)$, замечаем, что в ней довольно много нулей. Так, $[4]\cdot[3]=[0]$, хотя оба сомножителя [4] и [3] отличны от [0]. Таким образом, хотя $\mathbb{Z}/(6)$ – коммутативное ассоциативное кольцо с 1, оно не является областью целостности: в нем есть делители нуля.

Поля. Условие того, что кольцо вычетов – поле. Коммутативное ассоциативное кольцо A называется полем, если в нем, кроме аксиом (1)-(8), которые уже не один раз перечислялись, выполняется еще аксиома

(9) для любого $a \in A$, $a \neq 0$, существует такой элемент $a^{-1} \in A$, что $aa^{-1}=1$.

Иначе говоря, аксиома (9) утверждает, что всякий ненулевой элемент в поле обратим. Таким образом, в поле можно не только складывать, вычитать, умножать элементы, но и делить на любой ненулевой элемент. Как было показано ранее (когда мы говорили о делителях 1), элемент a^{-1} с указанным свойством единствен; он называется обратным к a элементом.

Хорошо известными всем примерами полей являются поле рациональных чисел $\mathbb{Q}$ и поле вещественных чисел $\mathbb{R}$. Формально кольцо, состоящее из единственного элемента 0, является полем, так как аксиомы (1-(9) в нем тривиальным образом выполнены; однако, обычно его полем не считают.

Предложение 3. *Всякое поле является областью целостности.*

Доказательство. Пусть K – поле; тогда, по определению, K является коммутативным ассоциативным кольцом с 1, и потому надо доказать только, что в нем нет делителей 0, т.е. что если $a, b \in K$, $a \neq 0$, $b \neq 0$, то $ab \neq 0$. Но это тривиально: если $ab=0$, то $b = 1\cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}\cdot 0 = 0$ в противоречие с предположением $b \neq 0$.

Теорема 2. *Пусть A – область целостности, в которой все идеалы главные, и пусть $n \in A$, причем $n \neq 0$ и n – не делитель 1. Тогда равносильны следующие условия:*

(1) *кольцо вычетов $A/(n)$ является полем;*
(2) *кольцо вычетов $A/(n)$ является областью целостности;*

(3) *n – простой элемент кольца A.*

Доказательство. (1) $\Rightarrow$ (2) совпадает с предыдущим предложением.

(2) $\Rightarrow$ (3). Пусть $A/(n)$ – область целостности. Если n – не простой элемент, то у n есть нетривиальный делитель $a \in A$. Существует элемент $b \in A$, такой что $n = ab$. При этом a не делится на n (иначе элемент a был бы ассоциирован с n и был бы тривиальным делителем n). Покажем, что b не делится на n. В противном случае существовал бы элемент $c \in A$, такой что $b = nc$, и мы имели бы: $n \cdot 1 = n = ab = n(ac)$; поскольку A – область целостности, а $n \neq 0$, отсюда следовало бы что $1 = ac$, т.е. что a – делитель 1, и потому a – тривиальный делитель n. Таким образом, $[a]_n \neq [0]_n$, $[b]_n \neq [0]_n$, но $[a]_n[b]_n = [ab]_n = [n]_n = [0]_n$, а это противоречит тому, что $A/(n)$ – область целостности.

(3) $\Rightarrow$ (2). Пусть элемент $n \neq 0$ простой, и пусть $[a]_n$ – ненулевой элемент кольца вычетов $A/(n)$. Поскольку $[a]_n \neq [0]_n$, элемент $a \in A$ не делится на n, а значит, a взаимно прост с простым элементом n. Но тогда существуют элементы $b, c \in A$, такие что $ab + cn = 1$. Отсюда следует, что $ab \equiv 1 \pmod{n}$, т.е. $[a]_n[b]_n = [ab]_n = [1]_n$. Итак, для произвольного ненулевого элемента $[a]_n$ кольца $A/(n)$ нашелся обратный к нему элемент $[b]_n \in A/(n)$.

Благодаря этой теореме, у нас, кроме полей $\mathbb{Q}$ и $\mathbb{R}$, появилось еще бесконечно много примеров полей. Именно, по теореме 8 полями являются кольца вычетов $\mathbb{Z}/(2)$, $\mathbb{Z}/(3)$, $\mathbb{Z}/(5)$, $\mathbb{Z}/(7)$, $\mathbb{Z}/(11)$, $\ldots$. Мы будем называть эти кольца вычетов полями вычетов по простым модулям.

8. Обратимые элементы кольца вычетов

Обратимые элементы кольца. Пусть A – коммутативное ассоциативное кольцо с 1. Напомним, что элемент $\varepsilon \in A$ называется обратимым, или делителем 1, если существует такой элемент $\delta \in A$, что $\varepsilon\delta = 1$. Мы показали ранее, что такой элемент δ единствен, и ввели для него обозначение ε^{-1}. Множество всех обратимых элементов кольца A будем обозначать через A^*.

Предложение 1. *Пусть A – коммутативное ассоциативное кольцо с 1. Множество A^* всех его обратимых элементов является абелевой группой относительно умножения кольца A.*

Доказательство. Мы видели ранее (см. предложение 3), что если $\varepsilon, \delta \in A^*$, то $\varepsilon\delta \in A^*$, так что умножение ставит в соответствие паре элементов из A^* снова элемент из A^*. Таким образом, умножение кольца A индуцирует на A^* алгебраическую операцию. Эта операция ассоциативна и коммутативна, потому что кольцо A коммутативно и ассоциативно. Далее, по предложению 3 $1 \in A^*$, и если $\varepsilon \in A^*$, то и $\varepsilon^{-1} \in A^*$, и они обладают теми свойствами, которыми должны обладать единица и обратный элемент в группе: $1 \cdot \varepsilon = \varepsilon$ для любого $\varepsilon \in A^*$; $\varepsilon^{-1}\varepsilon = 1$ для любого $\varepsilon \in A^*$. Этим завершается доказательство предложения.

Мы будем называть A^* группой обратимых элементов кольца A.

Обратимые элементы кольца вычетов. В кольце вычетов обратимые классы вычетов допускают простое описание.

Предложение 2. *Пусть A – коммутативное ассоциативное кольцо с 1, в котором все идеалы главные, $n \in A$, $n \neq 0$, и пусть $\alpha \in A/(n)$. Следующие условия равносильны:*

(1) *класс вычетов α обратим в $A/(n)$;*
(2) *все элементы $a \in \alpha$ взаимно просты с n;*
(3) *существует элемент $a \in \alpha$, взаимно простой с n.*

Доказательство. (2) $\Rightarrow$ (3) – тривиально. Докажем, что (3) $\Rightarrow$ (1). Пусть $a \in A$, элемент из класса α, взаимно простой с n. Тогда, во-первых, $\alpha = [a]_n$, во-вторых, существуют такие $b, c \in A$, что $ab+cn = 1$. Последнее равенство влечет сравнение $ab \equiv 1 \pmod n$, откуда следует, что $\alpha[b]_n = [a]_n[b]_n = [ab]_n = [1]_n$. Класс $[b]_n \in A/(n)$ оказался обратным к классу α, что и доказывает, что $\alpha \in (A/(n))^*$.

(1) $\Rightarrow$ (2). Пусть $\alpha \in (A/(n))^*$ и пусть $a \in \alpha$; тогда $\alpha = [a]_n$. Выберем любой элемент b в обратном классе α^{-1}, так что $\alpha^{-1} = [b]_n$. Тогда $[ab]_n = [a]_n[b]_n = \alpha\alpha^{-1} = [1]_n$, откуда следует, что $ab \equiv 1 \pmod n$. Это значит, что существует $c \in A$, для которого $ab - cn = 1$; но тогда a и n взаимно просты по предложению 5, (1).

9. Функция Эйлера

О числе элементов конечного множества. Если X – конечное множество, то через $|X|$ мы будем обозначать число элементов в нем. Следующее простое утверждение часто используется при работе с конечными множествами.

Пусть $f : X \to Y$ – биективное отображение, и пусть одно из множеств X, Y конечно; тогда и другое из этих множеств конечно, и $|X| = |Y|$.

Мы не доказываем это утверждение, потому что для доказательства надо было бы точно определить все термины, использованные в формулировке. Но с понятиями "число элементов множества", "натуральное число" мы знакомы лишь из школьного курса, и поэтому имеем о них только наглядно-наивное представление. Точные определения могут быть даны в рамках теории множеств; но там как раз существование биективного отображения одного множества на другое принимается за определение того, что множества состоят из одинакового количества элементов, так что наше наивно очевидное утверждение, строго говоря, является определением.

Определение функции Эйлера. Пусть $n \in \mathbb{Z}$, $n > 1$. Обозначим через $X(n)$ множество $\{0, 1, 2, \ldots, n-1\}$, а через $X'(n)$ – подмножество $X(n)$, состоящее из всех таких чисел, которые взаимно просты с n. Кольцо $\mathbb{Z}/(n)$ состоит из классов вычетов $[0], [1], \ldots, [n-1]$, а группа $(\mathbb{Z}/(n))^*$ обратимых элементов кольца вычетов $\mathbb{Z}/(n)$ – из тех и только тех классов $[i]$, $0 \le i < n$, для которых числа i и n взаимно просты. Поэтому отображение из $X'(n)$ в $\mathbb{Z}/(n)$, сопоставляющее числу $i \in X'(n)$ класс вычетов $[i] \in \mathbb{Z}/(n)$, является биективным отображением $X'(n)$ на $(\mathbb{Z}/(n))^*$. Следовательно, последние два множества состоят из одинакового числа элементов. Положим

$$\varphi(n) = |X'(n)| = |(\mathbb{Z}/(n))^*|.$$

Итак, число $\varphi(n)$ может быть определено двумя способами: оно равно количеству обратимых элементов кольца $\mathbb{Z}/(n)$, а также количеству тех из чисел $0, 1, 2, \ldots, n-1$, которые взаимно просты с n.

