

Теория чисел Экзамен

Оглавление

1.	Основные множества. Понятия группы, кольца и поля.....	2
2.	Понятие целостного кольца. Теорема о погружении целостного кольца в поле.	4
3.	Понятие Евклидова кольца. Понятие о том, что кольцо целых чисел – евклидово.....	5
4.	Понятие наибольшего общего делителя и теорема о его существовании. Соотношения Безу ..	7
5.	Теорема о свойствах наибольшего общего делителя и алгоритм Евклида.....	8
6.	Теорема Ламе	10
7.	Понятие простого числа. Теорема о бесконечности множества простых чисел.	11
8.	Основная теорема арифметики.	13
9.	Решето Эратосфена в кольце целых чисел.	15
10.	Понятие класса вычетов. Свойства классов вычетов.	15
11.	Теорема о кольце классов вычетов	17
12.	Теорема о количестве числа решений уравнения $ax = b(m)$	21
13.	Расширенный алгоритм Евклида и его приложения	25
14.	Китайская теорема об остатках	29
15.	Функция Эйлера, ее свойства. Теорема Эйлера и малая теорема Ферма.	31
16.	Схема ассиметричного шифрования RSA и ее связь с функцией Эйлера.....	35
17.	Теорема о числе корней многочлена по простому модулю	38
18.	Теорема о числе решений многочлена по составному модулю.....	39
19.	Теорема о подъеме числа решений	43
20.	Квадратичные вычеты. Понятие символа Лежандра. Критерий Эйлера. Формулировка квадратичного закона взаимности	45
21.	Схема асимметричного шифрования Рабина-Вильямса и ее связь с квадратичными вычетами.....	55
22.	Алгоритм нахождения корней многочленов по простому модулю	57
23.	Двоичный алгоритм возведения в степень и области его применения	59
24.	Понятия показателя и первообразного корня. Их свойства.....	60
25.	Теорема о существовании первообразного корня по простому модулю	62
26.	Схема Диффи-Хеллмана выработки общего ключа и ее связь с первообразными корнями	66
27.	Понятие систематической дроби. Периодичность систематической дроби	68
28.	Понятие цепной дроби. Подходящие дроби и их свойства.	73
29.	Теорема о сходимости подходящих дробей	79
30.	Квадратичные иррациональности. Приведенные квадратичные иррациональности и теорема о периодичности квадратичных иррациональностей.....	81

1. Основные множества. Понятия группы, кольца и поля.

Определение 1.1. Мы будем называть множеством совокупность объектов, обладающих некоторым одинаковым свойством, например, множество букв или цифр.

1. Если все элементы некоторого множества U также принадлежат другому множеству V , то будем говорить, что U является подмножеством множества V и использовать запись $U \subseteq V$.
2. Будем говорить, что два множества равны и использовать запись $U = V$, если одновременно выполнено $U \subseteq V$ и $V \subseteq U$.
3. Если выполнено $U \subseteq V$ и множество V содержит элементы, которые не принадлежат U , то будем называть U собственным подмножеством и использовать обозначение $U \subset V$.
4. Если множество не содержит ни одного элемента, то будем говорить, что оно содержится в любом другом множестве. Такое множество мы будем называть пустым и обозначать его символом \emptyset .
5. Если множество U не пусто, то в нем содержится хотя бы один элемент a ; будем обозначать символом $a \in U$ принадлежность элемента a множеству U .
6. Если множество W состоит из элементов двух множеств U и V , то такое множество называется объединением множеств U и V и обозначается символом $U \cup V$.

Определение 1.2. Будем называть множеством натуральных чисел множество, образованное фиксированным элементом 1, которое вместе с элементом n содержит и элемент $n + 1$.

$$N = \{1, 2, 3, 4, 5, \dots\}$$

Определение 1.4. Сопоставим каждому натуральному числу n формальный символ $-n$, который мы будем называть «обратным» к n , а множество таких символов обозначим $-N$. Тогда множество целых чисел может быть определено как объединение

$$Z = -N \cup 0 \cup N = \{\dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\},$$

где символ 0 принято называть нулем. Множество $0 \cup N = \{0, 1, 2, 3, 4, 5, \dots\}$ мы будем обозначать символом N_0 . Отметим, что множество целых чисел обладает одним важным свойством, а именно, свойством упорядоченности.

Определение 1.8. Пусть U – произвольное непустое множество. Мы будем говорить, что на множестве U задана:

- унарная операция δ : $U \rightarrow U$, если любому элементу a множества U может быть сопоставлен элемент $\delta(a)$ множества U ;
- бинарная операция $*$: $U \times U \rightarrow U$, если любым двум упорядоченным, то есть записанным в определенном порядке, элементам a, b множества U можно сопоставить элемент множества U , обозначаемый символом $a * b$.

Определение 1.9. Бинарная операция $*$ называется ассоциативной, если для любых трех элементов a, b, c с множества U выполнено равенство

$$(a * b) * c = a * (b * c).$$

Определение 1.10. Бинарная операция $*$ называется коммутативной, если для любых двух элементов a, b множества U выполнено равенство

$$a * b = b * a.$$

Определение 1.12. Непустое множество U называется группой, если

1. на множестве U задана ассоциативная бинарная операция $*$;
2. относительно операции $*$ во множестве U существует нейтральный элемент e ;
3. для любого элемента a множества U найдется элемент $a^{-1} \in U$ такой, что $a * a^{-1} = e$.

Элемент a^{-1} принято называть обратным элементом к элементу a .

Если операция $*$ коммутативна, то группа называется коммутативной или абелевой.

Если в качестве бинарной операции $*$ используется операция сложения « $+$ », то группа называется аддитивной, если же используется операция умножения « \cdot », то группа называется мультипликативной.

Определение 1.15. Непустое множество U называется кольцом, если

1. на множестве U заданы две ассоциативные бинарные операции « $+$ » и « \cdot »;
1. операция « $+$ » коммутативна;
2. относительно операции « $+$ » множество U является группой;
3. выполнены законы дистрибутивности:

$$a(b + c) = ab + bc \text{ и } (b + c)a = ba + ca.$$

Группа, образованная элементами кольца U относительно операции « $+$ », называется аддитивной группой кольца. Нейтральный элемент аддитивной группы называется нулевым элементом кольца U и обозначается, как правило, символом 0 .

Если операция « \cdot » коммутативна, то кольцо называется коммутативным.

Если кольцо U содержит нейтральный элемент, относительно операции « \cdot », то такой элемент называется единичным элементом, а кольцо U – кольцом с единицей. Единичный элемент, как правило, обозначают символом 1 .

Определение 1.19. Пусть U кольцо. Если множество ненулевых элементов кольца U образует группу относительно операции « \cdot », то U называется телом. Если данная группа – коммутативна, то такое тело называется полем. Группа, образованная ненулевыми элементами тела (поля) U называется мультипликативной группой тела (поля).

Для того, чтобы предъявить менее тривиальный способ построения полей, нам потребуется понятие эквивалентности элементов множества.

Определение 1.20. Будем говорить, что на множестве U задано отношение эквивалентности « \sim »

- рефлексивно, то есть $a \sim a$;
- симметрично, то есть из $a \sim b$ следует $b \sim a$;
- транзитивно, то есть из $a \sim b$ и $b \sim c$ следует $a \sim c$.

Отношение эквивалентности может быть использовано для построения новых множеств, отличных от описанных нами ранее. Представляется естественным обозначить все эквивалентные между собой элементы множества U за новый элемент, определить новое множество, состоящее из указанных элементов, и определить на новом множестве элементарные операции сложения и умножения.

Именно такая последовательность действий используется в ходе доказательства следующей теоремы.

Теорема 1.3. Пусть U целостное кольцо с единицей. Тогда найдется поле F такое, что $F \supset U$.

2. Понятие целостного кольца. Теорема о погружении целостного кольца в поле.

Определение 1.11. Кольцо называется целостным (или областью целостности), если в нём произведение любых двух ненулевых элементов отлично от нуля (т.е. из того, что $ab = 0$, следует, что либо $a = 0$, либо $b = 0$).

Теорема о погружении целостного кольца в поле (теорема 1.3).

Доказательство теоремы 1.3 состоит из нескольких шагов. На первом шаге строится множество пар элементов целостного кольца U и на этом множестве вводится понятие эквивалентности. Множество эквивалентных пар образует один класс, а множество классов – поле F .

На втором шаге определяются операции сложения и умножения элементов поля F (классов эквивалентности) и показывается, что введенные операции не зависят от выбора представителей классов эквивалентности. На третьем шаге доказательства предъявляются классы эквивалентности, содержащие элементы кольца U . Множество таких классов содержит в себе кольцо U . Показывается, что введенные в поле F операции не выводят за пределы кольца U , т.е. результатом сложения и умножения классов эквивалентности, содержащих элементы кольца U , также являются классы эквивалентности, содержащие элементы кольца U .

Теорема 1.3. Пусть U целостное кольцо с единицей. Тогда найдется поле F такое, что $F \supset U$.

Доказательство. Пусть U целостное кольцо, т.е. коммутативное кольцо с единицей. Рассмотрим множество упорядоченных пар (a, b) элементов из U таких, что $b \neq 0$ и введем отношение эквивалентности двух пар

$$(a, b) \sim (c, d), \text{ если } ad = bc.$$

Данное отношение:

- рефлексивно, поскольку из коммутативности кольца U и равенства $ab = ba$ следует, что $(a, b) \sim (a, b)$;
- симметрично, поскольку из равенства $ad = bc$ следует равенство $bc = ad$ и условие $(c, d) \sim (a, d)$;
- транзитивно, поскольку из $(a, b) \sim (c, d)$ и $(c, d) \sim (e, f)$ следуют равенства

$$ad = bc, cf = ed.$$

Тогда $adf = bcf = bed$ и $af = be$, следовательно, $(a, b) \sim (e, f)$ и отношение \sim задает отношение эквивалентности на множестве пар (a, b) .

Выберем произвольную пару (a, b) и рассмотрим множество пар, эквивалентных паре (a, b) . Будем называть это множество классом эквивалентности и обозначать символом $\frac{a}{b}$. Тогда равенство

$\frac{a}{b} = \frac{c}{d}$ означает, что $(a, b) \sim (c, d)$ или $ad = bc$.

Множество классов будем обозначать символом F . Определим операции сложения и умножения новых символов (классов эквивалентности) равенствами:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{и} \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

Приведенные определения корректно определены, поскольку для $b \neq 0$, $d \neq 0$ кольцо U не содержит делителей нуля и величина $bd \neq 0$, и не зависят от выбора представителей классов. Действительно, пусть $(a_1, b_1) \sim (a, b)$, тогда $a_1b = ab_1$, или $a_1bd = adb_1$, для любого $d \in U$, $d \neq 0$, следовательно,

$$\frac{a_1}{b_1} + \frac{c}{d} = \frac{a_1d + b_1c}{b_1d} = \frac{(a_1d + b_1c)b}{b_1db} = \frac{adb_1 + b_1cb}{b_1db} = \frac{ad + bc}{bd} = \frac{a}{b} + \frac{c}{d}.$$

Аналогично,

$$\frac{a_1}{b_1} \times \frac{c}{d} = \frac{a_1d}{b_1d} = \frac{a_1db}{b_1db} = \frac{a_1db_1}{b_1db} = \frac{a}{b} \times \frac{c}{d}.$$

Легко проверить, что нейтральными элементами для введенных операций являются классы

$$\frac{0}{b} \text{ и } \frac{1}{1},$$

а сами операции определяют на множестве классов \mathbb{F} структуру поля.

Покажем, что $\mathbb{U} \subset \mathbb{F}$. Сопоставим элементу $c \in \mathbb{U}$ все дроби вида $\frac{cb}{b}$. Тогда, из равенства

$$(cb)b_1 = b(cb_1)$$

следует, что элементу c сопоставлен только один класс эквивалентности в \mathbb{F} . При этом, различным элементам $c_1 \neq c$ сопоставляются различные классы. В противном случае выполнены равенства

$$\frac{cb}{b} = \frac{c_1b_1}{b_1}$$

или

$$cbb_1 = c_1b_1b.$$

Так как $b \neq 0$, $b_1 \neq 0$, то, сокращая, получим $c = c_1$. Следовательно, элементам кольца \mathbb{U} однозначно сопоставляются дроби вида $\frac{cb}{b} \in \mathbb{F}$.

Поскольку

$$\frac{c_1b_1}{b_1} + \frac{c_2b_2}{b_2} = \frac{(c_1 + c_2)b_1b_2}{b_1b_2}$$

и

$$\frac{c_1b_1}{b_1} \times \frac{c_2b_2}{b_2} = \frac{(c_1c_2)b_1b_2}{b_1b_2}$$

то операции сложения и умножения в \mathbb{F} оставляют множество дробей $\{\frac{cb}{b}\}$ замкнутым, т.е не выводят за его пределы, и индуцируют на нем структуру коммутативного кольца \mathbb{U} . \square

3. Понятие Евклидова кольца. Понятие о том, что кольцо целых чисел – евклидово.

Определение 2.4. Кольцо U называется евклидовым, если на нем задана норма $N : U \rightarrow \mathbb{N}_0$ такая, что для любых двух элементов $a, b \in U$, где $a \neq 0$, найдутся элементы $q, r \in U$ удовлетворяющие условию

$$b = qa + r, \text{ где } N(r) < N(a) \text{ или } r = 0. \quad (2.2)$$

Мы будем называть операцию вычисления пары q, r , удовлетворяющей (2.2), операцией деления с остатком, величину r – остатком от деления, или просто, остатком, а величину q – частным.