Мы определили число $\varphi(n)$ для $n \ge 2$; положим $\varphi(1) = 1$. Таким образом, определена функция $\varphi : \mathbb{N} \to \mathbb{N}$; она называется функцией Эйлера.

Функция $\varphi(n)$ при примарном n. (Число n называется примарным, если оно является степенью простого числа). Пусть p – положительное простое число. Тогда все числа $1, 2, \ldots, p-1$ взаимно просты с p, и потому $\varphi(p) = p-1$. Следующий по трудности случай – это когда $n = p^s$, где число p простое, а $s \ge 1$. Отметим, что число $a \in \mathbb{Z}$ взаимно просто с p^s тогда и только тогда, когда оно не делится на p. Действительно, если $a \div p$, то p – общий делитель a и p^s, а значит, эти числа не взаимно просты. Если же a не делится на простое число p, то a взаимно просто

с p, а потому из произведением p^s нескольких экземпляров p. Таким образом, из множества $X(p^s) = \{0, 1, 2, \ldots, p^s - 1\}$ не взаимно просты с p^s только p^{s-1} чисел

$$0, p, 2p, \ldots, p^s - p = (p^{s-1} - 1)p,$$

а остальные $p^s - p^{s-1}$ чисел этого множества взаимно просты с p^s. Итак,

$$\varphi(p^s) = p^s - p^{s-1} = p^s(1 - 1/p).$$

Декартово произведение множеств. В этом пункте мы напомним одно общематематическое понятие, которое будет нам здесь (и не только здесь) удобно использовать. Пусть X, Y – множества. Их декартовым произведением называется множество $X \times Y$, элементами которого являются всевозможные упорядоченные пары (x, y), первая компонента x которых принадлежит множеству X, а вторая – множеству Y. Итак,

$$X \times Y = \{(x, y) \mid x \in X,\, y \in Y\}.$$

Если $X_0 \subseteq X$, $Y_0 \subseteq Y$, то для любых элементов $x_0 \in X_0$, $y_0 \in Y_0$ упорядоченная пара (x_0, y_0) принадлежит $X \times Y$. Таким образом, $X_0 \times Y_0$ – подмножество $X \times Y$; точнее,

$$X_0 \times Y_0 = \{(x, y) \in X \times Y \mid x \in X_0,\, y \in Y_0\}.$$

Следующее утверждение часто используется в математических рассуждениях.

Пусть X, Y – конечные множества. Тогда декартово произведение $X \times Y$ тоже конечно и $|X \times Y| = |X| \cdot |Y|$.

Все сказанное об утверждении о множествах, связанных биективным отображением, справедливо и теперь. Отметим лишь, что в рамках теории множеств произведение натуральных чисел определяется, грубо говоря, как число элементов некоторого декартова произведения. Все же мы дадим пояснение к последнему утверждению, заставляющее поверить в его справедливость. Пусть $X = \{x_1, \ldots, x_m\}$, $Y = \{y_1, \ldots, y_n\}$. Для каждого i, $1 \le i \le m$, в произведении $X \times Y$ содержится n элементов (x_i, y_j), первая компонента которых равна x_i. Поскольку первая компонента может принимать одно из m значений $x_1, \ldots, x_m$, общее число элементов декартова произведения является суммой m слагаемых, каждое из которых равно n. Эта сумма, конечно, равна mn.

Мультипликативность функции Эйлера. Пусть m, n – взаимно простые натуральные числа. Напомним, что для любого натурального числа N мы обозначаем через $X(N)$ множество всех неотрицательных чисел, меньших N, а через $X'(N)$ – множество состоящее из всех тех чисел из$X(N)$, которые взаимно просты с N. Определим отображение f из множества $X(mn)$ в декартово произведение $(\mathbb{Z}/(m)) \times (\mathbb{Z}/(n))$: если $a \in X(mn)$, то положим $f(a) = ([a]_m, [a]_n)$.

Лемма. *(1). Отображение $f : X(mn) \to (\mathbb{Z}/(m)) \times (\mathbb{Z}/(n))$ биективно.*

(2). Число $a \in X(mn)$ тогда и только тогда принадлежит $X'(mn)$, когда $f(a) \in (\mathbb{Z}/(m))^* \times (\mathbb{Z}/(n))^*$.

Доказательство. (1). *Инъективность.* Пусть $a, b \in X(mn)$ и $f(a) = f(b)$. Это значит, что $([a]_m, [a]_n) = ([b]_m, [b]_n)$, т.е. $[a]_m = [b]_m$, $[a]_n = [b]_n$. Но тогда $a \equiv b \pmod m$ и $a \equiv b \pmod n$, и поэтому $a - b$ делится на взаимно простые числа m, n. Следовательно, $a - b$ делится и на их произведение mn. Но оба числа $a, b \in X(mn)$ положительны и меньше mn; потому $-mn < a - b < mn$, а в этом промежутке на mn делится только число 0. Итак, $a - b = 0$ и $a = b$.

Сюръективность. Пусть $(\beta, \gamma) \in \mathbb{Z}/(m) \times \mathbb{Z}/(n)$, и пусть $b \in \beta$, $c \in \gamma$ – какие-то представители этих классов вычетов. По китайской теореме об остатках, существует число $a' \in \mathbb{Z}$, такое что $a' \equiv b \pmod m$, $a' \equiv c \pmod n$. Пусть a – остаток от деления a' на mn. Тогда $a \in X(mn)$ и $[a]_m = [a']_m = [b]_m = \beta$, $[a]_n = [a']_n = [c]_n = \gamma$, так что $f(a) = ([a]_m, [a]_n) = (\beta, \gamma)$.

(2). Если $a \in X'(mn)$, то a взаимно просто с mn, и, очевидно, a взаимно просто с m и с n, а это значит, что классы $[a]_m$ и $[a]_n$ обратимы, т.е. $[a]_m \in (\mathbb{Z}/(m))^*$, $[a]_n \in (\mathbb{Z}/(n))^*$. Таким образом, $f(a) = ([a]_m, [a]_n) \in (\mathbb{Z}/(m))^* \times (\mathbb{Z}/(n))^*$. Обратно, пусть $([a]_m, [a]_n) = f(a) \in (\mathbb{Z}/(m))^* \times (\mathbb{Z}/(n))^*$; тогда $[a]_m \in (\mathbb{Z}/(m))^*$, $[a]_n \in (\mathbb{Z}/(n))^*$, а это значит, что число a взаимно просто с m и с n. Но тогда a взаимно просто и с произведением mn, т.е. $a \in X'(mn)$.

Предложение 1. *Если m, n – взаимно простые натуральные числа, то $\varphi(mn) = \varphi(m)\varphi(n)$.*

Доказательство. Используя оба варианта определения функции Эйлера, находим, что $\varphi(mn) = |X'(mn)|$, $\varphi(m) = |(\mathbb{Z}/(m))^*|$, $\varphi(n) = |(\mathbb{Z}/(n))^*|$. Из предыдущей леммы следует, что отображение f биективно отображает множество $X'(mn)$ на декартово произведение $(\mathbb{Z}/(m))^* \times (\mathbb{Z}/(n))^*$, поэтому

$$\varphi(mn) = |X'(mn)| = |(\mathbb{Z}/(m))^* \times (\mathbb{Z}/(n))^*| = |(\mathbb{Z}/(m))^*| \cdot |(\mathbb{Z}/(n))^*| = \varphi(m)\varphi(n).$$

Предложение 2. *Если $n_1, n_2, \ldots, n_r$ – попарно взаимно простые натуральные числа, то $\varphi(n_1 n_2 \ldots n_r) = \varphi(n_1)\varphi(n_2)\ldots\varphi(n_r)$.*

Доказательство. Тривиальная индукция по r.

Явная формула для функции Эйлера. Следующая теорема позволяет вычислить значение функции Эйлера от числа n, если мы знаем разложение n в произведение простых множителей, и даже если мы знаем только, на какие простые числа делится n

Теорема 1. *Пусть $n > 1$ – натуральное число, и пусть $p_1, \ldots, p_r$ – все его различные положительные простые делители. Тогда*

$$\varphi(n) = n(1 - \frac{1}{p_1})\ldots(1 - \frac{1}{p_r}).$$

Доказательство. Собирая вместе одинаковые сомножители в разложении числа n в произведение положительных простых чисел, получим, что $n = p_1^{s_1} \ldots p_r^{s_r}$, где $s_1, \ldots, s_r \geq 1$. Если $i \neq j$, то различные простые числа p_i, p_j взаимно просты, а потому взаимно просты и их степени $p_i^{s_i}$, $p_j^{s_j}$. Таким образом, числа $p_1^{s_1}, \ldots, p_r^{s_r}$ попарно взаимно просты, и мы получаем по предложению 2, что $\varphi(n) = \varphi(p_1^{s_1})\ldots\varphi(p_r^{s_r})$. Но мы уже вычислили значение функции Эйлера для случая, когда аргумент – степень простого числа: $\varphi(p_i^{s_i}) = p_i^{s_i}(1 - 1/p_i)$. Таким образом,

$$\varphi(n) = \varphi(p_1^{s_1})\ldots\varphi(p_r^{s_r}) = p_1^{s_1}(1 - \frac{1}{p_1}) \cdot \ldots \cdot p_r^{s_r}(1 - \frac{1}{p_r}) =$$
$$= p_1^{s_1} \cdots p_r^{s_r}(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r}) = n(1 - \frac{1}{p_1})\ldots(1 - \frac{1}{p_r}).$$

10. Теоремы Эйлера, Ферма и Вильсона

Теорема Эйлера. *Пусть $n > 1$ – целое число, и пусть α – обратимый элемент кольца вычетов $\mathbb{Z}/(n)$. Тогда $\alpha^{\varphi(n)} = [1]_n$.*

Доказательство. Обозначим для краткости абелеву группу $(\mathbb{Z}/(n))^*$, состоящую из всех обратимых элементов кольца $\mathbb{Z}/(n)$, через G, а число $\varphi(n)$ – через r. Пусть $\alpha_1, \ldots, \alpha_r$ – все элементы абелевой группы G.