Стоит отметить, что из данного нами определения следует, что отличный от нуля элемент a евклидового кольца U , удовлетворяющий условию $N(a) = 0$, должен делить любой элемент b этого

кольца. Способ определения нормы существенно влияет на определение операции деления с остатком. Проиллюстрируем это на примере введенных ранее колец.

Теорема 2.1. Кольцо целых чисел Z является евклидовым кольцом, то есть для любой пары целых чисел a, b таких, что $a \neq 0$, найдутся целые q, r такие, что

$$b = qa + r, |a| > r \geq 0$$

и такая пара чисел q, r — единственна.

Для доказательства теоремы 2.1 нам необходимо постулировать ряд аксиом, выполненных для кольца целых чисел.

Аксиома 1 (Архимеда). Для любых целых чисел a, b найдется такое целое число, что $ac > b$. Данную аксиому принято называть аксиомой Архимеда.

Аксиома 2. Пусть $M \subset Z$ конечное, непустое подмножество во множестве целых чисел, тогда M содержит минимальный и максимальный элементы, т.е. такие элементы a и b , что

$$a \leq c \leq b, \text{ для всех } c \in M.$$

Следует отметить, что указанные аксиомы тесно связаны с введенным нами ранее свойством упорядоченности множества целых чисел. Приводимое далее доказательство теоремы 2.1 также использует свойства введенных на множестве целых чисел операций «больше», «меньше».

Доказательство теоремы 2.1. Предположим, что a, b неотрицательные целые числа и $a \neq 0$. Тогда, в силу аксиомы Архимеда найдется такое целое число c , что $ac > b$.

Множество чисел, удовлетворяющих указанному неравенству, — конечно. Действительно из неравенства $ac > b \geq 0$ следует, что выполнено неравенство $c \geq 0$. Тогда, из второй аксиомы следует, что рассматриваемое множество содержит минимальный элемент и для этого элемента выполнены неравенства

$$ac > b \geq a(c - 1). \quad (2.3)$$

Обозначим $q = c - 1$ и $r = b - a(c - 1)$, тогда из (2.3) следует оценка (2.2), т.е. неравенство

$$a = ac - a(c - 1) > b - a(c - 1) = r \geq 0.$$

Докажем, что полученное представление единственно. Если это не так, то найдутся целые q_1, r_1 такие, что

$$aq + r = b = aq_1 + r_1, a > r_1 \geq 0.$$

или

$$a(q - q_1) = r_1 - r.$$

Поскольку правая часть равенства удовлетворяет неравенствам $a > |r_1 - r| \geq 0$, а левая всегда кратна a , то равенство возможно только в случае, когда $r_1 - r = 0$, следовательно, $r_1 = r$, $q_1 = q$ и для случая $b > a > 0$ теорема доказана.

4. Понятие наибольшего общего делителя и теорема о его существовании. Соотношения Безу

Определение 2.6. Пусть a, b элементы евклидового кольца U . Элемент $d \in U$, $d \neq 0$, называется наибольшим общим делителем, если

1. $d|a$ и $d|b$, (d делит a и d делит b)
2. для любого общего делителя $\delta \neq 0$ такого, что $\delta|a$ и $\delta|b$ выполнено $\delta|d$.

Далее мы будем обозначать наибольший общий делитель символом НОД (a, b) .

Теорема 2.4. Пусть U евклидово кольцо и $a, b \in U$, одновременно не равные нулю. Тогда наибольший общий делитель НОД (a, b) существует и, с точностью до ассоциированных значений, единственен.

Доказательство. Рассмотрим множество $D = \{au + bv, u, v \in U\}$, образованное всеми возможными линейными комбинациями элементов a, b с коэффициентами $u, v \in U$. Выберем в этом множестве отличный от нуля элемент d такой, что его норма $N(d)$ минимальна (поскольку хотя бы один из элементов a, b отличен от нуля, то найдется хотя бы один отличный от нуля элемент d ; поскольку множество N_0 , которому принадлежат значения нормы, ограничено снизу, то среди всех ненулевых элементов d найдется элемент с минимальной нормой).

Предположим, что d не делит a . Тогда найдутся такие $q, r \in U$, что

$$a = dq + r, N(r) < N(d), r \neq 0.$$

Тогда r удовлетворяет равенству

$$r = a - dq = a - (au + bv)q = a(1 - u) + bvq$$

и, следовательно, принадлежит множеству D . Однако, это противоречит тому, что d имеет наименьшую норму среди элементов множества D . Таким образом, предположение не верно, $r = 0$ и $d|a$. Аналогичными рассуждениями получаем, что $d|b$, следовательно, d – общий делитель.

Пусть теперь δ другой общий делитель a и b . Обозначим $a = c\delta$, $b = s\delta$, тогда из равенства

$$d = au + bv = c\delta u + s\delta v = \delta(cu + sv)$$

следует, что δ делит d .

Теперь покажем, что выбранный таким образом элемент d единственен. Пусть найдется d_2 – второй, отличный от d , наибольший общий делитель элементов a и b . Поскольку d_2 общий делитель, а d – наибольший общий делитель, то $d_2|d$. Аналогично, поскольку d общий делитель, а d_2 – наибольший общий делитель, то $d|d_2$, и мы получили, что $d \sim d_2$.

Следствие 2.4. (соотношение Безу). Пусть a, b элементы евклидового кольца U . Тогда найдутся элементы $u, v \in U$ такие, что

$$au + bv \sim \text{НОД} (a, b).$$

Для определения наибольшего общего делителя как единственного элемента евклидового кольца необходимо ввести дополнительное ограничение и указать способ выбора одного значения НОД (a, b) из множества ассоциированных элементов.

- В кольце целых чисел \mathbb{Z} мы накладываем условие НОД $(a, b) > 0$.
- В кольце многочленов от одной переменной $\mathbb{Q}[x]$ мы накладываем условие унитарности многочлена $d(x) = \text{НОД}(a(x), b(x))$, то есть

$$d(x) = x^n + d_{n-1}x^{n-1} + \cdots + d_0 \in \mathbb{Q}[x].$$

- В кольце целых гауссовых чисел из четырех ассоциированных друг с другом чисел

$$a + bi, -a - bi, -b + ai, b - ai$$

всегда можно выбрать такой, что $0 < a \leq |b|$.

5. Теорема о свойствах наибольшего общего делителя и алгоритм Евклида.

Теорема 2.5 (о свойствах НОД). Пусть U эвклидово кольцо и $a, b \in U$, тогда выполнены следующие утверждения.

1. $\text{НОД}(a, b) \sim \text{НОД}(b, a)$.
2. Если $a \neq 0$, то $\text{НОД}(a, 0) \sim a$.
3. Если $\varepsilon \in U^*$ обратимый элемент кольца, то $\text{НОД}(a, \varepsilon) \sim \varepsilon$.
4. $\text{НОД}(ac, bc) \sim c \text{НОД}(a, b)$ для любого, отличного от нуля $c \in U$.
5. $\text{НОД}(a, b) \sim \text{НОД}(a, a \pm b)$.
6. Пусть $b = aq+r$, где $N(r) < N(a)$ или $r = 0$, тогда $\text{НОД}(a, b) \sim \text{НОД}(a, r)$.
7. Пусть для некоторого элемента $c \neq 0$ и $\varepsilon \in U^*$ выполнено $\text{НОД}(a, c) \sim \varepsilon$, тогда $\text{НОД}(a, bc) \sim \text{НОД}(a, b)$.
8. Если $\varepsilon \in U^*$ обратимый элемент кольца, то $\text{НОД}(a, b\varepsilon) \sim \text{НОД}(a, b)$.

Доказательство.

Первое утверждение теоремы следует из определения наибольшего общего делителя.

Для доказательства второго утверждения леммы заметим, что, согласно соотношению Безу, для некоторого отличного от нуля элемента $u \in U$ выполнено равенство $\text{НОД}(a, 0) = au$. Поскольку $a | au$, то $N(a) \leq N(au)$ для любого, отличного от нуля $u \in U$. Таким образом, a имеет минимальную норму из элементов вида au и является наибольшим общим делителем элементов a и 0 .

Для доказательства третьего утверждения достаточно заметить, что выполнено условие $\text{НОД}(a, \varepsilon) | \varepsilon$, тогда учитывая, что ε делит любой элемент кольца U и, в том числе, элемент $\text{НОД}(a, \varepsilon)$, получаем $\text{НОД}(a, \varepsilon) \sim \varepsilon$.

Для доказательства четвертого утверждения обозначим $d = \text{НОД}(a, b)$ и $\delta = \text{НОД}(ac, bc)$. Тогда $d | a$ и мы получаем, что $dc | ac$. Аналогично, $d | b$ и $dc | bc$, следовательно, $dc | \text{НОД}(ac, bc) = \delta$ или $dcs = \delta$ для некоторого $s \in U$. Если $N(s) = N(1)$, то s обратимый элемент кольца U и выполнено условие $dc \sim \delta$, из которого следует четвертое утверждение леммы.

Предположим, что $N(s) > 1$. Поскольку $\delta | ac$, то найдется такой элемент $t \in U$, что $\delta t = ac$, тогда, записывая $a = dl$, $dcs \cdot t = dl \cdot c$. Сокращая на $c \neq 0$ и $d \neq 0$, получим $st = l$, откуда $a = dl = dst$ и $ds | a$. Аналогично получаем, что $ds | b$, следовательно $ds | d$ или $ds = d$ для некоторого v . Сокращая на d получаем $sv = 1$ и s – обратимый элемент.

Для доказательства пятого и шестого утверждений леммы обозначим $d = \text{НОД}(a, b)$,

$s = \begin{cases} a \pm b \\ b - aq \end{cases}$ или, $\delta = \text{НОД}(a, s)$. Тогда $d|a$, $d|b$, следовательно, $d|s$ и тогда $d|\delta$. С другой стороны, $\delta|a$, $\delta|s$ следовательно $\delta|b = \pm(a - s)$, и $\delta|b = aq + s$, и мы получаем, что $\delta|d$ и тогда $d \sim \delta$.

Для доказательства седьмого утверждения леммы обозначим $d = \text{НОД}(a, b)$. Легко видеть, что $d|\text{НОД}(a, bc)$. Обозначим $\delta = \text{НОД}(a, bc)$. Тогда $\delta|bc$ и найдется некоторый элемент $u \in U$ такой, что $bu = bc$. Если $\text{НОД}(\delta, c) \sim 1$, то воспользовавшись утверждением леммы 2.6 получаем, что $\delta|b$ и $\delta|d$, откуда сразу вытекает условие $\delta \sim d$. Таким образом, для доказательства седьмого утверждения леммы осталось показать, что $\text{НОД}(\delta, c) \sim 1$. Пусть это не так, тогда обозначим $\text{НОД}(\delta, c) = 1$ и $N(l) > 1$. Тогда $l|\delta|a$, откуда следует, что $l|\text{НОД}(a, c) \sim 1$ и $l \sim 1$. Полученное условие, вместе со вторым утверждением леммы 2.7, опровергает предположение $N(l) > 1$ и завершает доказательство седьмого утверждения.

Поскольку восьмое утверждение является прямым следствием третьего и седьмого утверждений, то теорема доказана.

Алгоритм Эвклида.

Пусть U эвклидово кольцо и $a, b \in U$ – отличные от нуля элементы этого кольца. Используя операцию деления с остатком, см. равенство (2.2), определим $r_{-1} = b$, $r_0 = a$ и последовательность

$$b = aq_1 + r_1,$$

$$a = r_1q_2 + r_2,$$

$$r_1 = r_2q_3 + r_3,$$

...

$$r_{k-1} = r_kq_{k+1} + r_{k+1},$$

...

$$r_{n-1} = r_nq_{n+1}, r_{n+1} = 0, n \in N_0.$$

Теорема 2.6. Пусть a, b отличные от нуля элементы эвклидового кольца U . Определим величины $r_{-1}, r_0, \dots, r_{n+1}, q_1, \dots, q_{n+1} \in U$ равенствами (2.11). Тогда найдется такой индекс $n \in N_0$, что $r_{n+1} = 0$ и

$$r_n \sim \text{НОД}(a, b).$$

Доказательство. В силу определения операции деления с остатком для всех $n = 0, 1, \dots$ выполнено равенство $N(r_{n+1}) < N(r_n)$ или $r_{n+1} = 0$. Тогда, последовательность величин $N(r_1), N(r_2), \dots$ является убывающей последовательностью целых чисел, ограниченных, в силу определения нормы, снизу нулем. Следовательно, найдется индекс, для которого будет выполнено условие $N(r_{n+1}) = 0$. Тогда, либо $r_{n+1} = 0$, либо r_{n+1} нацело делит r_n и уже элемент $r_{n+2} = 0$.

Теперь, из второго и шестого утверждения теоремы 2.5, получаем соотношения $\text{НОД}(a, b) \sim \text{НОД}(r_1, a) \sim \dots \sim \text{НОД}(r_n, 0) \sim r_n$, если $r_{n+1} = 0$, или $\text{НОД}(a, b) \sim \dots \sim \text{НОД}(r_{n+1}, 0) \sim r_{n+1}$, если $r_{n+2} = 0$.

Теорема доказана.

6. Теорема Ламе

Теорема 2.7 (Ламе). Пусть a, b целые числа и $b > a > 0$. Количество операций деления с остатком в алгоритме 2.1 может быть оценено сверху величиной $1 + \log_2 b$, где c положительная, эффективно вычислимая константа.

Для доказательства этой теоремы нам потребуется сделать небольшое отступление и доказать лемму о свойствах элементов последовательности Фибоначчи.

Определение 2.8. Мы будем называть рекуррентную последовательность целых чисел

$$A_0 = 0, A_1 = 1,$$

$$A_{n+1} = A_n + A_{n-1}, \text{ при } n = 1, 2, \dots$$

Последовательностью Фибоначчи.

Лемма 2.8. Пусть $z = \frac{1+\sqrt{5}}{2}$ действительный, положительный корень уравнения $z^2 = z + 1$. Тогда для последовательности Фибоначчи при всех натуральных n выполнено неравенство

$$A_{n+1} \geq z^{n-1}.$$

Доказательство леммы 2.8. При $n = 1$, очевидно, $A_2 = 1 > 0$ и утверждение леммы выполнено. Далее проведем доказательство по индукции. Пусть условие леммы выполнено для всех индексов, меньших либо равных n . Тогда, в силу выбора z , выполнено неравенство

$$A_{n+1} = A_n + A_{n-1} \geq z^{n-2} + z^{n-3} = z^{n-3}(z + 1) = z^{n-1}.$$

Доказательство теоремы Ламе. Вначале мы докажем неравенство

$$r_{k-1} \geq A_{n+1-k}, \text{ при } k = 0, 1, \dots, n$$

где последовательность r_{-1}, r_0, \dots, r_n определена равенством (2.11), а последовательность Фибоначчи A_1, A_2, \dots равенством (2.12). При $k = n$ выполнено $r_{n-1} = r_n q_{n+1} \geq 1 = A_1$. Далее по индукции.

Пусть для всех $n, n-1, \dots, k$ неравенство (2.14) выполнено. Тогда

$$r_{k-1} = r_k q_{k+1} + r_{k+1} \geq r_k + r_{k+1} \geq A_{n-k} + A_{n-(k+1)} = A_{n+1-k}.$$

Из неравенства (2.14) и леммы 2.8 при $k = 0$ получаем

$$b = r_{-1} \geq A_{n+1} \geq z^{n-1} \text{ или } n \leq 1 + \log_z b.$$

Учитывая значение $z = \frac{1+\sqrt{5}}{2}$ мы получаем неравенство

$$n \leq 1 + \frac{\log_2 b}{\log_2(1 + \sqrt{5})}$$

которое завершает доказательство теоремы.

7. Понятие простого числа. Теорема о бесконечности множества простых чисел.

Определение 3.1. Множество делителей элемента $a \in U$

$$\{\varepsilon, a\varepsilon : \varepsilon \in U^*\},$$

определенное для всех возможных обратимых элементов кольца U , называется множеством несобственных делителей элемента a , а сами делители из указанного множества – несобственными делителями. Делители элемента a , отличные от указанных, называются собственными делителями элемента a .

Определение 3.2. Если необратимый элемент $a \in U$ обладает только несобственными делителями, то такой элемент будем называть неразложимым. В кольце целых чисел положительные неразложимые элементы принято называть простыми числами.

Определение 3.3. Если необратимый элемент $a \in U$ обладает собственным делителем $v \in U$, то такой элемент принято называть разложимым или составным элементом.

Лемма 3.1. Пусть $a \in U$ отличный от нуля, разложимый элемент и $a = uv$, где v – собственный делитель элемента a . Тогда выполнены следующие утверждения.

1. Элемент $u \in U$ также является собственным делителем элемента a .
2. Выполнено строгое неравенство $N(v) < N(a)$.

Доказательство. Рассмотрим элемент $a = uv$ и предположим, что элемент u является несобственным делителем элемента a . Тогда, в силу определения несобственного делителя, либо $u \in U^*$ – обратимый элемент кольца, либо $u = \varepsilon a$, где ε обратимый элемент кольца. Если u обратим, то найдется $u^{-1} \in U^*$ такой, что $uu^{-1} = 1$. Тогда

$$au^{-1} = uvu^{-1} \text{ или } v = au^{-1}.$$

Последнее равенство противоречит тому, что v несобственный делитель элемента a . Если же делитель u имеет вид $u = \varepsilon a$, то из равенства

$$a = uv = \varepsilon av$$

и того факта, что a отличен от нуля, следует, что $\varepsilon v = 1$, т.е. элемент v обратим. Это также противоречит тому, что v несобственный делитель. Из полученных противоречий следует доказательство первого утверждения леммы.

Перед доказательством второго утверждения заметим, что в силу определения нормы выполнено неравенство $N(v) \leq N(a)$, таким образом нам достаточно доказать, что $N(v) \neq N(a)$. Предположим, что это не так и $N(v) = N(a)$. Если норма мультипликативна, то из равенств

$$N(v) = N(a) = N(uv) = N(u)N(v), N(v) \neq 0$$

следует, что $N(u) = 1$. Тогда, из второго утверждения леммы 2.7 вытекает, что v обратим, а это противоречит доказанному выше первому утверждению леммы. В случае аддитивной нормы, из равенств

$$N(v) = N(a) = N(uv) = N(u) + N(v)$$

получаем, что $N(u) = 0$ и опять, из леммы 2.7 следует противоречие с тем, что u собственный делитель. Теперь мы можем строго доказать, что неразложимые элементы существуют.

Теорема 3.1 (Теорема о существовании). Пусть U – евклидово кольцо, содержащее хотя бы один необратимый элемент a . Тогда в кольце U найдется хотя бы один неразложимый элемент r и $r|a$.

Доказательство. Пусть $a \in U$ – отличный от нуля, необратимый элемент кольца и элементы p_1, \dots, p_k образуют множество всех возможных делителей элемента a . Вычислим значения нормы и упорядочим элементы p_1, \dots, p_k так, что

$$N(p_1) \leq N(p_2) \leq \dots \leq N(p_k).$$

Без ограничения общности считаем, что элемент $r = p_1$ имеет минимальное значение нормы, тогда этот элемент является неразложимым.

Предположим обратное, тогда найдется элемент $v \in U$, являющийся собственным делителем элемента p_1 . Следовательно $v|p_1|a$ и v также является делителем элемента a , т.е. должен быть среди элементов p_2, \dots, p_k и удовлетворять неравенству $N(v) \geq N(p_1)$. Вместе с тем, из утверждения леммы 3.1 следует, что $N(v) < N(p_1)$. Полученное противоречие позволяет говорить, что у p_1 имеются только несобственные делители, т.е. он неразложим. Теорема доказана.

Теорема 3.2. Пусть евклидово кольцо U удовлетворяет условиям теоремы 3.1. Тогда множество неразложимых элементов кольца U бесконечно.

Доказательство. Предположим, что утверждение теоремы не выполнено. Тогда в кольце U найдется лишь конечное число неразложимых элементов, которые мы обозначим p_1, \dots, p_k для некоторого натурального k . Определим элемент

$$r = p_1 \cdots p_k + \varepsilon, \quad \varepsilon \in U^*$$

являющийся произведением всех неразложимых элементов кольца, к которому прибавлен произвольный обратимый элемент кольца U . Поскольку операции сложения и умножения не выводят за пределы кольца, то построенный элемент $r \in U$.

Легко проверить, что $r \neq 0$. Действительно, если выполнено равенство $p_1 \cdot p_2 \cdots p_k + \varepsilon = 0$, то

$$-p_1 \cdot p_2 \cdots p_k \varepsilon^{-1} = 1$$

Поскольку p_i неразложимые элементы, то они не могут быть обратимыми элементами кольца и, следовательно, равенство $r = 0$ не выполнено. Теперь предположим, что найдется индекс i такой, что $i \in \{1, 2, \dots, k\}$ и $r = p_i$, тогда выполнено равенство

$$p_1 \cdots p_k + \varepsilon = p_i, \text{ или } p_i (1 - p_1 \cdots p_{i-1} p_{i+1} \cdots p_k) \varepsilon^{-1} = 1,$$

из которого вытекает противоречие с тем, что элементы p_1, \dots, p_k необратимы, следовательно, мы делаем заключение, что все элементы p_1, \dots, p_k отличны от элемента r . Если элемент r неразложим, то мы в явном виде предъявили неразложимый элемент, отличный от p_1, \dots, p_k и, тем самым, опровергли исходное предположение.

Если же элемент r разложим, то, основываясь на доказательстве теоремы 3.1, будем считать, что существует элемент v – неразложимый собственный делитель элемента r . Поскольку для любого индекса $i \in \{1, 2, \dots, k\}$ выполнено равенство

$$r = q_i p_i + \varepsilon, \quad q_i = p_1 \cdots p_{i-1} p_{i+1} \cdots p_k, \quad \varepsilon \neq 0$$

то ни один из неразложимых элементов p_1, \dots, p_k не делит элемент r и, следовательно, отличен от элемента v . Теорема доказана.

8. Основная теорема арифметики.

Лемма 3.2. Пусть $a, b \in U$ не ассоциированные друг с другом, неразложимые элементы кольца U . Тогда $\text{НОД}(a, b) \sim 1$.

Доказательство. Поскольку a неразложимый элемент кольца U , то его делителями являются элементы $\{\varepsilon, \varepsilon a : \varepsilon \in U^*\}$. Аналогично, делителями b являются элементы $\{\varepsilon, \varepsilon b : \varepsilon \in U^*\}$. Поскольку $a \neq \varepsilon b$ для некоторого $\varepsilon \in U^*$, то общими делителями элементов a, b являются обратимые элементы кольца U , тогда $\text{НОД}(a, b) \sim 1$.

Лемма 3.3. Пусть a, b взаимно простые элементы евклидового кольца U . Если p неразложимый элемент кольца и $p|ab$, тогда либо $p|a$, либо $p|b$.

Доказательство. Если элемент $p|a$, то утверждение леммы выполнено. Будем считать, что это не так. Тогда p не делит a и, поскольку p неразложим, выполнено $\text{НОД}(a, p) \sim 1$ (иначе существовал бы необратимый элемент d , который делил p , что противоречит тому, что p неразложим). Поскольку $p|ab$, то существует элемент u такой, что $ab = pu$, тогда, из утверждения леммы 2.6 следует, что $p|b$. Лемма доказана.

Теорема 3.3 (Основная теорема арифметики). Пусть a произвольный, отличный от нуля элемент евклидового кольца U , тогда его можно представить в виде произведения

$$a = \varepsilon \cdot p_1 \cdots p_k$$

где $\varepsilon \in U^*$, а p_1, \dots, p_k неразложимые элементы кольца U . Данное представление единственno, с точностью до перестановки элементов p_1, \dots, p_k и обратимых сомножителей кольца U .

Доказательство. Начнем с доказательства существования указанного представления. Если a обратимый элемент, то выполнено равенство $n = \varepsilon$ для некоторого $\varepsilon \in U^*$. Если a неразложимый элемент, что выполнено равенство $a = p_1$ для некоторого неразложимого элемента $p_1 \in U$. Осталось рассмотреть случай, когда a разложимый элемент.

В этом случае, согласно утверждению теоремы 3.1, найдется неразложимый элемент $p_1 \in U$ такой, что $p_1|a$ и $a = p_1a_1$ для некоторого $a_1 \in U$. При этом, согласно лемме 3.1, будет $N(a_1) < N(a)$.

Применяя к элементу a_1 рассуждения, аналогичные тем, что мы применили к элементу a , получим цепочку равенств

$$\begin{aligned} a &= p_1 a_1, & N(a_1) &< N(a), \\ a &= p_1 p_2 a_2, & N(a_2) &< N(a_1), \\ &\dots \\ a &= p_1 p_2 \cdots p_k a_k, & N(a_k) &< N(a_{k-1}). \end{aligned}$$

Поскольку величины $N(a_k) < \cdots < N(a_1) < N(a)$ принимают неограниченные целые значения и убывают, то процесс не сможет длиаться бесконечно (см. вторую аксиому Арихимеда) и обернется на некотором шаге k . Это означает, что величина a_k окажется неразложимым элементом и, обозначая $p_{k+1} = a_k$, мы получим искомое равенство.

Зафиксируем некоторый индекс $i \in \{1, \dots, k\}$ и рассмотрим ассоциированный с p_i элемент π_i . Тогда π_i также неразложим, кроме того выполнены равенства $p_i = \varepsilon \pi_i$, где $\varepsilon \in \mathbb{U}^*$, и

$$a = p_1 \cdots p_{i-1} \cdot \varepsilon \pi_i \cdot p_i \cdots p_k.$$

Существование доказано.

Для доказательства единственности предположим, что существует другое представление элемента a в виде произведения и выполнено равенство

$$\varepsilon p_1 \cdots p_k = a = \gamma q_1 \cdots q_s, \quad (3.2)$$

где $k, s \in \mathbb{N}_0$, а $p_1, \dots, p_k, q_1, \dots, q_s$ неразложимые элементы кольца \mathbb{U} . Кроме того, без ограничения общности, будем считать, что выполнено условие $k \leq s$.