Пусть $\alpha \in G$; определим отображение $f : G \to G$, положив $f(\beta) = \alpha\beta$ для любого $\beta \in G$ (напомним, что G – группа, так что произведение элементов $\alpha, \beta \in G$ снова принадлежит G). Покажем, что отображение f биективно:

сюръективность – если $\beta \in G$, то $\alpha^{-1}\beta \in G$, и $f(\alpha^{-1}\beta) = \alpha\alpha^{-1}\beta = \beta$;

инъективность – если $\beta, \gamma \in G$ и $f(\beta) = f(\gamma)$, то

$$\beta = \alpha^{-1}\alpha\beta = \alpha^{-1}f(\beta) = \alpha^{-1}f(\gamma) = \alpha^{-1}\alpha\gamma = \gamma.$$

Из биективности f следует, что множество $\{f(\alpha_1), \ldots, f(\alpha_r)\}$ состоит из элементов $\alpha_1, \ldots, \alpha_r$, взятых каждый по одному разу, а значит, два произведения $f(\alpha_1)f(\alpha_2)\ldots f(\alpha_r)$ и $\alpha_1\alpha_2\ldots\alpha_r$ отличаются лишь порядком сомножителей. Но группа G абелева, так что произведение не зависит от порядка сомножителей, и мы получаем:

$$\alpha_1\alpha_2\ldots\alpha_r = f(\alpha_1)f(\alpha_2)\ldots f(\alpha_r) = (\alpha\alpha_1)(\alpha\alpha_2)\ldots(\alpha\alpha_r) = \alpha^r(\alpha_1\alpha_2\ldots\alpha_r).$$

Домножив обе части последнего равенства на элемент $\gamma = (\alpha_1\alpha_2\ldots\alpha_r)^{-1}$, получим: $[1]_n = (\alpha_1\alpha_2\ldots\alpha_r)\gamma = \alpha^r(\alpha_1\alpha_2\ldots\alpha_r)\gamma = \alpha^r$, что мы и хотели доказать.

Следствие. *Пусть a, n – целые числа, причем $n > 1$, а число a взаимно просто с n. Тогда $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Доказательство. Поскольку a и n взаимно просты, класс вычетов $[a]_n$ обратим в кольце $\mathbb{Z}/(n)$, и потому по теореме Эйлера будет $[a^{\varphi(n)}]_n = [a]_n^{\varphi(n)} = [1]_n$, а это и значит, что $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Отметим, что сам Л.Эйлер доказал именно это утверждение.

Частным случаем теоремы Эйлера является

Малая теорема Ферма. *Пусть p – положительное простое число.*
(1). Если α – ненулевой элемент поля вычетов $\mathbb{Z}/(p)$, то $\alpha^{p-1} = [1]_p$.
(2). Для любого $\alpha \in \mathbb{Z}/(p)$ будет $\alpha^p = \alpha$.

Доказательство. (1). Поскольку $\varphi(p) = p - 1$, утверждение следует из теоремы Эйлера.

(2). Если $\alpha \in \mathbb{Z}/(p)$, $\alpha \neq 0$, то $\alpha^{p-1} = [1]_p$ по первому утверждению теоремы. Умножая обе части на α, получаем соотношение $\alpha^p = \alpha$, которое, очевидно, верно и для исключенного ранее случая $\alpha = [0]_p$.

Следствие. *Пусть p – положительное простое число. Если целое число a не делится на p, то $a^{p-1} \equiv 1 \pmod{p}$. Для любого целого числа a выполняется сравнение $a^p \equiv a \pmod{p}$.*

Это следствие выводится из малой теоремы Ферма так же, как предыдущее следствие выводилось из теоремы Эйлера.

Теорема Вильсона. *Пусть p – положительное простое число. Тогда произведение всех ненулевых элементов поля $\mathbb{Z}/(p)$ равно $[-1]_p$.*

Доказательство. Сначала докажем простую лемму.

Лемма. *Если $\alpha \neq 0$ – элемент поля $\mathbb{Z}/(p)$, и $\alpha \neq [\pm 1]_p$, то $\alpha \neq \alpha^{-1}$.*

Доказательство. Если $\alpha = \alpha^{-1}$, то $\alpha^2 - [1]_p = [0]_p$, и потому $(\alpha - [1]_p)(\alpha + [1]_p) = 0$. Но в поле произведение элементов нулевое лишь тогда, когда один из сомножителей нулевой. Таким образом, должно выполняться одно из равенств $\alpha - [1]_p = [0]_p$, $\alpha + [1]_p = [0]_p$.

Вернемся к доказательству теоремы Вильсона. Если $p = 2$, то $[-1]_2 = [1]_2$, и утверждение тривиально. Пусть $p \geq 3$; все ненулевые элементы поля $\mathbb{Z}/(p)$, отличные от элементов $[\pm 1]_p$, разбиваются на непересекающиеся пары, состоящие из элемента α и обратного к нему элемента α^{-1}. Произведение элементов каждой такой пары равно $[1]_p$, а потому произведение всех элементов поля $\mathbb{Z}/(p)$, отличных от $[0]_p$, $[\pm 1]_p$, равно $[1]_p$. Следовательно, произведение всех ненулевых элементов поля $\mathbb{Z}/(p)$ равно $[1]_p \cdot [-1]_p \cdot [1]_p = [-1]_p$.

Поскольку $[1]_p, [2]_p, \ldots, [p-1]_p$ – это все ненулевые элементы поля $\mathbb{Z}/(p)$, мы получаем по теореме Вильсона, что

$$[(p-1)!]_p = [1 \cdot 2 \cdot \ldots \cdot (p-1)] = [1]_p[2]_p \ldots [p-1]_p = [-1]_p,$$

и тем самым доказано

Следствие. *Пусть p – положительное простое число. Тогда $(p-1)!+1$ делится на p.*

11. Сравнения первой степени с одной неизвестной

Сравнения первой степени и их решения. Сравнением первой степени с неизвестной x над кольцом A называется выражение вида $ax \equiv b \pmod{n}$, где $a, b, n \in A$. Отметим, что написанное выражение не надо воспринимать содержательно: оно не означает, что линейный двучлен $ax - b$ делится на n. Оно представляет собой просто слово определенного вида в алфавите, состоящем из элементов кольца A и пяти графических знаков

$$x \qquad \equiv \qquad \mathrm{mod} \qquad (\qquad)$$

Решением сравнения $ax \equiv b \pmod{n}$ называется элемент $x_0 \in A$, такой что $ax_0 \equiv b \pmod{n}$. Последнее сравнение уже воспринимается содержательно: оно означает, что два элемента ax_0 и b кольца A сравнимы по модулю n, т.е. что их разность $ax_0 - b$ делится в кольце A на n.

Естественно возникают вопросы: при каких условиях сравнение разрешимо? если оно разрешимо, то как устроено множество всех решений? как найти все решения?

Условие разрешимости сравнения. Следующая теорема дает полный ответ на первые два вопроса.

Теорема 1. *Пусть A – область главных идеалов, $a, b, n \in A$; далее, пусть d – наибольший общий делитель a и n, а $n_1 \in A$ таково, что $n = dn_1$.*

(1) Сравнение $ax \equiv b \pmod{n}$ разрешимо тогда и только тогда, когда b делится на d.

(2) Если $x_0 \in A$ – решение сравнения $ax \equiv b \pmod{n}$, то элемент $x_1 \in A$ является решением этого сравнения тогда и только тогда, когда $x_1 \equiv x_0 \pmod{n}$.

Доказательство. (1). Пусть $x_0 \in A$ – решение сравнения $ax \equiv b \pmod{n}$; тогда $b \equiv ax_0 \pmod{n}$, и тем более $b \equiv ax_0 \pmod{d}$, потому что $n \div d$. Но a тоже делится на d, поэтому $b \equiv 0 \cdot x_0 = 0 \pmod{d}$, и $b \div d$. Обратно, пусть $b \div d$ и пусть $b_1 \in A$ – такой элемент, что $b = b_1 d$. Поскольку d – наибольший общий делитель a и n, по теореме 4.1,(4) существует такой элемент $z_0 \in A$, что $az_0 \equiv d \pmod{n}$; но тогда $a(b_1 z_0) \equiv b_1 d = b \pmod{n}$, т.е. $x_0 = b_1 z_0$ – решение нашего сравнения $ax \equiv b \pmod{n}$.