Рассмотрим p_1 и предположим, что среди q_1, \dots, q_s найдется элемент, ассоциированный с p_1 . Изменяя очередность записи множителей, будем считать, что это q_1 , тогда $p_1 = q_1 \gamma_1$ для некоторого $\gamma_1 \in \mathbb{U}^*$, а равенство (3.2) принимает вид

$$\varepsilon \gamma_1 p_2 \cdots p_k = \gamma q_2 \cdots q_s. \quad (3.3)$$

Если же мы предположим, что среди элементов q_1, \dots, q_s не найдется элемента ассоциированного с p_1 , то выбрав один из неассоциированных элементов, скажем q_s , получим, согласно утверждению леммы 3.2, условие $\text{НОД}(p_1, q_s) \sim 1$. Теперь, воспользовавшись утверждением леммы 2.6, мы можем сказать, что $p_1 | q_1 \cdots q_{s-1}$. Поскольку p_1 неразложим, то согласно лемме 3.3 найдется такой индекс, скажем единица, что $p_1 | q_1$. Поскольку q_1 также неразложим, то последнее условие возможно, если p_1 ассоциирован с q_1 , т.е. $p_1 = q_1 \gamma_1$ для некоторого $\gamma_1 \in \mathbb{U}^*$. Это снова приводит нас к равенству (3.3).

Продолжая рассуждения аналогичным образом для всех индексов $i = 2, \dots, k$ получим равенство

$$\varepsilon \gamma_1 \cdots \gamma_k = \gamma$$

в случае, когда $k = s$, или равенство

$$\varepsilon \gamma_1 \cdots \gamma_k = \gamma q_{k+1} \cdots q_s$$

при $k < s$.

В первом случае, мы получили условие $p_i \sim q_i$ для всех $i = 1, \dots, k$, которое эквивалентно утверждению теоремы. Во втором случае мы можем записать равенство

$$1 = \varepsilon^{-1} \gamma_1^{-1} \cdots \gamma_k^{-1} \gamma q_{k+1} \cdots q_s$$

из которого сразу следует, что величины q_{k+1}, \dots, q_s являются обратными элементами кольца \mathbb{U} . Теорема доказана. \square

9. Решето Эратосфена в кольце целых чисел.

Лемма 3.4. Пусть a разложимый элемент эвклидового кольца U и p его неразложимый делитель с наименьшей нормой. Если норма мультипликативна, то $N(p) \leq \sqrt{N(a)}$. Если же норма аддитивна, то $N(p) \leq \frac{N(a)}{2}$

Из утверждения леммы 3.4 следует, что у разложимого элемента a всегда найдется неразложимый делитель p , норма которого ограничена значением, зависящим от нормы элемента a . Если же такого делителя не существует, то элемент a – неразложимый.

Сформулированная идея легла в основу решета Эратосфена — алгоритма поиска всех неразложимых элементов кольца U , норма которых ограничена сверху некоторым натуральным значением b . Данный алгоритм может быть реализован только в тех эвклидовых кольцах, в которых число элементов, имеющих заданное значение нормы, конечно.

Для кольца целых чисел решето Эратосфена состоит в следующем. Выпишем все натуральные, необратимые целые числа от 2 до максимального значения b , упорядочив их по возрастанию нормы, т.е.

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, \dots, b - 1, b.$$

Первое число в этой последовательности будет иметь минимально возможную норму для необратимого элемента, поэтому оно не может быть разделено на какой-либо другой обратимый элемент с меньшей нормой. Следовательно, данное число является неразложимым элементом.

Отметим двойку в качестве неразложимого элемента, вычеркнем из рассматриваемой последовательности все элементы, которые делятся на двойку, и получим следующую последовательность чисел

$$\textcircled{2}, 3, 5, 7, 9, 11, 13, 15, \dots, b.$$

Рассмотрим среди оставшихся чисел первое неотмеченное число с наименьшей нормой, т.е. тройку. Данное число не делится на отмеченный ранее неразложимый элемент с меньшей нормой и, следовательно, само является неразложимым элементом кольца. Тогда, отметим тройку в качестве неразложимого элемента, вычеркнем из рассматриваемой последовательности все элементы, которые делятся на тройку, и получим следующую последовательность чисел

$$\textcircled{2} \textcircled{3}, 5, 7, 11, 13, \dots, b.$$

Далее, мы повторим эту процедуру применительно к первому неотмеченному элементу с минимальной нормой, т.е. пятерке, потом к семерке и так далее, до тех пор, пока мы не отметим элемент p такой, что $N(p) > \sqrt{N(b)}$ (при этом может оказаться, что число b будет вычеркнуто ранее). Все оставшиеся числа, согласно утверждению леммы 3.4, будут положительными неразложимыми элементами кольца целых чисел, т.е. простыми числами. Добавляя к ним ассоциированные элементы, мы получим множество всех неразложимых элементов кольца целых чисел, норма которых не превосходит заданной величины.

10. Понятие класса вычетов. Свойства классов вычетов.

Лемма 4.2. Отношение $a \equiv b \pmod{m}$ есть отношение эквивалентности в кольце U .

Доказательство. Нам необходимо показать выполнимость свойств, указанных в определении 1.20. Свойства рефлексивности $a \equiv a \pmod{m}$ и симметричности $a + b \equiv b + a \pmod{m}$ следуют из утверждений леммы 4.1. Для доказательства выполнимости свойства транзитивности заметим следующее. Пусть $b \equiv a \pmod{m}$ и $c \equiv b \pmod{m}$, тогда выполнены равенства

$$c = b + lm = a + km + lm = a + (k + l)m,$$

для некоторых элементов $k, l \in U$, и $m | (c - a)$. Мы получили сравнение $a \equiv c \pmod{m}$, которое завершает доказательство леммы.

Лемма 4.3. Пусть U целостное кольцо, m – отличный от нуля элемент кольца U и a – произвольный элемент кольца U . Рассмотрим множество

$$\overline{a_m} = \{a + km, k \in U\}$$

в котором элемент k пробегает все возможные значения из кольца U . Элемент $b \in U$ сравним с a тогда и только тогда, когда $b \in \overline{a_m}$.

Доказательство. Если $b \in \overline{a_m}$, то, в силу определения 4.1, найдется такой элемент $k \in U$, что $b = a + km$ или $b - a = km$. Отсюда следует, что $m | (b - a)$ и $a \equiv b \pmod{m}$.

Теперь обратное утверждение. Пусть элемент $b \in U$ сравним с элементом a по модулю m . Тогда $m | (b - a)$ и найдется элемент k кольца U такой, что $b - a = km$ или $b = a + km$. Последнее равенство говорит о том, что $b \in \overline{a_m}$.

Определение 4.2. Пусть m – отличный от нуля элемент целостного кольца U . Множество $\overline{a_m}$, определяемое равенством (4.1), будем называть классом вычетов по модулю m , элементы множества $\overline{a_m}$ – вычетами по модулю m или, просто, вычетами, а элемент $a \in U$ из равенства (4.1) будем называть представителем класса вычетов $\overline{a_m}$.

Определение 4.2. Пусть m – отличный от нуля элемент целостного кольца U . Множество $\overline{a_m}$, определяемое равенством (4.1), будем называть классом вычетов по модулю m , элементы множества $\overline{a_m}$ – вычетами по модулю m или, просто, вычетами, а элемент $a \in U$ из равенства (4.1) будем называть представителем класса вычетов $\overline{a_m}$.

Лемма 4.4. Пусть $\overline{a_m}$ класс вычетов по модулю m , тогда для любого $b \in \overline{a_m}$ выполнено равенство $\overline{b_m} = \overline{a_m}$, т.е. класс вычетов не зависит от выбора своего представителя.

Доказательство. Пусть $\overline{a_m} = \{a + km, k \in U\}$ и $b = a + km \in \overline{a_m}$. Рассмотрим произвольный элемент $c \in \overline{a_m}$. Тогда найдется элемент $l \in U$ такой, что

$$c = a + lm = b - km + lm = b + (k - l)m, k - l \in U.$$

Из данного равенства следует, что элемент $c \in \overline{b_m}$, следовательно в силу того, что элемент c был выбран произвольно, множество $\overline{a_m}$ содержится во множестве $\overline{b_m}$.

Аналогично, выбирая произвольный элемент $c \in \overline{b_m}$, $c = b + lm$, где $l \in U$, получим равенство

$$c = b + lm = a + km + lm = a + (k + l)m, k + l \in U,$$

из которого следует, что $c \in \overline{a_m}$ и включение $\overline{b_m} \subset \overline{a_m}$, следовательно, $\overline{b_m} = \overline{a_m}$.

11. Теорема о кольце классов вычетов

Определение 4.2. Пусть t – отличный от нуля элемент целостного кольца \mathbb{U} . Множество \bar{a}_m , определяемое равенством (4.1), будем называть классом вычетов по модулю t , элементы множества \bar{a}_m – вычетами по модулю t или, просто, вычетами, а элемент $a \in \mathbb{U}$ из равенства (4.1) будем называть представителем класса вычетов \bar{a}_m .

Лемма 4.4. Пусть \bar{a}_m класс вычетов по модулю t , тогда для любого $b \in \bar{a}_m$ выполнено равенство $\bar{b}_m = \bar{a}_m$, т.е. класс вычетов не зависит от выбора своего представителя.

Доказательство. Пусть $\bar{a}_m = \{a + km, k \in \mathbb{U}\}$ и $b = a + km \in \bar{a}_m$.

Рассмотрим произвольный элемент $c \in \bar{a}_m$. Тогда найдется элемент $l \in \mathbb{U}$ такой, что

$$c = a + lm = b - km + lm = b + (k - l)m, \quad k - l \in \mathbb{U}.$$

Из данного равенства следует, что элемент $c \in \bar{b}_m$, следовательно, в силу того, что элемент c был выбран произвольно, множество \bar{a}_m содержится во множестве \bar{b}_m .

Аналогично, выбирая произвольный элемент $c \in \bar{b}_m$, $c = b + lm$, где $l \in \mathbb{U}$, получим равенство

$$c = b + lm = a + km + lm = a + (k + l)m, \quad k + l \in \mathbb{U},$$

из которого следует, что $c \in \bar{a}_m$ и включение $\bar{b}_m \subset \bar{a}_m$, следовательно, $\bar{b}_m = \bar{a}_m$. Лемма доказана. \square

Лемма 4.5. Пусть t отличный от нуля элемент евклидового кольца \mathbb{U} . Пусть $a \in \mathbb{U}$ произвольный элемент, а r – остаток от деления элемента a на t , тогда

1. элемент a принадлежит классу вычетов \bar{r} ,
2. в случае, если остатков от деления несколько, то все они принадлежат одному классу вычетов.

Доказательство. Запишем равенство

$$a = qt + r, \quad 0 \leq N(r) < N(m),$$

тогда a принадлежит классу \bar{r} в силу определения класса вычетов, как множества элементов кольца \mathbb{U} , удовлетворяющих условию (4.1). Из леммы 4.3 также следует, что $a \equiv r \pmod{m}$.

Пусть в результате деления с остатком были получены два остатка r_1 и r_2 , удовлетворяющие равенствам

$$a = q_1t + r_1, \quad a = q_2t + r_2,$$

тогда выполнено $r_2 - r_1 = (q_1 - q_2)t$ и мы получаем, что $m|(r_2 - r_1)$. Таким образом выполнено сравнение $r_1 \equiv r_2 \pmod{m}$ которое, с учетом леммы 4.3, завершает доказательство. \square

Утверждение доказанной леммы позволяет предложить способ проверки, принадлежат ли два заданных элемента кольца одному классу вычетов.

Вернемся к вопросу о построении нового множества, состоящего из классов вычетов. Нам потребуется следующая лемма.

Лемма 4.6. Пусть \mathbb{U} евклидово кольцо и $t \in \mathbb{U}$ отличный от нуля элемент. Тогда каждый элемент кольца \mathbb{U} принадлежит только одному классу вычетов по модулю t .

Доказательство. Пусть элемент c принадлежит двум классам вычетов \bar{a} и \bar{b} . Тогда найдутся такие $k, l \in \mathbb{U}$, что $c = a + kt = b + lt$, следовательно $b - a = (k - l)t$ и $t|(b - a)$. Таким образом мы получили, что $a \equiv b \pmod{t}$ и, согласно первому утверждению леммы 4.1 и утверждению леммы 4.3, классы вычетов \bar{a} и \bar{b} совпадают. \square

Из утверждения леммы следует, что классы вычетов образуют непересекающиеся подмножества кольца \mathbb{U} , объединение которых образует все кольцо \mathbb{U} .