(2) Пусть $a_1 \in A$ таково, что $a = da_1$. Легко видеть, что a_1, n_1 взаимно просты. Действительно, из того, что d – наибольший общий делитель $a = da_1$ и $n = dn_1$, следует, что существуют такие элементы $z_0, u_0 \in A$, что $d = da_1 z_0 + dn_1 u_0$. Сокращая на d (ведь A – область целостности), получаем, что $1 = a_1 z_0 + n_1 u_0$, откуда и следует, что 1 является наибольшим общим делителем a_1 и n_1.

Пусть теперь $x_0, x_1 \in A$ – решения сравнения $ax \equiv b \pmod{n}$. Тогда

$$da_1 x_1 \equiv b \equiv da_1 x_0 \pmod{dn_1},$$

откуда следует, что $a_1 x_1 \equiv a_1 x_0 \pmod{n_1}$. Но a_1 и n_1 взаимно просты, и потому существует такой элемент $q \in A$, что $qa_1 \equiv 1 \pmod{n_1}$. Следовательно,

$$x_1 = 1 \cdot x_1 \equiv qa_1 x_1 \equiv qa_1 x_0 \equiv 1 \cdot x_0 = x_0 \pmod{n_1}.$$

Обратно, если $ax_0 \equiv b \pmod{n}$ и $x_1 \equiv x_0 \pmod{n_1}$, то $dx_1 \equiv dx_0 \pmod{dn_1}$, т.е. $dx_1 \equiv dx_0 \pmod{n}$. Тогда $ax_1 = a_1dx_1 \equiv a_1dx_0 = ax_0 \equiv b \pmod{n}$, т.е. x_1 – тоже решение сравнения $ax \equiv b \pmod{n}$.

Решение сравнений над $\mathbb{Z}$. Пусть $a, b, n \in \mathbb{Z}$, причем $a \neq 0$, $n \neq 0$, и пусть сравнение. $ax \equiv b \pmod{n}$ разрешимо. Обозначим через d наибольший общий делитель чисел a и n; по теореме 1, число b тоже делится на d. Существуют такие целые числа a_1, b_1, n_1, что $a = da_1$, $b = db_1$, $n = dn_1$; выше мы увидели, что $(a_1, n_1) = (1)$.

Мы укажем сейчас два алгорифма нахождения решений нашего сравнения.

1. Пользуясь алгорифмом Евклида, найдем наибольший общий делитель d чисел a и n и его линейное представление $d = au + nv$, где u, v – некоторые целые числа. Тогда b_1u – одно из решений сравнения $ax \equiv b \pmod{n}$. Действительно, $a(b_1u) = b_1(au) = b_1(d - nv) \equiv b_1d = b \pmod{n}$.

2. Поскольку числа a_1 и n_1 взаимно просты, по теореме Эйлера получаем, что $a_1^{\varphi(n_1)} \equiv 1 \pmod{n_1}$; поэтому

$$a_1(b_1a_1^{\varphi(n_1)-1}) = b_1a_1^{\varphi(n_1)} \equiv b_1 \pmod{n_1}.$$

Умножив обе части и модуль получившегося сравнения на d, получим, что $a(b_1a_1^{\varphi(n_1)-1}) \equiv b \pmod{n_1}$. Таким образом, $b_1a_1^{\varphi(n_1)-1}$ – одно из решений сравнения $ax \equiv b \pmod{n}$.

Зная частное решение $x_0 = b_1u$ или $x_0 = b_1a_1^{\varphi(n_1)-1}$, общее решение найдем по формуле $x_1 = x_0 + kn_1$, где k – любое целое число.

Уравнения первой степени над кольцом вычетов. Пусть $n \neq 0$ – целое число. Уравнением над кольцом $\mathbb{Z}/(n)$ называется выражение вида $\alpha x = \beta$, где $\alpha, \beta \in \mathbb{Z}/(n)$. Решением этого уравнения называется элемент $\xi \in A$, такой что $\alpha\xi = \beta$.

Теорема 2. *Пусть a, b, n – целые числа, причем $n \neq 0$. Обозначим через d положительный наибольший общий делитель a и n. Уравнение $[a]_nx = [b]_n$ разрешимо тогда и только тогда, когда $b \div d$. Если уравнение разрешимо, то оно имеет в точности d решений.*

Доказательство. Класс $\xi = [x_0]_n$ является решением уравнения тогда и только тогда, когда $ax_0 \equiv b \pmod{n}$, т.е. когда x_0 – решение сравнения $ax \equiv b \pmod{n}$. По теореме 1 такое число x_0 существует тогда и только тогда, когда $b \div d$. Обозначим через n_1 число n/d. Если существует решение $[x_0]_n$, то произвольное решение уравнения имеет вид $[x_0 + kn_1]_n$, где $k \in \mathbb{Z}$. Очевидно, следующие d решений различны:

$$[x_0]_n,\ [x_0 + n_1]_n,\ [x_0 + 2n_1]_n,\ \dots\ ,\ [x_0 + (d-1)n_1]_n.$$

Если k – произвольное целое число, то обозначим через q, r неполное частное и остаток от деления k на d, так что $k = r + dq$, $0 \leq r < d$. Тогда

$$x_0 + kn_1 = x_0 + rn_1 + qdn_1 = x_0 + rn_1 + qn \equiv x_0 + rn_1 \pmod{n},$$

и поэтому $[x_0 + kn_1]_n = [x_0 + rn_1]_n$, т.е. решение $[x_0 + kn_1]_n$ совпадает с одним из перечисленных выше d решений.

Диофантовы уравнения первой степени. Как правило, одного уравнения недостаточно для того, чтобы определить значения двух неизвестных величин. Ситуация меняется, если на неизвестные накладываются дополнительные ограничения. Например, можно потребовать, чтобы решение целыми или даже натуральными числами. Алгебраическое уравнение для по крайней мере двух неизвестных называется диофантовым, если требуется найти лишь целочисленные решения этого уравнения.

Простейшим диофантовым уравнением является уравнение первой степени с двумя неизвестными величинами. Такое уравнение имеет вид $ax+by=c$, где a, b, c – целые числа. Пара целых чисел (x_0, y_0) называется решением этого диофантова уравнения, если выполняется числовое равенство $ax_0+by_0=c$. Если (x_0, y_0) – решение нашего диофантова уравнения, то $ax_0 \equiv c \pmod b$, т.е. x_0 – решение сравнения $ax \equiv c \pmod b$. Обратно, если x_0 – решение сравнения $ax \equiv c \pmod b$, то $ax_0 - c \vdots b$, и потому существует такое целое число y_0, что $ax_0 - c = by_0$, так что $ax_0 + b(-y_0) = c$, и $(x_0, -y_0)$ – решение уравнения $ax+by=c$. Поскольку для разрешимости сравнения $ax \equiv c \pmod b$ необходимо и достаточно, чтобы число c делилось на наибольший общий делитель чисел a и b, то же условие необходимо и достаточно для существования решения диофантова уравнения $ax+by=c$.

Опишем множество всех решений диофантова уравнения $ax+by=c$, предполагая для простоты, что a и b взаимно просты. Пусть (x_0, y_0) – какое-то решение уравнения, и пусть (x_1, y_1) – его произвольное решение. Тогда x_1 решает сравнение $ax \equiv c \pmod b$, и потому $x_1 = x_0 + kb$ для некоторого $k \in \mathbb{Z}$; подставляя это значение в диофантово уравнение и учитывая, что $ax_0 + by_0 = c$, находим:

$$c = a(x_0 + kb) + by_1 = ax_0 + by_0 + b(y_1 - y_0 + ak) = c + b(y_1 - y_0 + ak),$$

откуда получаем, что $y_1 = y_0 - ka$. Итак, если (x_0, y_0) – одно из решений диофантова уравнения $ax+by=c$, то произвольное решение уравнения имеет вид $(x_0 + kb, y_0 - ka)$.

Если дополнительно потребовать, чтобы решение уравнения давалось неотрицательными числами, то иногда решение диофантова уравнения может оказаться единственным. Решим для примера следующую задачу. В кульке ровно 500 г конфет двух сортов; одна конфета в красном фантике весит 14 г, а одна конфета в синем фантике весит 23 г. Сколько в кульке конфет каждого из сортов? Задача сводится к решению в натуральных числах уравнения

$$14x + 23y = 500.$$

Найдем частное решение этого уравнения. Число y должно удовлетворять сравнению $23y \equiv 500 \pmod{14}$. Заменяя коэффициент 23 при y на сравнимый с ним по модулю 14 коэффициент -5, получим сравнение $-5y \equiv 500 \pmod{14}$, которое имеет очевидное решение $y_0 = -100$. Подставив y_0 в наше уравнение, найдем соответствующее ему значение переменной x:

$$x_0 = (500 - 23y_0)/14 = (500 + 2300)/14 = 200.$$

Итак, мы нашли частное решение уравнения $(200, -100)$; общее решение имеет вид $(200 + 23k, -100 - 14k)$, где k – целое число. Поскольку по смыслу задачи обе переменные должны быть неотрицательны, получаем для k неравенства $200 + 23k > 0$, $-100 - 14k > 0$, откуда следует, что $-200/23 < k < -100/14$. Единственным целым числом k, удовлетворяющим этим неравенствам, является -8. Таким образом, $x_1 = 200 + 23 \cdot (-8) = 16$, $y_1 = -100 - 14 \cdot (-8) = 12$ и есть единственное решение нашей задачи.

12. Сравнения второй степени с одной неизвестной

Сравнения второй степени. В этом и следующем параграфах мы выясняем условия разрешимости в целых числах сравнения $x^2 \equiv a \pmod n$, где a и $n > 1$ – целые числа. При этом мы будем предполагать, что a и n взаимно просты; общий случай в значительной степени сводится к этому при помощи несложного анализа, однако формулировки становятся громоздкими и не очень поучительными. Целью этого параграфа является сведение проблемы к случаю нечетного простого модуля.

Выше мы определили, что такое решение сравнения первой степени. Аналогично этому, число $x_0 \in \mathbb{Z}$ называется решением сравнения $x^2 \equiv a \pmod{n}$, если целые числа x_0^2, a сравнимы по модулю n.

Сведение к случаю примарного модуля. Благодаря следующей теореме мы сведем случай произвольного модуля n к случаям $n = 2^s$ и $n = p^s$, где p – нечетное простое число. Эти случаи будут разобраны в следующих пунктах.

Теорема 1. *Пусть $n = p_1^{s_1} \cdots p_r^{s_r}$, где p_1, ... , p_r – попарно различные положительные простые числа, и пусть $a \in \mathbb{Z}$. Сравнение $x^2 \equiv a \pmod{n}$ разрешимо тогда и только тогда, когда разрешимы все сравнения $x^2 \equiv a \pmod{p_1^{s_1}}$, ... , $x^2 \equiv a \pmod{p_r^{s_r}}$.*

Доказательство. Пусть все сравнения $x^2 \equiv a \pmod{p_1^{s_1}}$, ... , $x^2 \equiv a \pmod{p_r^{s_r}}$ разрешимы, и пусть x_i – решение сравнения $x^2 \equiv a \pmod{p_i^{s_i}}$ $(1 \le i \le r)$. Поскольку при $i \ne j$ простые числа p_i и p_j различны, они взаимно просты, а значит, взаимно просты и их степени. Таким образом, числа $p_1^{s_1}, \ldots, p_r^{s_r}$ попарно взаимно просты. По китайской теореме об остатках существует целое число x_0, такое что $x_0 \equiv x_i \pmod{p_i^{s_i}}$ для всех i, $(1 \le i \le r)$. Но тогда $x_0^2 \equiv x_i^2 \equiv a \pmod{p_i^{s_i}}$ для всех i. Значит, число $x_0^2 - a$ делится на каждое из попарно взаимно простых чисел $p_1^{s_1}, \ldots, p_r^{s_r}$, а потому делится и на их произведение $p_1^{s_1} \cdots p_r^{s_r} = n$. Таким образом, $x_0^2 \equiv a \pmod{n}$, т.е. x_0 – решение сравнения $x^2 \equiv a \pmod{n}$.

Наоборот, если сравнение $x^2 \equiv a \pmod{n}$ разрешимо, и x_0 – его решение, то x_0 решает и каждое из сравнений $x^2 \equiv a \pmod{p_i^{s_i}}$, $1 \le i \le r$.

Сравнение $x^2 \equiv a \pmod{2^s}$.

Теорема 2. *Пусть a – нечетное число.*

(1) *Сравнение $x^2 \equiv a \pmod{2}$ разрешимо.*

(2) *Сравнение $x^2 \equiv a \pmod{4}$ разрешимо тогда и только тогда, когда a сравнимо с 1 по модулю 4.*

(3) *Если $s \ge 3$, то сравнение $x^2 \equiv a \pmod{2^s}$ разрешимо тогда и только тогда, когда a сравнимо с 1 по модулю 8.*

Доказательство. Заметим сначала, что квадрат любого нечетного числа сравним с 1 по модулю 8. В самом деле, если u нечетно, то u сравнимо по модулю 8 с одним из чисел 1, 3, 5, 7, а потому число u^2 сравнимо по модулю 8 с одним из чисел $1^2 = 1$, $3^2 = 9$, $5^2 = 25$, $7^2 = 49$; но все эти квадраты при делении на 8 дают остаток 1. Отсюда сразу следует необходимость условий утверждений (2) и (3). Утверждение (1) и достаточность условия в утверждении (2) тривиальны. Поэтому остается доказать лишь, что если $s \ge 3$, $a \equiv 1 \pmod{8}$, то сравнение $x^2 \equiv a \pmod{2^s}$ разрешимо.

Последнее утверждение будем доказывать индукцией по s. Случай $s = 3$ тривиален. Пусть $s > 3$ и пусть уже найдено число $y_0 \in \mathbb{Z}$, такое что $y_0^2 \equiv a \pmod{2^{s-1}}$. Если $y_0^2 \equiv a \pmod{2^s}$, то y_0 является решением и для сравнения $x^2 \equiv a \pmod{2^s}$. Если же $y_0^2 \not\equiv a \pmod{2^s}$, то остаток от деления $y_0^2 - a$ на 2^s равен 2^{s-1}, потому что он не равен 0, меньше числа 2^s и делится на 2^{s-1}; поэтому $y_0^2 \equiv a + 2^{s-1} \pmod{2^s}$. Положим $x_0 = y_0 + 2^{s-2}$; заметив, что число y_0, очевидно, нечетно, а потому представимо в виде $y_0 = 2k + 1$, и что $2(s-2) \ge s$, получаем:

$$x_0^2 = (y_0 + 2^{s-2})^2 = y_0^2 + 2 \cdot 2^{s-2} y_0 + 2^{2(s-2)} \equiv y_0^2 + 2^{s-1}(2k+1) \equiv$$
$$\equiv a + 2^{s-1} + (2^{s-1} \cdot 2k + 2^{s-1}) \equiv a \pmod{2^s}.$$

Таким образом, мы построили решение x_0 сравнения $x^2 \equiv a \pmod{2^s}$.

Сравнение $x^2 \equiv a \pmod{p^s}$, где p – нечетное простое.

Теорема 3. *Пусть p – нечетное простое число, $s \geq 1$, и пусть a – целое число, не делящееся на p. Сравнение $x^2 \equiv a \pmod{p^s}$ разрешимо тогда и только тогда, когда разрешимо сравнение $x^2 \equiv a \pmod{p}$.*

Доказательство. Необходимость очевидна; достаточность докажем индукцией по s. Если $s = 1$, то утверждение теоремы становится тавтологией. Пусть $s > 1$, и пусть уже найдено число $y_0 \in \mathbb{Z}$, такое что $y_0^2 \equiv a \pmod{p^{s-1}}$. Решение x_0 сравнения $x^2 \equiv a \pmod{p^s}$ будем искать в форме $x_0 = y_0 + bp^{s-1}$. Поскольку $2(s-1) \geq s$, находим, что $x_0^2 = y_0^2 + 2y_0p^{s-1} \cdot b + b^2p^{2(s-1)} \equiv y_0^2 + 2y_0p^{s-1} \cdot b \pmod{p^s}$. Поэтому для того, чтобы число x_0^2 было сравнимо с a по модулю p^s, необходимо и достаточно, чтобы выполнялось сравнение $y_0^2 + 2y_0p^{s-1} \cdot b \equiv a \pmod{p^s}$, которое эквивалентно сравнению $(2y_0p^{s-1})b \equiv (a - y_0^2) \pmod{p^s}$. Остается доказать, что последнее сравнение разрешимо относительно b, т.е. что свободный член этого сравнения $a - y_0^2$ делится на наибольший общий делитель коэффициента $2y_0p^{s-1}$ и модуля p^s. Но это так: очевидно, что y_0 и 2 взаимно просты с p, и поэтому p^{s-1} является наибольшим общим делителем $2y_0p^{s-1}$ и p^s, а число $a - y_0^2$ делится на p^{s-1}, потому что $y_0^2 \equiv a \pmod{p^{s-1}}$.

13. Символ квадратичного вычета и теорема взаимности

Символ квадратичного вычета. Пусть $p > 0$ – нечетное простое число, и пусть a – целое число, не делящееся на p. Определим символ $\left(\dfrac{a}{p}\right)$, положив

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если сравнение } x^2 \equiv a \pmod{p} \quad \text{имеет решенин;} \\ -1, & \text{если сравнение } x^2 \equiv a \pmod{p} \quad \text{не имеет решений.} \end{cases}$$

Этот символ называется символом Лежандра, или символом квадратичного вычета. Мы говорим, что число a является квадратичным вычетом по модулю p (квадратичным невычетом по модулю p), если $\left(\dfrac{a}{p}\right) = 1$ (соответственно, $\left(\dfrac{a}{p}\right) = -1$).

Отметим здесь простейшие свойства символа квадратичного вычета.

(1) *Если целые числа a, b не делятся на p, то $\left(\dfrac{ab^2}{p}\right) = \left(\dfrac{a}{p}\right)$.*

(2) *Если $a, b \in \mathbb{Z}$, a не делится на p и $a \equiv b \pmod{p}$, то $\left(\dfrac{a}{p}\right) = \left(\dfrac{b}{p}\right)$.*

Благодаря свойству (2), вместе с элементом a весь класс вычетов $[a]$ состоит из квадратичных вычетов или квадратичных невычетов.

(3) *Число классов квадратичных вычетов по модулю p и число классов квадратичных невычетов по модулю p оба равны $(p-1)/2$.*

Доказательство. Всего имеется $p - 1$ классов вычетов по модулю p, состоящих из элементов, не делящихся на p – это классы $[1], [2], \ldots, [p-1]$. Класс $[a]$ состоит из квадратичных вычетов тогда и только тогда, когда он является квадратом в поле $\mathbb{Z}/(p)$. Таким образом, из квадратичных вычетов состоят следующие $(p-1)/2$ классов

$$[1]^2 = [(p-1]^2,\ [2]^2 = [p-2]^2,\ \ldots\ [(p-1)/2]^2 = [(p+1)/2]^2,$$

и только они. Поэтому остальные $(p-1)/2$ классов состоят из квадратичных невычетов.