Пусть $a, b \in \mathbb{U}$ два элемента, не сравнимые между собой по модулю m . Из леммы 4.3 следует, что классы вычетов $\bar{a}, \bar{b} \in \mathbb{U}/(m)$ различны. Определим для данных классов операции сложения и умножения

$$\bar{c} = \bar{a} + \bar{b}, \quad \bar{d} = \bar{a} \cdot \bar{b}, \quad (4.2)$$

где представители классов \bar{c}, \bar{d} определяются условиями

$$c \equiv a + b \pmod{m}, \quad d \equiv ab \pmod{m}.$$

Теорема 4.1. *Пусть \mathbb{U} евклидово кольцо и $m \in \mathbb{U}$ отличный от нуля элемент. Множество классов вычетов $\mathbb{U}/(m)$ образует кольцо, относительно операций сложения и умножения, определенных равенствами (4.2).*

Доказательство. Для доказательства теоремы нам необходимо проверить выполнимость всех свойств определения 1.15. Начнем с операции сложения и рассмотрим два класса \bar{a}, \bar{b} , заданных своими представителями a, b и, используя операцию деления с остатком, определим элемент c равенством

$$a + b = qm + c.$$

Тогда $c \equiv a + b \pmod{m}$ и класс вычетов \bar{c} является суммой классов \bar{a} и \bar{b} . В силу коммутативности кольца \mathbb{U} получаем равенства $b + a = a + b = qm + c$ и

$$\bar{a} + \bar{b} = \bar{b} + \bar{a},$$

т.е. коммутативность введенной нами операции сложения.

Пусть 0 – нейтральный элемент кольца \mathbb{U} относительно операции сложения. Рассмотрим класс вычетов $\bar{0} = \{c \cdot m, c \in \mathbb{U}\}$, состоящий из всех элементов кольца, делящихся на m . Тогда $a \equiv a + 0 \pmod{m}$ и мы получаем, что класс $\bar{0}$ является нейтральным классом, относительно введенной нами операции сложения в $\mathbb{U}/(m)$.

Аналогично, из равенства $0 \equiv a + (-a) \pmod{m}$, выполненного для любого отличного от нуля $m \in \mathbb{U}$, мы получаем, что класс $\bar{-a}$ является обратным к классу \bar{a}_m , относительно введенной нами операции сложения в $\mathbb{U}/(m)$.

Теперь рассмотрим операцию умножения классов и определим элемент d равенством

$$ab = s \cdot m + d$$

для некоторого $s \in \mathbb{U}$. Выполнено равенство $d \equiv ab \pmod{m}$ из которого следует, что $\bar{a} \cdot \bar{b} = \bar{d}$. Из коммутативности операции умножения в кольце \mathbb{U} следует коммутативность операции умножения в $\mathbb{U}/(m)$.

Пусть 1 – нейтральный элемент кольца \mathbb{U} относительно операции умножения, тогда из сравнения $a \cdot 1 \equiv a \pmod{m}$ следует, что класс вычетов $\bar{1} = \{1 + k \cdot m, k \in \mathbb{U}\}$, является нейтральным классом, относительно введенной нами операции умножения в $\mathbb{U}/(m)$.

Нам осталось проверить дистрибутивность введенных операций сложения и умножения. В силу дистрибутивности кольца \mathbb{U} мы можем записать равенства

$$c(a + b) = ca + cb = qm + r$$

из которых следуют сравнения $c(a+b) \equiv r \pmod{m}$ и $ca+cb \equiv r \pmod{m}$, следовательно, класс вычетов \bar{r} совпадает как с классом $\bar{c}(\bar{a} + \bar{b})$, так и с классом $\bar{c} \cdot \bar{a} + \bar{c} \cdot \bar{b}$. Теорема доказана. \square

12. Теорема о количестве числа решений уравнения $ax = b(m)$

Теперь рассмотрим произвольный многочлен первой степени

$$f(x) = ax - b \in \mathbb{V}[x], \quad \text{где } a \not\equiv 0 \pmod{m},$$

и сравнение $f(x) \equiv 0 \pmod{m}$, которое может быть записано в виде

$$ax \equiv b \pmod{m}. \quad (5.1)$$

Верна следующая теорема.

Теорема 5.1. Пусть \mathbb{U} эвклидового кольца и a, b, m элементы кольца \mathbb{U} такие, что a, m отличны от нуля. Тогда количество классов вычетов, удовлетворяющих сравнению (5.1), равно

1. единице, если $1 \sim \text{НОД}(a, m)$,
2. числу классов вычетов по модулю $d = \text{НОД}(a, m)$, если $d|b$,
3. в противном случае сравнение неразрешимо.

Доказательство. Начнем с первого утверждения теоремы. Допустим, что выполнено условие $\text{НОД}(a, m) \sim 1$ и покажем, что в этом случае найдется класс вычетов по модулю m , удовлетворяющий сравнению (5.1).

Воспользуемся соотношением Безу (см. соотношение 2.4.А) и найдем $u, v \in \mathbb{U}$ такие, что

$$au + mv \sim \text{НОД}(a, m).$$

Тогда, учитывая, что $\text{НОД}(a, m) \sim 1$, найдется $\varepsilon \in \mathbb{U}^*$ такой, что

$$au + mv = \varepsilon \quad \text{или} \quad au\varepsilon^{-1} = 1 - mv\varepsilon^{-1}.$$

Следовательно, $au\varepsilon^{-1} \equiv 1 \pmod{m}$ и, умножая правую и левую части последнего сравнения на b , получим, что класс вычетов, представителем которого является $ub\varepsilon^{-1}$, удовлетворяет сравнению (5.1).

Покажем, что такой класс единственен. Для этого предположим обратное, т.е. то, что найдутся два различных класса вычетов, удовлетворяющих сравнению (5.1). Обозначим эти классы вычетов следующим образом

$$\bar{x}_1 = \{x_1 + k_1m, k_1 \in \mathbb{U}\}, \quad \bar{x}_2 = \{x_2 + k_2m, k_2 \in \mathbb{U}\}.$$

Поскольку данные классы удовлетворяют сравнению (5.1), то для любых двух представителей x_1, x_2 будет выполнено сравнение

$$ax_1 \equiv b \equiv ax_2 \pmod{m}.$$

Следовательно, в силу определения операции сравнения, выполнено равенство

$$m|ax_1 - ax_2 = a(x_1 - x_2),$$

и найдется такой элемент $u \in \mathbb{U}$, что $mu = a(x_1 - x_2)$. Поскольку **НОД**(a, m) ~ 1 , то из утверждения леммы 2.6 следует, что $m|(x_1 - x_2)$, и найдется элемент $v \in \mathbb{U}$ такой, что

$$mv = x_1 - x_2, \quad \text{или} \quad x_1 = x_2 + vm.$$

Тогда x_1 принадлежит классу вычетов \bar{x}_2 по модулю m и является его представителем, следовательно, в силу леммы 4.4, классы вычетов совпадают. Первое утверждение доказано.

Пусть **НОД**(a, m) = d , тогда из шестого утверждения леммы 4.1 следует, что элемент d должен делить элемент b . Если это условие не выполнено, то сравнение (5.1) неразрешимо.

Теперь будем считать, что $d|b$. Определим элементы $a_1, b_1, m_1 \in \mathbb{U}$ равенствами

$$a = a_1d, \quad b = b_1d, \quad m = m_1d.$$

Тогда из четвертого утверждения леммы 4.1 следует, что сравнение $a_1x \equiv b_1 \pmod{m_1}$ разрешимо. Поскольку $\text{НОД}(a_1, m_1) \sim 1$, то, в силу первого утверждения теоремы, это сравнение имеет единственное решение \bar{x}_{m_1} – класс вычетов по модулю m_1

$$\bar{x}_{m_1} = \{x + lm_1, l \in \mathbb{U}\}. \quad (5.2)$$

Выберем произвольный элемент кольца $l \in \mathbb{U}$ и зафиксируем элемент $x_l = x + lm$ – некоторый представитель класса вычетов \bar{x}_{m_1} . Поскольку выполнено сравнение $a_1x \equiv b_1 \pmod{m_1}$, то найдется элемент $k \in \mathbb{U}$ такой, что $a_1x_l = b_1 + km_1$, тогда

$$\begin{aligned} ax_l &= a_1dx_l = a_1d(x + lm_1) = \\ &= da_1x + lm_1d = d(b_1 + km_1) + lm_1d = b + (k + l)m, \end{aligned}$$

т.е. выполнено сравнение

$$ax_l \equiv b \pmod{m}$$

и x_l является представителем класса вычетов, удовлетворяющего сравнению (5.1). Нам осталось определить, сколько различных классов вычетов по модулю m содержится в определяемом равенством (5.2) множестве \bar{x}_{m_1} .

В силу свойств кольца \mathbb{U} найдется натуральное число n и конечное число элементов $r_1, \dots, r_n \in \mathbb{U}$, являющихся остатками от деления на d и представителями различных классов вычетов по модулю d , т.е.

$$r_i \not\equiv r_j \pmod{d}, \quad \text{при } i \neq j.$$

Теперь, используя операцию деления с остатком, для любого элемента $l \in \mathbb{U}$ можно определить элементы $q, r_i \in \mathbb{U}$, удовлетворяющие равенству $l = qd + r_i$, $0 \leq N(r_i) < N(d)$, для некоторого индекса i . Следовательно, для любого элемента из множества (5.2), выполнено равенство

$$x_l = x + lm_1 = x + (qd + r_i)m_1 = (x + r_i m_1) + qm,$$

т.е.

$$x_l \equiv x + r_i m_1 \pmod{m}.$$

Предположим, что найдутся два различных индекса $i, j \in \{1, \dots, n\}$ такие, что

$$x + r_i m_1 \equiv x + r_j m_1 \pmod{m},$$

тогда, учитывая второе утверждение леммы 4.1, получим сравнение

$$r_i m_1 \equiv r_j m_1 \pmod{m},$$

что равносильно условию $m|m_1(r_i - r_j)$. Учитывая равенство $m = dm_1$, мы можем считать, что найдется элемент $v \in \mathbb{U}$ такой, что

$$dm_1 v = mv = m_1(r_i - r_j), \quad \text{или} \quad d|(r_i - r_j).$$

Из последнего условия следует, что $r_i \equiv r_j \pmod{d}$, а это противоречит выбору остатков r_1, \dots, r_n . Следовательно, все величины $x + r_i m_1$, $i = 1, \dots, n$ принадлежат различным классам по модулю m . Что и требовалось доказать. \square

13. Расширенный алгоритм Евклида и его приложения

Пусть, как и ранее, \mathbb{U} эвклидового кольца, a, b, m элементы этого кольца и $m \neq 0$. Как мы показали выше, поиск классов вычетов, удовлетворяющих сравнению $ax \equiv b \pmod{m}$ сводится к соотношению Безу, т.е. поиску элементов $u, v \in \mathbb{U}$ таких, что

$$a_1u + m_1v \sim \text{НОД}(a_1, m_1),$$

и

$$a_1 = \frac{a}{d}, \quad m_1 = \frac{m}{d}, \quad d = \text{НОД}(a, m).$$

Данное нами ранее во второй главе доказательство теоремы 2.4, следствием которой является соотношение Безу, не было конструктивным и не содержало в себе каких-либо рекомендаций по поиску неизвестных значений u, v . Сейчас мы исправим эту ситуацию и опишем алгоритм, базирующийся на алгоритме Эвклида вычисления наибольшего общего делителя.

Пусть a, m произвольные элементы эвклидового кольца и r_{-1}, r_0, \dots последовательность элементов, удовлетворяющих равенствам $r_{-1} = m$, $r_0 = a$ и

$$\begin{aligned} r_{-1} &= r_0q_1 + r_1, \\ r_0 &= r_1q_2 + r_2, \\ r_1 &= r_2q_3 + r_3, \\ &\dots \\ r_{n-1} &= r_nq_{n+1}, \quad r_{n+1} = 0, \quad n \in \mathbb{N}_0. \end{aligned} \tag{5.3}$$

В силу утверждения теоремы 2.6 величина r_n является наибольшим общим делителем элементов a и m . Тогда, определим две последова-

тельности элементов u_{-1}, u_0, \dots и v_{-1}, v_0, \dots равенствами

$$\begin{aligned} u_{-1} &= 0, \\ u_0 &= 1, \\ v_{-1} &= 1, \\ v_0 &= 0, \\ u_{k+1} &= u_{k-1} - q_k u_k, \\ v_{k+1} &= v_{k-1} - q_k v_k. \end{aligned} \tag{5.4}$$

Теорема 5.2. Пусть a , m элементы евклидового кольца \mathbb{U} , последовательность элементов кольца r_{-1}, r_0, \dots, r_n определена равенствами (5.3) и представляет собой последовательность остатков в алгоритме Эвклида, а последовательности u_{-1}, u_0, \dots и v_{-1}, v_0, \dots определены равенствами (5.4). Тогда, выполнено равенство

$$au_k + mv_k = r_k, \quad k = -1, 0, \dots, n, \tag{5.5}$$

в частности $au_n + mv_n \sim \text{НОД}(a, m)$.

Доказательство. Легко видеть, что при $k = -1, 0$ равенство (5.5) выполнено в силу выбора элементов u_{-1}, v_{-1} и u_0, v_0 . Теперь предположим, что равенство (5.5) выполнено для всех значений $-1, 0, 1, \dots, k$ и покажем, что оно выполнено и для индекса $k + 1$. С учетом равенств (5.3) и (5.4) получаем

$$\begin{aligned} au_{k+1} + mv_{k+1} &= a(u_{k-1} - q_k u_k) + m(v_{k-1} - q_k v_k) = \\ &= au_{k-1} + mv_{k-1} - q(au_k + mv_k) = r_{k-1} - qr_k = r_{k+1}. \end{aligned}$$

Теорема доказана. □

Следствие 5.2.А. Пусть a, m элементы евклидового кольца \mathbb{U} и u, v элементы, удовлетворяющие соотношению Безу

$$au + mv \sim \text{НОД}(a, m).$$

Тогда для любого $s \in \mathbb{U}$ элементы

$$u_s = u - \frac{ms}{\text{НОД}(a, m)}, \quad v_s = v + \frac{as}{\text{НОД}(a, m)}$$

также удовлетворяют соотношению Безу.