(4) *Если $a \in \mathbb{Z}$, a не делится на p, то $a^{(p-1)/2} \equiv \left(\dfrac{a}{p}\right) \pmod{p}$.*

Доказательство. Иначе говоря, утверждение гласит: если класс $\alpha \in \mathbb{Z}/(p)$ состоит из квадратичных вычетов, то $\alpha^{(p-1)/2} = [1]$, а если он состоит из квадратичных невычетов, то $\alpha^{(p-1)/2} = -[1]$. Первое утверждение следует из малой теоремы Ферма: если класс $\alpha \in \mathbb{Z}$ состоит из квадратичных вычетов, то существует класс $\beta \in \mathbb{Z}/(p)$, такой что $\alpha = \beta^2$, и $\alpha^{(p-1)/2} = \beta^{p-1} = [1]$.

Нам придется сейчас воспользоваться одним общим фактом о корнях многочленов над полем, который будет доказан в следующей главе.

Если K – поле, то для многочлена степени $n > 0$ с коэффициентами из K существует не более n элементов поля K, в которых значение многочлена равно 0.

Применяя это утверждение к многочлену $x^{(p-1)/2} - [1]$ над полем $\mathbb{Z}/(p)$, получаем, что существует не более $(p-1)/2$ классов $\alpha \in \mathbb{Z}/(p)$, таких что $\alpha^{(p-1)/2} = [1]$. Но мы уже знаем, что все $(p-1)/2$ классов квадратичных вычетов обладают этим свойством; поэтому ни один класс, не состоящий из квадратичных вычетов, не удовлетворяет этому условию. Таким образом, если класс α состоит из квадратичных невычетов, то $\alpha^{(p-1)/2} \neq [1]$. Но по малой теореме Ферма все же будет

$$[0] = \alpha^{p-1} - [1] = (\alpha^{(p-1)/2} - [1])(\alpha^{(p-1)/2} + [1]),$$

и, поскольку первый сомножитель отличен от $[0]$, а кольцо $\mathbb{Z}/(p)$ является полем и тем более областью целостности, в $[0]$ обращается второй сомножитель. Итак, если класс α состоит из квадратичных невычетов, то $\alpha^{(p-1)/2} + [1] = [0]$.

Мультипликативность символа квадратичного вычета. Из предыдущей формулы легко вывести следующее важное свойство.

(5) *Если a, b – не делящиеся на p целые числа, то* $\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$.

Доказательство. По свойству (4)

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Остается заметить, что в левой и правой частях сравнения стоят числа ± 1, которые сравнимы по модулю $p \geq 3$ только если они равны.

Выражение символа квадратичного вычета при помощи наименьших вычетов. До сих пор в качестве представителей классов вычетов по модулю n мы всегда выбирали числа от 0 до n. Но часто бывает полезно использовать и другие полные системы вычетов. Если в каждом классе выбрать наименьший по абсолютной величине представитель, то при нечетном n всё кольцо $\mathbb{Z}/(n)$ будет состоять из классов $[0]$, $\pm[1]$, $\ldots$, $\pm[(n-1)/2]$.

Воспользуемся этой системой представителей для того, чтобы получить еще одну формулу для символа квадратичного вычета.

(6) *Пусть $a \in \mathbb{Z}$, причем a не делится на p. Для каждого i, $1 \leq i < p/2$, пусть ε_i, $u_i \in \mathbb{Z}$ таковы что $\varepsilon_i = \pm 1$, $1 \leq u_i < p/2$ и $[ai] = \varepsilon_i [u_i]$. Тогда* $\left(\dfrac{a}{p}\right) = \varepsilon_1 \varepsilon_2 \ldots \varepsilon_r$, *где через r для краткости обозначено число $(p-1)/2$.*

Доказательство. Заметим сначала, что такие ε_i, u_i существуют и единственны. Действительно, поскольку a и i не делятся на p, класс $[ai]$ ненулевой; если v_i наименьший по абсолютной величине представитель класса $[ai]$, то ε_i равно 1 или -1 в зависимости от того, положительно или отрицательно число v_i, а $u_i = |v_i|$.

Дальнейшие рассуждения напоминают доказательство теоремы Эйлера. Докажем сначала, что при $1 \leq i, j < p/2$ и $i \neq j$ числа u_i, u_j различны. Действительно, если $u_i = u_j$, то $[ai] = \varepsilon_i [u_i] = \pm \varepsilon_j [u_j] = \pm [aj]$, т.е. $a(i+j) = ai + aj \equiv 0 \pmod{p}$ или $a(i-j) = ai - aj \equiv 0 \pmod{p}$. Поскольку a не делится на простое число p,

это означает, что одно из чисел $i+j$, $i-j$ делится на p. Но при $1 \le i, j < p/2$ мы имеем: $2 \le i+j < p$, $-p < i-j < p$, так что число $i+j$ не делится на p, а $i-j$ может делиться на p лишь если $i-j=0$, т.е. если $i=j$.

Таким образом, r чисел $u_1, u_2, \ldots, u_r$ различны; но каждое из них совпадает с одним из r чисел $1, 2, \ldots, r$. Поэтому среди чисел u_i встречается каждое из чисел $1, 2, \ldots, r$, причем ровно по одному разу. Значит, $u_1 u_2 \ldots u_r = 1 \cdot 2 \cdot \ldots \cdot r = r!$.

Теперь мы получаем:

$$r!\left(\frac{a}{p}\right) \equiv r!a^r = (a \cdot 1)(a \cdot 2)\ldots(a \cdot r) \equiv (\varepsilon_1 u_1)(\varepsilon_2 u_2)\ldots(\varepsilon_r u_r) =$$
$$= \varepsilon_1 \varepsilon_2 \ldots \varepsilon_r \cdot u_1 u_2 \ldots u_r = r!\varepsilon_1 \varepsilon_2 \ldots \varepsilon_r \pmod p.$$

Значит, разность $\left(\frac{a}{p}\right) - \varepsilon_1 \varepsilon_2 \ldots \varepsilon_r$, умноженная на $r!$, делится на p; но $r!$ не делится на p, поэтому на p делится разность $\left(\frac{a}{p}\right) - \varepsilon_1 \varepsilon_2 \ldots \varepsilon_r$. Каждое из чисел $\left(\frac{a}{p}\right)$ и $\varepsilon_1 \varepsilon_2 \ldots \varepsilon_r$ равно ± 1; следовательно, предыдущая разность может принимать лишь значения -2, 0, 2, из которых на $p \ge 3$ делится лишь 0. Итак, мы доказали, что

$$\left(\frac{a}{p}\right) - \varepsilon_1 \varepsilon_2 \ldots \varepsilon_r = 0.$$

Еще одна формула для символа. Для дальнейшего преобразования нашей формулы для символа квадратичного вычета нам понадобится функция, которая сопоставляет каждому вещественному числу x наибольшее целое число $[x]$, не превосходящее x. Например, $[5/2] = 2$, ([-1]=1), $[-3,1] = -4$. К сожалению, традиционное обозначение этой функции, называемой "целая часть x"или "антье от x"(от французского entier, что означает "целый"), совпадает с нашим обозначением для класса вычетов, содержащего некоторое целое число. Однако, из контекста всегда будет ясно, какой именно смысл мы придаем квадратным скобкам, так что недоразумения не возникнут.

Заметим, что $\varepsilon_i = 1$, если существует такое целое число k, что $kp < ai < kp + p/2$, т.е. $2k < 2ai/p < 2k+1$. Таким образом, $\varepsilon_i = 1$, если $[2ai/p]$ четно. Аналогично, $\varepsilon_i = -1$, если существует такое целое число k, что $kp + p/2 < ai < kp + p$, т.е. $2k+1 < 2ai/p < 2k+2$, откуда следует, что $[2ai/p]$ нечетно. В обоих случаях $\varepsilon = (-1)^{[2ai/p]}$, и мы получаем новый вариант формулы для символа квадратичного вычета.

(7) *Пусть $a \in \mathbb{Z}$, причем a не делится на p. Тогда*

$$\left(\frac{a}{p}\right) = (-1)^{\left[\frac{2a\cdot 1}{p}\right] + \left[\frac{2a\cdot 2}{p}\right] + \cdots + \left[\frac{2a\cdot r}{p}\right]}.$$

Символ $\left(\frac{a}{p}\right)$ при нечетном a и при $a=2$. Если a нечетно, то мы можем получить формулу, более удобную, чем формула из (7). Заодно получится явная формула для значения символа при $a=2$.

(8) *Если целое число a нечетно и не делится ни на p, то*

$$\left(\frac{a}{p}\right) = (-1)^{\left[\frac{1\cdot a}{p}\right] + \left[\frac{2a}{p}\right] + \cdots + \left[\frac{ra}{p}\right]}.$$

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

Доказательство. Если a нечетно, то $p+a$ четно. Пользуясь свойствами (2), (5) и (7), а также тем тривиальным фактом, что $[n+x]=n+[x]$ для любого целого n, получаем:

$$\left(\frac{a}{p}\right)=\left(\frac{p+a}{p}\right)=\left(\frac{2}{p}\right)=\left(\frac{(p+a)/2}{p}\right)=\left(\frac{2}{p}\right)\cdot(-1)^{\left[\frac{p+a}{p}\right]+\left[\frac{2p+2a}{p}\right]+\dots+\left[\frac{rp+ra}{p}\right]}=$$
$$=A\cdot(-1)^{\left[\frac{1\cdot a}{p}\right]+\left[\frac{2a}{p}\right]+\dots+\left[\frac{ra}{p}\right]},$$

где $A=\left(\frac{2}{p}\right)\cdot(-1)^{1+2+\dots+\frac{p-1}{2}}=\left(\frac{2}{p}\right)\cdot(-1)^{\frac{p^2-1}{8}}$. Покажем, что $A=1$, чем будет доказано свойство (8). Для этого в предыдущем равенстве положим $a=1$; поскольку $\left(\frac{1}{p}\right)=1$, а $[i/p]=0$ для всех i, $1\le i\le r$, мы получим соотношение $1=A\cdot 1$, что и надо было. С другой стороны, из только что доказанного равенства $\left(\frac{2}{p}\right)\cdot(-1)^{\frac{p^2-1}{8}}=1$ следует, что $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$, а это и есть утверждение (9).

Закон взаимности Гаусса.

Теорема 1. *Пусть p, q – нечетные положительные простые числа. Тогда*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Доказательство. Пусть $r=(p-1)/2$, $s=(q-1)/2$. Поскольку

$$\left(\frac{p}{q}\right)=(-1)^{\left[\frac{1\cdot p}{q}\right]+\left[\frac{2p}{q}\right]+\dots+\left[\frac{sp}{q}\right]},\qquad \left(\frac{q}{p}\right)=(-1)^{\left[\frac{1\cdot q}{p}\right]+\left[\frac{2q}{p}\right]+\dots+\left[\frac{rq}{p}\right]},$$

достаточно доказать, что

$$\left(\left[\frac{1\cdot p}{q}\right]+\left[\frac{2p}{q}\right]+\dots+\left[\frac{sp}{q}\right]\right)+\left(\left[\frac{1\cdot q}{p}\right]+\left[\frac{2q}{p}\right]+\dots+\left[\frac{rq}{p}\right]\right)=\frac{p-1}{2}\cdot\frac{q-1}{2}.$$

Но это становится очевидным, если интерпретировать это равенство геометрически. Рассмотрим на плоскости прямоугольник с вершинами $O=(0,0)$, $A=(q,0)$, $B=(0,p)$, $C=(q,p)$. Число S точек с целыми координатами внутри этого прямоугольника (не включая границы) равно, очевидно, $\frac{p-1}{2}\cdot\frac{q-1}{2}$. С другой стороны, это число разбивается в сумму трех слагаемых: число S_1 точек с целыми координатами внутри треугольника OAC, число S_2 точек с целыми координатами внутри треугольника OBC и число S_3 точек с целыми координатами на диагонали OC (не считая граничную точку диагонали O).

Покажем, $S_3=0$, т.е. что на диагонали OC прямоугольника нет точек с целыми координатами, кроме точки O. Действительно, уравнение прямой OC имеет вид $px=qy$, и если бы точка (c,d) с целыми положительными координатами принадлежала диагонали, то число $pc=qd$ делилось бы на q, а тогда делилось бы на q и число c, потому что p не делится на простое число q; но тогда было бы $c\ge q$, и поэтому точка (c,d) лежала бы не на диагонали OC, а на ее продолжении.

Сосчитаем теперь число S_1 точек с целыми координатами, лежащих внутри треугольника OAC. Если (i,j) – такая точка, то $1\le i\le s=[q/2]$, $1\le j<\frac{pi}{q}$; поэтому для фиксированного i число точек (i,j) с целым j, лежащих внутри треугольника OAC, равно $\left[\frac{pi}{q}\right]$, а общее число точек с целыми координатами равно $\left[\frac{1\cdot p}{q}\right]+\left[\frac{2p}{q}\right]+\dots+\left[\frac{sp}{q}\right]$.

Точно так же, если (i,j) – точка с целыми координатами, лежащая внутри треугольника OBC, то $1 \le j \le r = [p/2]$, $1 \le i < \dfrac{qj}{p}$; поэтому для фиксированного j число точек (i,j) с целым i, лежащих внутри треугольника OBC, равно $\left[\dfrac{qj}{p}\right]$, а общее число S_2 точек с целыми координатами, лежащих внутри треугольника OBC, равно $\left[\dfrac{1\cdot q}{p}\right] + \left[\dfrac{2q}{p}\right] + \dots + \left[\dfrac{rq}{p}\right]$.

Итак,

$$\left(\left[\frac{1\cdot p}{q}\right] + \left[\frac{2p}{q}\right] + \dots + \left[\frac{sp}{q}\right]\right) + \left(\left[\frac{1\cdot q}{p}\right] + \left[\frac{2q}{p}\right] + \dots + \left[\frac{rq}{p}\right]\right) =$$
$$= S_1 + S_2 = S = \frac{p-1}{2}\cdot\frac{q-1}{2}\ ,$$

что и требовалось.

Применение закона взаимности для вычисления символа квадратичного вычета. Пользуясь законом взаимности и свойством (9), которое называется дополнением к закону взаимности, а также мультипликативностью и другими свойствами символа, можно алгорифмически вычислять значения символа квадратичного вычета. Суть алгорифма будет ясна из следующего примера.

$$\left(\frac{33}{199}\right) = \left(\frac{3}{199}\right)\left(\frac{37}{199}\right) = \left(\frac{199}{3}\right)\cdot(-1)^{\frac{199-1}{2}\frac{3-1}{2}}\cdot\left(\frac{199}{37}\right)\cdot(-1)^{\frac{199-1}{2}\frac{37-1}{2}} =$$
$$= -\left(\frac{1}{3}\right)\left(\frac{14}{37}\right) = -\left(\frac{2}{37}\right)\left(\frac{7}{37}\right) = -(-1)^{\frac{37^2-1}{8}}\left(\frac{37}{7}\right)\cdot(-1)^{\frac{37-1}{2}\frac{7-1}{2}} =$$
$$= -\left(\frac{2}{7}\right) = -(-1)^{\frac{7^2-1}{8}} = -1.$$

Прокомментируем эту выкладку, последовательно объясняя, что мы делаем, переходя от каждого выражения к следующему.

- Пользуемся мультипликативностью символа;
- для каждого из двух получившихся символов применяем закон взаимности;
- считаем знак и приводим "числители" символов по модулю "знаменателей" (свойство (2));
- первый из символов равен, очевидно, 1, а второй раскладываем в произведение, пользуясь мультипликативностью символа;
- первый символ вычисляем по свойству (9), а ко второму применяем закон взаимности;
- приводим "числитель" символа по модулю "знаменателя";
- вычисляем символ по свойству (9).

14. Уравнение Пелля

В предыдущем параграфе изучались сравнения вида $x^2 \equiv a \pmod{n}$; как легко понять, решение диофантова уравнения $x^2 = a + ny$ сводится к решению такого сравнения. Здесь мы рассмотрим еще один класс диофантовых уравнений степени 2.

Уравнением Пелля называется уравнение вида

$$x^2 - dy^2 = 1,$$

где $d > 0$ – целое число, не являющееся квадратом. Решения этого уравнения будем записывать в виде пар целых чисел (x_0, y_0). У уравнения Пелля есть тривиальное решение $(1,0)$; можно доказать (но мы здесь этого не делаем), что всякое

уравнение Пелля имеет и нетривиальные решения. Наша цель – описать множество всех решений.

Начнем с нескольких простых замечаний. Если (u, v) – решение уравнения Пелля, то $(\pm u, \pm v)$ – тоже решения. Поэтому существуют нетривиальные решения (u, v) с $u > 0$, $v > 0$ (тогда, конечно, $u > 1$); множество первых компонент u таких решений – непустое подмножество $\mathbb{N}$, поэтому в нем есть наименьший элемент u_1. Пусть (u_1, v_1) – то решение, первой компонентой которого является u_1. Еще раз напомним основное свойство решения (u_1, v_1): $u_1 > 0$, $v_1 > 0$, и если (u, v) – любое решение с $u > 0$, $v > 0$, то $u_1 \leq u$.

Второе замечание касается чисел вида $a+b\sqrt{d}$ с рациональными a, b. Поскольку d – не квадрат в $\mathbb{Z}$, а значит, и в $\mathbb{Q}$, при $b \neq 0$ такое число является иррациональным. Легко видеть, что сумма, разность, произведение и частное таких чисел (последнее – если делитель отличен от 0) – снова число того же вида. Кроме того, рациональные числа a, b однозначно определяются числом $a + b\sqrt{d}$: если $a + b\sqrt{d} = a_1 + b_1\sqrt{d}$, и $b \neq b_1$ или $a \neq a_1$, то число $\sqrt{d} = (a - a_1)/(b - b_1)$ (соответственно, число $1/\sqrt{d} = (b - b_1)/(a - a_1)$) было бы рациональным, что неверно.

Прежде, чем сформулировать основной результат, описывающий множество решений уравнения Пелля, докажем несколько лемм.

Лемма 1. *Если (u, v) – решение уравнения $x^2-dy^2 = 1$, то $(u+v\sqrt{d})^{-1} = u-v\sqrt{d}$.*

Доказательство. Поскольку (u, v) – решение уравнения $x^2 - dy^2 = 1$, выполнено соотношения $u^2 - dv^2 = 1$. Таким образом, $(u + v\sqrt{d})(u - v\sqrt{d}) = u^2 - dv^2 = 1$, а это значит, что $(u + v\sqrt{d})^{-1} = u - v\sqrt{d}$.