Доказательство. Сформулированное утверждение следует из равенства

$$\begin{aligned} au_s + mv_s &= \\ &= a \left(u - \frac{ms}{\text{НОД}(a, m)} \right) + m \left(v + \frac{as}{\text{НОД}(a, m)} \right) = \\ &= au + mv \sim \text{НОД}(a, m). \end{aligned}$$

Кроме того, если $\text{НОД}(a, m) \sim 1$, в силу определения операции сравнения получаем, что

$$u_s \equiv u \pmod{m}, \quad v_s \equiv v \pmod{a}.$$

Следствие доказано. □

Следствие 5.2.В. Пусть $n \geq 2$ натуральное число и a_1, \dots, a_n произвольные элементы евклидового кольца \mathbb{U} . Тогда найдутся такие элементы $z_1, \dots, z_n \in \mathbb{U}$, что

$$a_1 z_1 + \dots + a_n z_n \sim \text{НОД}(a_1, \dots, a_n).$$

Доказательство. Определим последовательность элементов кольца $d_1, \dots, d_n \in \mathbb{U}$ условиями

$$d_1 = a_1, \quad d_k \sim \text{НОД}(d_{k-1}, a_k), \quad \text{для всех } k = 2, \dots, n.$$

Тогда, последний элемент этой последовательности d_n будет являться наибольшим общим делителем элементов a_1, \dots, a_n . С другой стороны, воспользовавшись утверждением теоремы 5.2, мы можем последовательно найти элементы u_k и v_k , для $k = 1, 2, \dots, n$, удовлетворяющие равенствам

$$a_k u_k + v_k d_{k-1} = \text{НОД}(a_k, d_{k-1}) = d_k, \quad \text{для всех } k = 2, \dots, n.$$

Тогда

$$\begin{aligned} d_n &= u_n a_n + v_n d_{n-1} = u_n a_n + v_n (u_{n-1} a_{n-1} + v_{n-1} d_{n-2}) = \\ &= u_n a_n + v_n u_{n-1} a_{n-1} + v_n v_{n-1} (u_{n-2} a_{n-2} + v_{n-2} d_{n-3}) = \dots \\ &\dots = u_n a_n + v_n u_{n-1} a_{n-1} + v_n v_{n-1} u_{n-2} a_{n-2} + \dots + v_n v_{n-1} \dots v_2 u_1 a_1, \end{aligned}$$

и мы получаем точные равенства для неизвестных z_1, \dots, z_n

$$\begin{aligned} z_n &= u_n, \\ z_{n-1} &= v_n u_{n-1}, \\ z_{n-2} &= v_n v_{n-1} u_{n-2}, \\ &\dots \\ z_2 &= v_n v_{n-1} \dots v_3 u_2, \\ z_1 &= v_n v_{n-1} \dots v_2 u_1. \end{aligned}$$

Следствие доказано. □

14. Китайская теорема об остатках

Переидем к рассмотрению систем сравнений и рассмотрим систему

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ \dots \\ x \equiv a_k \pmod{m_k}, \end{cases} \quad (5.6)$$

где элементы a_1, \dots, a_k и m_1, \dots, m_k принадлежат евклидовому кольцу \mathbb{U} , а кроме того,

$$\text{НОД}(m_i, m_j) \sim 1, \quad \text{при } i \neq j,$$

т.е. элементы m_1, \dots, m_k попарно взаимно-просты. Под решением указанной системы сравнений мы будем подразумевать множество элементов кольца \mathbb{U} , удовлетворяющих всем сравнениям, содержащимся в системе 5.6. Строение указанного множества решений дает следующая теорема.

сравнению

$$x \equiv \sum_{i=1}^k a_i b_i c_i \pmod{M}, \quad (5.7)$$

$$\text{где } b_i = \frac{1}{m_i} \left(\prod_{j=1}^k m_j \right) = \frac{M}{m_i} \text{ и } c_i \equiv b_i^{-1} \pmod{m_i}.$$

Доказательство. В силу выбора параметров b_i, c_i для каждого члена суммы, стоящей в правой части сравнения (5.7), выполнены сравнения

$$a_i b_i c_i \equiv a_i \pmod{m_i}, \quad a_i b_i c_i \equiv 0 \pmod{m_j}, \quad j \neq i, \quad i = 1, \dots, k,$$

из которых следует, что x удовлетворяет системе уравнений (5.6).

Покажем, что данное решение по модулю M единственno. Для этого предположим, что существует другое решение, скажем, y . Тогда выполнены сравнения $x - y \equiv 0 \pmod{m_i}$ для $i = 1, \dots, k$, или

$$x - y = m_1 c_1 = m_2 c_2 = \dots = m_k c_k,$$

при некоторых целых значениях c_1, \dots, c_k . Поскольку все числа m_1, \dots, m_k взаимно просты, то применяя лемму 2.6, получаем, что $m_i | c_j$ при всех $i \neq j$, что равносильно $x - y \equiv 0 \pmod{M}$. Последнее сравнение завершает доказательство теоремы. \square

Следствие 5.3.А. *Двум различным наборам элементов a_1, \dots, a_k и a'_1, \dots, a'_k кольца \mathbb{U} соответствуют два различных класса вычетов x и x' по модулю M , удовлетворяющих системе сравнений (5.6).*

Доказательство. Пусть наборы чисел a_1, \dots, a_k и a'_1, \dots, a'_k таковы, что найдется хотя бы один индекс j , $j = 1, \dots, k$ такой, что выполнено условие $a_j \not\equiv a'_j \pmod{m_i}$.

Определим, согласно (5.7), решения

$$x \equiv \sum_{i=1}^k a_i b_i c_i \pmod{M}, \quad x' \equiv \sum_{i=1}^k a'_i b_i c_i \pmod{M}$$

и предположим, что $x \equiv x' \pmod{M}$. Тогда для выбранного ранее индекса j будет выполнено $m_j | M$ и, следовательно, $x \equiv x' \pmod{m_j}$. Последнее сравнение равносильно $a_j \equiv a'_j \pmod{m_j}$, что противоречит нашему предположению. \square

Рассмотрим частный случай, который будет нам встречаться впоследствии несколько раз.

Следствие 5.3.В. *Пусть для всех индексов $i = 1, \dots, k$ выполнено неравенство $N(a) < N(m_i)$, тогда системе сравнений*

$$\begin{cases} x \equiv a \pmod{m_1}, \\ \dots \\ x \equiv a \pmod{m_k}, \end{cases}$$

удовлетворяет единственный класс вычетов $x \equiv a \pmod{M = m_1 \cdots m_k}$.

Доказательство. Очевидно, что $x \equiv a \pmod{M}$ удовлетворяет указанной системе сравнений. В силу первого следствия, такое решение единственно. \square

15. Функция Эйлера, ее свойства. Теорема Эйлера и малая теорема Ферма.

Рассмотрим целое неотрицательное число m и его полную систему вычетов

$$0, 1, \dots, m - 1.$$

Среди этого множества выберем вычеты, взаимно простые с m .

Определение 2.6. *Множество вычетов по модулю m , взаимно простых с модулем m , называется приведенной системой вычетов. Мощность этого множества обозначается символом $\varphi(m)$. Функция целочисленного аргумента $\varphi(m)$ называется функцией Эйлера.*

Для вычисления значения функции Эйлера может быть использована следующая теорема.

Теорема 2.5. Пусть m натуральное целое число, для которого известно разложение на простые множители $m = \prod_{i=1}^r p_i^{\alpha_i}$, p_i – простые числа. Тогда

$$\varphi(m) = \prod_{i=1}^r (p_i^{\alpha_i} - p_i^{\alpha_i-1}), \quad (2.12)$$

в частности, если p – простое, то

$$\varphi(p) = p - 1, \quad \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

Доказательство. Если p простое число, то среди чисел $0, 1, \dots, p-1$ взаимно простых с p ровно $p-1$ в силу условия **НОД**(0, p) = p (см. третье утверждение леммы 1.2). Следовательно, $\varphi(p) = p-1$.

Пусть $m = p^\alpha$ для некоторого целого $\alpha > 1$. Тогда для любого наименьшего неотрицательного вычета z , $0 \leq z < p^\alpha$, выполнено либо равенство **НОД**(z , p^α) = 1, либо условие $p \mid \text{НОД}(z, p^\alpha)$. Поскольку среди чисел $0, 1, \dots, p^\alpha - 1$ чисел кратных p ровно $p^{\alpha-1}$, то мы получаем, что $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Для доказательства основного утверждения теоремы нам осталось доказать, что функция Эйлера мультипликативна, то есть для любых взаимно простых чисел a, b выполнено равенство

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Тогда подставляя в это равенство разложение m на множители, получим утверждение теоремы.

Пусть α один из вычетов по модулю a , а β , соответственно, вычет по модулю b . Тогда согласно китайской теореме об остатках, теорема 2.3, существует единственный вычет $\gamma \pmod{ab}$ такой, что

$$\gamma \equiv \alpha \pmod{a}, \quad \gamma \equiv \beta \pmod{b}.$$

В случае, если α не взаимно просто с a , **НОД**(α , a) > 1 или β не взаимно просто с b , **НОД**(β , b) > 1, то мы сразу получаем, что **НОД**(γ , ab) > 1. И наоборот, **НОД**(γ , ab) = 1 только тогда, когда α и β взаимно просты, соответственно, с a и b .

Таким образом, мы получаем взаимно однозначное соответствие между двумя множествами – множеством взаимно простых вычетов по модулю ab и множеством вычетов по модулю a и b , следовательно, $\varphi(ab) = \varphi(a)\varphi(b)$. Теорема доказана. \square

Вынося в равенстве (2.12) за скобки общий множитель m , мы получаем следующее соотношение.

Следствие 1. Для $\varphi(m)$ выполнено равенство

$$\varphi(m) = m \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

Функция Эйлера играет важнейшую роль не только в теории чисел, но и в криптографии. Ее применение основывается на следующей важной теореме.

Теорема 2.6 (Теорема Эйлера). *Пусть $a, m > 0$ взаимно простые целые числа, то есть $\text{НОД}(a, m) = 1$. Тогда*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Доказательство. Рассмотрим приведенную систему вычетов по модулю m

$$1, \dots, m-1,$$

состоящую из $\varphi(m)$ различных вычетов.

Домножим каждый из вычетов данной системы на a и получим тоже самое множество вычетов, только записанное в другом порядке. Это позволяет нам получить равенство

$$(1)a \cdot \dots \cdot (m-1)a \equiv 1 \cdot \dots \cdot m-1 \pmod{m}.$$

Сокращая на множитель, стоящий в правой части сравнения, получим утверждение теоремы. \square

Частным случаем теоремы Эйлера является хорошо известная малая теорема Ферма. Действительно, применяя утверждение теоремы 2.5, получим следующий результат.

Теорема 2.7 (Малая теорема Ферма). *Пусть p простое число и a целое, взаимно простое с p число. Тогда выполнено сравнение*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Еще одним следствием теоремы Эйлера может служить способ вычисления обратного элемента по модулю составного числа. Если числа a и m взаимно просты, то для вычисления $a^{-1} \pmod{m}$ можно воспользоваться сравнением

$$a^{\varphi(m)} \equiv a \cdot a^{\varphi(m)-1} \equiv 1 \pmod{m},$$

откуда

$$a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}. \quad (2.13)$$

Вычисление по формуле (2.13) может быть использовано в тех ситуациях, когда не реализована операция деления с остатком, либо эта операция выполняется слишком медленно.

16. Схема ассиметричного шифрования RSA и ее связь с функцией Эйлера

Согласно статье Эллиса, первый вариант данной схемы был разработан сотрудником британской спецслужбы GCHQ² Клиффордом Коксом (Clifford Cocks) в ноябре 1973 года [20].

Для зашифрования сообщения ξ необходимо определить модуль схемы — нечетное составное число m , являющееся произведением двух простых чисел p и q таких, что

$$\text{НОД}(p, q - 1) = \text{НОД}(q, p - 1) = 1.$$

Число m является известным и является открытым ключом получателя сообщения, числа p и q являются секретными, секретным ключом получателя сообщения, и используются для расшифрования сообщения.

Сообщение ξ представляется³ в виде целого числа $1 < s < m$ и зашифровывается путем вычисления

$$c \equiv s^m \pmod{m}.$$

Вычет c является шифртекстом и передается по открытым каналам связи получателю сообщения.