Лемма 2. *Пусть (u, v) и (u', v') – два решения уравнения $x^2 - dy^2 = 1$ и пусть w, t – такие целые числа, что $w + t\sqrt{d} = (u + v\sqrt{d})(u' + v'\sqrt{d})$. Тогда (w, t) – решение уравнения $x^2 - dy^2 = 1$.*

Доказательство. Поскольку (u, v) и (u', v') – решения уравнения $x^2 - dy^2 = 1$, выполнены соотношения $u^2 - dv^2 = u'^2 - dv'^2 = 1$. Из равенства

$$w + t\sqrt{d} = (u + v\sqrt{d})(u' + v'\sqrt{d})$$

следует, что $w = uu' + dvv'$, $t = uv' + vu'$; поэтому

$$w - t\sqrt{d} = (uu' + dvv') - (uv' + vu')\sqrt{d} = (u - v\sqrt{d})(u' - v'\sqrt{d}).$$

Отсюда получаем:

$$w^2-dt^2 = (w + t\sqrt{d})(w-t\sqrt{d}) = ((u + v\sqrt{d})(u' + v'\sqrt{d}))((u-v\sqrt{d})(u'-v'\sqrt{d})) =$$
$$= ((u + v\sqrt{d})(u-v\sqrt{d}))((u' + v'\sqrt{d})(u'-v'\sqrt{d})) = (u^2-dv^2)(u'^2- dv'^2) = 1 \cdot 1 = 1.$$

Итак, (w, t) – решение уравнения $x^2 - dy^2 = 1$.

Лемма 3. *Пусть (u, v) и (w, t) – два решения уравнения $x^2 - dy^2 = 1$ с неотрицательными u, v,w, t. Неравенство $u + v\sqrt{d} \leq w + t\sqrt{d}$ выполняется тогда и только тогда, когда $u \leq w$, а неравенство $u + v\sqrt{d} < w + t\sqrt{d}$ выполняется тогда и только тогда, когда $u < w$.*

Доказательство. Если $u < w$, то $v = \sqrt{(u^2 - 1)/d} < \sqrt{(w^2 - 1)/d} = t$, и потому $u + v\sqrt{d} < w + t\sqrt{d}$. Пусть теперь $u + v\sqrt{d} \leq w + t\sqrt{d}$; если бы было $w < u$, то по уже доказанному мы бы имели $w + t\sqrt{d} < u + v\sqrt{d}$ в противоречие с предположением, и потому $u \leq w$. Для доказательства утверждения о строгих неравенствах достаточно заметить, что если $u = w$, то $v = \sqrt{(u^2 - 1)/d} = \sqrt{(w^2 - 1)/d} = t$, и $u + v\sqrt{d} = w + t\sqrt{d}$.

Лемма 4. *Пусть (u', v') – решение уравнения $x^2 - dy^2 = 1$. Если $u' + v'\sqrt{d} \geq 1$, то u' и v' неотрицательны.*

Доказательство. Пусть $u = |u'|$, $v = |v'|$; тогда (u, v) – тоже решение уравнения $x^2 - dy^2 = 1$, и при этом $u \geq 1$, $v \geq 0$. Если $u = 1$, то $v = 0$ и потому $v' = 0$, а тогда неравенство $1 \leq u' + v'\sqrt{d} = u'$ влечет положительность u'. Пусть теперь $u > 1$; тогда $u + v\sqrt{d} > 1$. Покажем, что если хотя бы одно из чисел u', v' отрицательно, то $u' + v'\sqrt{d} < 1$. Для этого рассмотрим все возможные случаи.

$$u' + v'\sqrt{d} = \begin{cases} u - v\sqrt{d} = (u + v\sqrt{d})^{-1} < 1, & \text{если } u' > 0,\ v' \leq 0; \\ -u - v\sqrt{d} < 0, & \text{если } u' < 0,\ v' \leq 0; \\ -u + v\sqrt{d} = -(u + v\sqrt{d})^{-1} < 0 < 1, & \text{если } u' < 0,\ v' \geq 0. \end{cases}$$

(в последнем случае мы воспользовались тем, что число $u + v\sqrt{d} > 1$ положительно). Итак, соотношение $u' + v'\sqrt{d} \geq 1$ возможно лишь при неотрицательных u', v'

Перейдем к основному результату этого параграфа.

Теорема 1. *Пусть $d > 0$ – целое число, не являющееся квадратом, и пусть (u_1, v_1) – решение уравнения Пелля $x^2 - dy^2 = 1$ с наименьшим возможным $u_1 > 1$ и с $v_1 > 0$. Тогда:*

(1) для всякого целого n и для всякого $\varepsilon = \pm 1$ пара (u, v), такая что $u + v\sqrt{d} = \varepsilon(u_1 + v_1\sqrt{d})^n$, является решением уравнения $x^2 - dy^2 = 1$;

(2) если (u, v) – решение уравнения $x^2 - dy^2 = 1$, то существуют такие $n \in \mathbb{Z}$ и $\varepsilon = \pm 1$, что $u + v\sqrt{d} = \varepsilon(u_1 + v_1\sqrt{d})^n$.

Доказательство. (1) Поскольку вместе с (u, v) решением уравнения будет и пара $(-u, -v)$, достаточно доказать утверждение для $\varepsilon = 1$. Далее, пусть $n < 0$ и пусть $u + v\sqrt{d} = (u_1 + v_1\sqrt{d})^{-n}$; тогда $u - v\sqrt{d} = (u_1 + v_1\sqrt{d})^n$ по лемме 1, и, если уже доказано, что (u, v) решение, то ясно, что и $(u, -v)$ – решение. Таким образом, достаточно лишь доказать, что если $n \geq 0$ и $u + v\sqrt{d} = (u_1 + v_1\sqrt{d})^n$, то пара (u, v) – решение уравнения Пелля; но это легко получается индукцией по n с использованием леммы 2.

(2) Пусть (u', v') – произвольное решение уравнения $x^2 - dy^2 = 1$, и пусть $u = |u'|$, $v = |v'|$; тогда (u, v) – тоже решение уравнения $x^2 - dy^2 = 1$. Поскольку

$$u' + v'\sqrt{d} = \begin{cases} u - v\sqrt{d} = (u + v\sqrt{d})^{-1}, & \text{если } u' > 0,\ v' \leq 0; \\ -u - v\sqrt{d} = (-1)(u + v\sqrt{d}), & \text{если } u' < 0,\ v' \leq 0; \\ -u + v\sqrt{d} = (-1)(u + v\sqrt{d})^{-1}, & \text{если } u' < 0,\ v' \geq 0, \end{cases}$$

достаточно доказать, что для любого решения (u, v) с неотрицательными u, v существует целое число $n \geq 0$, такое что $u + v\sqrt{d} = (u_1 + v_1\sqrt{d})^n$. Мы будем доказывать это индукцией по u. Если $u = 1$ и (u, v) – решение уравнения Пелля $x^2 - dy^2 = 1$, то $v = 0$, и $u + v\sqrt{d} = 1 + 0 \cdot \sqrt{d} = (u_1 + v_1\sqrt{d})^0$. Пусть $u > 1$ и пусть наше утверждение уже доказано для всех решений (w, t) с $1 \leq w < z$, $t \geq 0$. Положим

$$w + t\sqrt{d} = (u_1 + v_1\sqrt{d})^{-1}(u + v\sqrt{d}) = (u_1 - v_1\sqrt{d})(u + v\sqrt{d}).$$

По лемме 2 пара (w, t) вместе с парами $(u_1, -v_1)$ и (u, v) является решением уравнения $x^2 - dy^2 = 1$. Заметим, что $u_1 \leq u$, потому что (u_1, v_1) – нетривиальное решение уравнения в положительных числах с минимальным возможным значением x; по лемме 3 получаем тогда, что $u_1 + v_1\sqrt{d} \leq u + v\sqrt{d}$. Кроме того, $u_1 + v_1\sqrt{d} > 1$; следовательно, справедливы неравенства

$$1 \leq (u_1 + v_1\sqrt{d})^{-1}(u + v\sqrt{d}) = w + t\sqrt{d} = (u_1 + v_1\sqrt{d})^{-1}(u + v\sqrt{d}) < u + v\sqrt{d},$$

откуда по леммам 3 и 4 следует, что w и t неотрицательны, а $w < u$. По предположению индукции существует такое число $n \geq 0$, что $w + t\sqrt{d} = (u_1 + v_1\sqrt{d})^n$; но тогда

$$u + v\sqrt{d} = (u_1 + v_1\sqrt{d})(w + t\sqrt{d}) = (u_1 + v_1\sqrt{d})(u_1 + v_1\sqrt{d})^n = (u_1 + v_1\sqrt{d})^{n+1},$$

что и надо было получить.

В качестве примера рассмотрим уравнение Пелля $x^2 - 7y^2 = 1$. Пара $(8, 3)$ является решением этого уравнения, и простой перебор показывает, что не существует нетривиального решения с меньшим значением x. Поэтому произвольное решение (u, v) этого уравнения находится из соотношения $u + v\sqrt{d} = \pm(8 + 3\sqrt{7})^n$ при надлежащем выборе знака и целого числа n. Полагая $n = 1, 2, 3, 4$, укажем несколько первых решений уравнения:

$$(8, 3), \quad (127, 48), \quad (2024, 765), \quad (32257, 12192).$$