Для расшифрования сообщения c Кокс предложил следующую последовательность действий. В начале вычисляются вычеты c_p и c_q , удовлетворяющие сравнениям

$$\begin{aligned} c_p &\equiv c^{z_q} \pmod{p}, \quad \text{где } z_q \equiv q^{-1} \pmod{p-1}, \\ c_q &\equiv c^{z_p} \pmod{q}, \quad \text{где } z_p \equiv p^{-1} \pmod{q-1}. \end{aligned}$$

Отметим, что вычеты c_p , c_q удовлетворяют сравнениям $c_p \equiv s \pmod{p}$, $c_q \equiv s \pmod{q}$. Действительно, учитывая малую теорему Ферма, теорема 2.7 и сравнение $qz_q \equiv 1 \pmod{p-1}$ получаем, что для вычета c_p выполнены сравнения

$$c_n \equiv c^{z_q} \equiv s^{pqz_q} \equiv s^p \equiv s \pmod{p}.$$

Аналогичные сравнения выполнены и для вычета c_q . Далее, используя китайскую теорему об остатках, теорема 2.3, находим вычет s , удовлетворяющий системе сравнений

$$\begin{cases} s \equiv c_p \pmod{p}, \\ s \equiv c_q \pmod{q}. \end{cases}$$

Для системы двух сравнений мы можем в явном виде предъявить значение s в виде

$$s = c_p q v + c_q p u,$$

где целые числа u, v удовлетворяют равенству $p u + q v = 1$ и могут быть найдены с помощью расширенного алгоритма Эвклида, см. алгоритм 2.1.

Отметим, что способ предложенный Коксом обладает рядом особенностей. Во первых значения вычетов z_p, z_q , а также чисел u, v , могут быть подсчитаны заранее, до получения сообщения s . Во вторых, при вычислении вычетов c_p, c_q используется возведение вычета в степень не более чем $\max\{p, q\}$, что являлось немаловажным при ручных вычислениях.

Естественным обобщением схемы Кокса является общезвестная схема RSA, предложенная в 1977 году и опубликованная лишь годом позже в статье [47].

Схема RSA названа по первым буквам фамилий ее авторов - Рона Райвеста (Ron Rivest), Ади Шамира (Adi Shamir) и Леонарда Эйдлемана (Leonard Adleman). В несколько модифицированном виде схема RSA активно применяется для шифрования данных в сети Internet и включена в различные международные и национальные стандарты в области информационной безопасности, среди которых можно отметить стандарты IEEE P1363 [?] и PKCS №1 [?].

Как и в схеме Кокса, необходимо определить модуль схемы — целое составное число m , являющееся произведением двух простых чисел p и q , а также секретный ключ d и открытый ключ e получателя сообщения, удовлетворяющие сравнению

$$ed \equiv 1 \pmod{\varphi(m)}, \quad 1 < e < \varphi(m), \quad 1 < d < \varphi(m), \quad (11.1)$$

где $\varphi(m)$ функция Эйлера, определенная равенством (2.12) и удовлетворяющая $\varphi(m) = (p-1)(q-1)$.

Сообщение ξ представляется в виде целого числа $1 < s < m$ и зашифровывается путем вычисления

$$c \equiv s^e \pmod{m}.$$

Вычет c является шифртекстом и передается по открытым каналам связи получателю сообщения.

Для расшифрования сообщения с необходимо вычислить

$$s \equiv c^d \pmod{m}.$$

Последнее сравнение выполнено, поскольку из сравнения (11.1) и теоремы Эйлера, см. теорему 2.6, следует $c^d \equiv s^{ed} \equiv s^1 \pmod{\varphi(m)} \equiv s \pmod{m}$.

Легко видеть, что схема Кокса является частным случаем схемы RSA при $e \equiv m \pmod{\varphi(m)}$. Способ расшифрования сообщений в схеме RSA, очевидно, может быть применен и для расшифрования сообщений в схеме Кокса.

Стойкость криптосхемы RSA основывается на трудоемкости решения задачи разложения числа m на два простых множителя. Как мы показали в предыдущих лекциях, решение этой задачи при больших значениях m является сложным. Вместе с тем, в схеме RSA присутствуют дополнительные параметры, а именно, секретный и открытый ключи d и e , а также собственно сообщение s , которое зашифровывается и передается по каналам связи. В некоторых случаях удается использовать эту дополнительную информацию для компрометации схемы. Прежде чем привести несколько примеров, сведем все параметры в одну таблицу.

Известные значения	Неизвестные значения
m, e, c	$d, p, q, \varphi(m), s$

17. Теорема о числе корней многочлена по простому модулю

Теперь мы можем рассмотреть общий случай. Рассмотрим сравнение второй степени

$$ax^2 + bx + c \equiv 0 \pmod{p}, \quad (4.14)$$

где p – нечетное простое число, $a \not\equiv 0 \pmod{p}$ и b, c – произвольные вычеты по модулю p .

Верна следующая теорема.

Теорема 4.2. *Пусть p нечетное простое число, a, b, c целые числа и a взаимно просто с p . Пусть $D \equiv b^2 - 4ac \pmod{p}$. Тогда*

1. если $\left(\frac{D}{p}\right) = -1$, то сравнение (4.14) не имеет решений,
2. если $D \equiv 0 \pmod{p}$, то сравнение (4.14) имеет единственное решение $e \equiv -\frac{b}{2a} \pmod{p}$,
3. если $\left(\frac{D}{p}\right) = 1$, то сравнение (4.14) имеет два различных решения e_1, e_2 , которые удовлетворяют сравнениям

$$e_1 \equiv \frac{-b - \xi}{2a} \pmod{p}, \quad e_2 \equiv \frac{-b + \xi}{2a} \pmod{p},$$

где $\xi^2 \equiv D \pmod{p}$.

Доказательство. Легко заметить, что решения сравнения $ax^2 + bx + c \equiv 0 \pmod{p}$ удовлетворяют также сравнению

$$x^2 + \frac{bx}{a} + \frac{c}{a} \equiv \left(x + \frac{b}{2a}\right)^2 - \left(\frac{D}{4a^2}\right) \equiv 0 \pmod{p}$$

и разрешимость сравнения (4.14) эквивалентна разрешимости сравнения

$$z^2 \equiv D \pmod{p}, \quad \text{где } z \equiv 2ax + b \pmod{p}.$$

Таким образом, мы свели поиск корней многочлена второй степени к поиску квадратных корней из D . Теперь все утверждения доказываемой нами теоремы вытекают из теоремы 4.1. \square

Мы доказали результат о разрешимости сравнения (4.14) по модулю простого числа p в зависимости от величины дискриминанта D . Теперь получим обратное утверждение – о разрешимости сравнения (4.14) для бесконечного множества простых чисел.

18. Теорема о числе решений многочлена по составному модулю

Рассмотрим вопрос о нахождении корней многочлена. Выберем некоторое целое число $m > 0$ с известным разложением на простые множители

$$m = \prod_{i=1}^k p_i^{\alpha_i}, \quad \alpha_i \in \mathbb{N}, \quad \alpha_i > 0, \quad (3.14)$$

и будем считать, что $\mathbb{U} = \mathbb{Z}_m$.

Рассмотрим произвольный многочлен $f(x)$ с целыми коэффициентами и зададимся вопросом о том, как найти его корни в кольце \mathbb{Z}_m . Другими словами, необходимо найти все решения уравнения $f(x) \equiv 0 \pmod{m}$ в кольце \mathbb{Z}_m .

Теорема 3.4. *Пусть $f(x)$ многочлен с целыми коэффициентами и $m > 0$ целое число, для которого известно разложение на простые множители (3.14). Тогда множество целых чисел, удовлетворяющих сравнению*

$$f(x) \equiv 0 \pmod{m} \quad (3.15)$$

и системе сравнений

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{\alpha_1}}, \\ \dots, \\ f(x) \equiv 0 \pmod{p_k^{\alpha_k}}, \end{cases} \quad (3.16)$$

совпадают.

Обозначим символом $N(m)$ число решений сравнения (3.15), тогда выполнено равенство

$$N(m) = N(p_1^{\alpha_1}) \cdots N(p_k^{\alpha_k}).$$

Доказательство. Пусть целое число e удовлетворяет сравнению (3.15). Тогда $m|f(e)$ и для любого индекса $i = 1, \dots, k$, выполнено $p_i^{\alpha_i}|f(e)$, следовательно, e удовлетворяет системе сравнений (3.16).

Обратно, если e удовлетворяет системе сравнений (3.16), то $p_i^{\alpha_i}|f(e)$ для любого $i = 1, \dots, k$, то есть $f(e)$ является общим кратным чисел $p_1^{\alpha_1}, \dots, p_k^{\alpha_k}$. Согласно лемме 2.6 наименьшее кратное чисел $p_1^{\alpha_1}, \dots, p_k^{\alpha_k}$ есть m . Следовательно, $m|f(e)$ и e является решением системы сравнений (3.16).

Предъявим способ построения решения сравнения (3.15) по известным решениям системы (3.16). Пусть числа a_1, \dots, a_k являются решением системы сравнений (3.16). Согласно «китайской теореме об остатках», теорема 2.3, найдется вычет e по модулю m такой, что $e \equiv a_i \pmod{p_i^{\alpha_i}}$ для всех $i = 1, \dots, k$. Тогда $f(e) \equiv f(a_i) \equiv 0 \pmod{p_i^{\alpha_i}}$ и, по доказанному ранее, e является решением сравнения (3.15).

Далее, пусть числа a_1, \dots, a_k пробегают все возможные наборы значений, являющихся решением системы (3.16), тогда, согласно следствию к теореме 2.3, соответствующие им решения принимают различные значения по модулю m . Таким образом, число решений сравнения (3.15) не менее $N(p_1^{\alpha_1}) \cdots N(p_k^{\alpha_k})$.

По доказанному ранее, каждое решение e сравнения (3.15) удовлетворяет системе сравнений (3.16) и, следовательно, ему соответствует некоторый набор чисел a_1, \dots, a_k . Это доказывает, что других решений, отличных от построенных, сравнение (3.15) не имеет. \square

Доказанная нами теорема сводит поиск корней сравнения (3.15) к поиску корней сравнения $f(x) \equiv 0 \pmod{p^\alpha}$ для некоторого простого числа p и натурального α .

Легко видеть, что если e является корнем $f(x) \pmod{p^\alpha}$, то это же значение должно являться корнем $f(x) \pmod{p}$: из условия $p^\alpha|f(e)$ очевидным образом следует условие $p|f(e)$. Таким образом, существование корня многочлена $f(x) \pmod{p}$ становится необходимым признаком существования корня многочлена $f(x) \pmod{p^\alpha}$.

Допустим, что нам известен корень многочлена $f(x) \pmod{p}$. Следующая теорема дает ответ на вопрос – как найти корень многочлена $f(x) \pmod{p^\alpha}$.

Теорема 3.5. Пусть p простое число, $f(x)$ многочлен с целыми коэффициентами и e целое число, удовлетворяющее условиям

$$f(e) \equiv 0 \pmod{p}, \quad f'(e) \not\equiv 0 \pmod{p}.$$

Тогда при любом натуральном $\alpha \geq 1$ существует единственное решение сравнения

$$f(x) \equiv 0 \pmod{p^\alpha},$$

принадлежащее классу вычетов $x \equiv e \pmod{p}$.

Доказательство. Докажем теорему индукцией по степеням простого числа p . При $\alpha = 1$, утверждение теоремы, очевидно, выполняется.

Предположим, что утверждение теоремы выполнено для всех целых степеней, меньших либо равных α , и обозначим e_α корень многочлена $f(x) \pmod{p^\alpha}$, то есть $f(e_\alpha) \equiv 0 \pmod{p^\alpha}$ и $e_\alpha \equiv e \pmod{p}$.

Обозначим $e_{\alpha+1}$ корень многочлена $f(x) \pmod{p^{\alpha+1}}$ и будем искать его в виде

$$e_{\alpha+1} = e_\alpha + tp^\alpha, \quad t \in \mathbb{Z}, \quad 0 \leq t < p. \quad (3.17)$$

Тогда $e_{\alpha+1} \equiv e_\alpha \equiv e \pmod{p}$. Воспользуемся равенством (3.9) и запишем сравнение

$$f(e_{\alpha+1}) = f(e_\alpha + tp^\alpha) \equiv f(e_\alpha) + tp^\alpha f'(e_\alpha) \pmod{p^{2\alpha}}.$$

Поскольку мы считаем, что $e_{\alpha+1}$ является корнем, то мы можем записать равенство

$$0 = f(e_\alpha) + tp^\alpha f'(e_\alpha) + hp^{\alpha+1},$$

для некоторого целого значения h . По предположению индукции $f(e_\alpha)$ делится на p^α , следовательно, сокращая полученное равенство на p^α , получаем сравнение

$$t \equiv -\frac{f(e_\alpha)}{p^\alpha f'(e_\alpha)} \pmod{p}. \quad (3.18)$$

Поскольку $f'(e_\alpha) \not\equiv 0 \pmod{p}$, то неизвестное значение t единственным образом определяется сравнением (3.18). \square

Таким образом, если нам известны корни многочлена $f(x)$ по модулю простого числа p , то теорема 3.5 дает нам способ определения всех корней многочлена $f(x)$ по модулю p^α . Этот способ часто называют подъемом решения. Однако он не работает, если многочлен $f(x)$ имеет кратные корни.

Действительно, согласно основной теореме арифметики для многочленов, если e корень многочлена $f(x) \pmod{p}$, то

$$f(x) \equiv (x - e)^\gamma u(x) \pmod{p}, \quad \text{НОД}((x - e), u(x)) = 1,$$

где натуральное число $\gamma \geq 1$ является кратностью корня e . Для производной многочлена выполнено сравнение

$$\begin{aligned} f'(x) &\equiv \gamma(x - e)^{\gamma-1}u(x) + (x - e)^\gamma u'(x) \equiv \\ &\equiv (x - e)^{\gamma-1}(\gamma u(x) + u'(x)) \pmod{p}, \end{aligned}$$

из которого следует, что при $\gamma > 1$ выполнено $f'(e) \equiv 0 \pmod{p}$ и условия теоремы 3.5 не выполнены.

Теорема 3.6. Пусть p простое число, $f(x)$ многочлен с целыми коэффициентами и e целое число, удовлетворяющее условиям

$$f(e) \equiv 0 \pmod{p}, \quad f'(e) \equiv 0 \pmod{p}.$$

Пусть $\beta \geq 1$ максимальное число такое, что $f(e) \equiv 0 \pmod{p^\beta}$. Тогда сравнение $f(x) \equiv 0 \pmod{p^\alpha}$ разрешимо только при $\alpha \leq \beta$ и корнем является значение e .

Доказательство. Очевидно, что при $\alpha \leq \beta$ из сравнения $f(e) \equiv 0 \pmod{p^\beta}$ следует утверждение теоремы. Покажем, что при $\alpha > \beta$ решений не существует.

Обозначим $e_{\beta+1} = e + tp^{\beta+1}$ и запишем сравнение

$$f(e_{\beta+1}) = f(e) + tp^{\beta+1}f'(e) \pmod{p^{2(\beta+1)}}.$$

Если $p^{\beta+1}$ не делит $f(e)$, то правая часть в приведенном сравнении не делится на $p^{\beta+1}$. Отсюда следует, что $f(e_{\beta+1})$ не делится на $p^{\beta+1}$, следовательно, теорема доказана. \square

19. Теорема о подъеме числа решений

Допустим, что нам известен корень многочлена $f(x) \pmod{p}$. Следующая теорема дает ответ на вопрос – как найти корень многочлена $f(x) \pmod{p^\alpha}$.

Теорема 3.5. Пусть p простое число, $f(x)$ многочлен с целыми коэффициентами и e целое число, удовлетворяющее условиям

$$f(e) \equiv 0 \pmod{p}, \quad f'(e) \not\equiv 0 \pmod{p}.$$

Тогда при любом натуральном $\alpha \geq 1$ существует единственное решение сравнения

$$f(x) \equiv 0 \pmod{p^\alpha},$$

принадлежащее классу вычетов $x \equiv e \pmod{p}$.

Доказательство. Докажем теорему индукцией по степеням простого числа p . При $\alpha = 1$, утверждение теоремы, очевидно, выполняется.

Предположим, что утверждение теоремы выполнено для всех целых степеней, меньших либо равных α , и обозначим e_α корень многочлена $f(x) \pmod{p^\alpha}$, то есть $f(e_\alpha) \equiv 0 \pmod{p^\alpha}$ и $e_\alpha \equiv e \pmod{p}$.

Обозначим $e_{\alpha+1}$ корень многочлена $f(x) \pmod{p^{\alpha+1}}$ и будем искать его в виде

$$e_{\alpha+1} = e_\alpha + tp^\alpha, \quad t \in \mathbb{Z}, \quad 0 \leq t < p. \quad (3.17)$$

Тогда $e_{\alpha+1} \equiv e_\alpha \equiv e \pmod{p}$. Воспользуемся равенством (3.9) и запишем сравнение

$$f(e_{\alpha+1}) = f(e_\alpha + tp^\alpha) \equiv f(e_\alpha) + tp^\alpha f'(e_\alpha) \pmod{p^{2\alpha}}.$$

Поскольку мы считаем, что $e_{\alpha+1}$ является корнем, то мы можем записать равенство

$$0 = f(e_\alpha) + tp^\alpha f'(e_\alpha) + hp^{\alpha+1},$$

для некоторого целого значения h . По предположению индукции $f(e_\alpha)$ делится на p^α , следовательно, сокращая полученное равенство на p^α , получаем сравнение

$$t \equiv -\frac{f(e_\alpha)}{p^\alpha f'(e_\alpha)} \pmod{p}. \quad (3.18)$$

Поскольку $f'(e_\alpha) \not\equiv 0 \pmod{p}$, то неизвестное значение t единственным образом определяется сравнением (3.18). \square

Таким образом, если нам известны корни многочлена $f(x)$ по модулю простого числа p , то теорема 3.5 дает нам способ определения всех корней многочлена $f(x)$ по модулю p^α . Этот способ часто называют подъемом решения. Однако он не работает, если многочлен $f(x)$ имеет кратные корни.

Действительно, согласно основной теореме арифметики для многочленов, если e корень многочлена $f(x) \pmod{p}$, то

$$f(x) \equiv (x - e)^\gamma u(x) \pmod{p}, \quad \text{НОД}((x - e), u(x)) = 1,$$

где натуральное число $\gamma \geq 1$ является кратностью корня e . Для производной многочлена выполнено сравнение

$$\begin{aligned} f'(x) &\equiv \gamma(x - e)^{\gamma-1}u(x) + (x - e)^\gamma u'(x) \equiv \\ &\equiv (x - e)^{\gamma-1}(\gamma u(x) + u'(x)) \pmod{p}, \end{aligned}$$

из которого следует, что при $\gamma > 1$ выполнено $f'(e) \equiv 0 \pmod{p}$ и условия теоремы 3.5 не выполнены.

Теорема 3.6. Пусть p простое число, $f(x)$ многочлен с целыми коэффициентами и e целое число, удовлетворяющее условиям

$$f(e) \equiv 0 \pmod{p}, \quad f'(e) \equiv 0 \pmod{p}.$$

Пусть $\beta \geq 1$ максимальное число такое, что $f(e) \equiv 0 \pmod{p^\beta}$. Тогда сравнение $f(x) \equiv 0 \pmod{p^\alpha}$ разрешимо только при $\alpha \leq \beta$ и корнем является значение e .

Доказательство. Очевидно, что при $\alpha \leq \beta$ из сравнения $f(e) \equiv 0 \pmod{p^\beta}$ следует утверждение теоремы. Покажем, что при $\alpha > \beta$ решений не существует.

Обозначим $e_{\beta+1} = e + tp^{\beta+1}$ и запишем сравнение

$$f(e_{\beta+1}) = f(e) + tp^{\beta+1}f'(e) \pmod{p^{2(\beta+1)}}.$$

Если $p^{\beta+1}$ не делит $f(e)$, то правая часть в приведенном сравнении не делится на $p^{\beta+1}$. Отсюда следует, что $f(e_{\beta+1})$ не делится на $p^{\beta+1}$, следовательно, теорема доказана. \square

20. Квадратичные вычеты. Понятие символа Лежандра. Критерий Эйлера. Формулировка квадратичного закона взаимности

Рассмотрим вопрос о нахождении корней многочленов по модулю простого числа p . Вначале мы рассмотрим случай многочленов второй степени, а потом перейдем к поиску корней многочленов произвольной степени.

Мы начнем с самого простого случая, а именно, с уравнения

$$x^2 \equiv a \pmod{p}. \quad (4.1)$$

Для x , удовлетворяющего (4.1), мы будем использовать выражение «квадратный корень из a по модулю простого числа p ».

4.1 Квадратичные вычеты

Рассмотрим вопрос о разрешимости сравнения (4.1).

Лемма 4.1. *Пусть p нечетное простое число, a – целое число, взаимно простое с p . Если сравнение (4.1) разрешимо, то оно имеет два различных решения.*

Доказательство. Вначале заметим, что из условия $\text{НОД}(a, p) = 1$ и третьего утверждения леммы 1.2 следует, что $a \not\equiv 0 \pmod{p}$.

Пусть x_1 – некоторое, отличное от нуля решение сравнения (4.1). Обозначим $x_2 \equiv -x_1 \pmod{p}$. Тогда x_2 также является решением сравнения (4.1), в силу того, что $(x_2)^2 \equiv (-x_1)^2 \equiv a \pmod{p}$.

Второе решение отлично от первого, так как в противном случае были бы выполнены сравнения

$$x_2 \equiv x_1 \pmod{p} \quad \text{или} \quad 2x_1 \equiv 0 \pmod{p},$$

что невозможно, так как $\text{НОД}(2, p) = \text{НОД}(x_1, p) = 1$ и $x_1 \neq 0$. \square

–

В случае, когда p четное простое число, то есть $p = 2$, решения сравнения (4.1) легко выписать в явном виде. Действительно, для a возможно всего два варианта $a = 0$ или 1 , из чего вытекает, что $x \equiv a \pmod{2}$.

Определение 4.1. Пусть a, p – целые, взаимно простые числа. Мы будем называть целое число a квадратичным вычетом по модулю p , если разрешимо сравнение (4.1). В противном случае мы будем называть число a квадратичным невычетом.

Следующая лемма позволяет получить узнать точное число квадратичных вычетов и квадратичных невычетов по модулю простого числа.

Лемма 4.2. Пусть p нечетное простое число. Среди чисел $1, 2, \dots, p-1$ содержится равное число квадратичных вычетов и квадратичных невычетов по модулю p .

Доказательство. Среди вычетов $1, 2, \dots, p-1$ квадратичными вычетами являются только те, квадраты которых сравнимы с числами

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2. \quad (4.2)$$

Для вычетов k таких, что $1 \leq k \leq \frac{p-1}{2}$, это очевидно. Для остальных вычетов, при $\frac{p-1}{2} < k \leq p-1$, выполнено

$$k^2 \equiv (p-k)^2 \equiv l^2 \pmod{p}, \quad \text{где } 1 \leq l < \frac{p-1}{2}.$$

Пусть среди чисел (4.2) найдется хотя бы одна пара совпадающих, то есть

$$k^2 \equiv l^2 \pmod{p}, \quad 1 \leq k < l \leq \frac{p-1}{2}.$$

Тогда сравнению $x^2 \equiv l^2 \pmod{p}$ удовлетворяет четыре решения: $k, l, -k$ и $-l$, что противоречит лемме 4.1.

Следовательно, числа (4.2) попарно несравнимы и среди всех вычетов по модулю p : $1, 2, \dots, p-1$ найдется ровно $\frac{p-1}{2}$ квадратичных вычетов. Остальные – квадратичные невычеты. \square

Определение 4.2. Пусть p нечетное простое число, a – целое число, взаимно простое с p . Мы будем называть символом Лежандра и обозначать символом $\left(\frac{a}{p}\right)$ функцию, удовлетворяющую равенству

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

Сформулируем теорему о числе решений сравнения (4.1).

Теорема 4.1. Пусть p нечетное простое число. Тогда число решений сравнения $x^2 \equiv a \pmod{p}$ может равняться нулю, если $\left(\frac{a}{p}\right) = -1$, единице, если $a \equiv 0 \pmod{p}$, и двум, если $\left(\frac{a}{p}\right) = 1$.

Доказательство. Доказательство первого и третьего утверждений теоремы, очевидно, следует из леммы 4.1 и определения символа Лежандра.

Нам осталось доказать второе утверждение при $a \equiv 0 \pmod{p}$. Легко видеть, что $x \equiv 0 \pmod{p}$ является решением сравнения (4.1). Пусть существует второе решение z такое, что $z \not\equiv 0 \pmod{p}$. Тогда равенство (4.1) можно записать в виде

$$zz = kp, \tag{4.3}$$

при некотором целом k .

Поскольку p простое число, то $\text{НОД}(z, p) = 1$ и из леммы 1.4 следует, что $k|z$. Тогда, сокращая в равенстве (4.3) множитель $z \neq 0$, получаем, что $z = lp$ или, что равносильно, $z \equiv 0 \pmod{p}$. Мы получили противоречие с выбором z , которое завершает доказательство теоремы. \square

Для проверки разрешимости сравнения (4.1) нам нужен эффективный алгоритм вычисления символа Лежандра. Докажем лемму, утверждения которой позволяют предъявить искомый алгоритм.

Лемма 4.3. Пусть p нечетное простое число, а целое число, взаимно простое с p , тогда для символа Лежандра $\left(\frac{a}{p}\right)$ выполнены следующие свойства.

1. Если $a \equiv b \pmod{p}$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. Выполнено сравнение $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$, которое принято называть «критерием Эйлера».
3. Верны равенства $\left(\frac{1}{p}\right) = 1$ и $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
4. Если $a = bc$, $a \neq 0$, где b, c целые числа, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \left(\frac{c}{p}\right)$.
5. Выполнено сравнение $\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}$.
6. Пусть числа a и p – нечетные простые, тогда

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

Последнее равенство принято называть «квадратичным законом взаимности Гаусса».

Доказательство. Первое утверждение леммы следует из того, что разрешимость сравнения (4.1) не зависит от представителя класса вычетов по модулю p .

Перейдем к доказательству с критерия Эйлера. Поскольку $p - 1$ является четным числом, то в силу малой теоремы Ферма, см. теорему 2.7, выполнено сравнение

$$a^{p-1} - 1 \equiv \left(a^{\frac{p-1}{2}} - 1\right) \left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}.$$

Тогда из леммы 1.4 следует, что для любого a , $\text{НОД}(a, p) = 1$, выполнено одно из сравнений

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \quad (4.4)$$

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \quad (4.5)$$

Пусть a квадратичный вычет по модулю p и x решение сравнения (4.1). Поскольку x взаимно просто с p , то применяя малую теорему Ферма, см теорему 2.7, получаем

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

Следовательно, любой квадратичный вычет a удовлетворяет сравнению (4.4).

Оставшиеся $\frac{p-1}{2}$ значений удовлетворяют сравнению (4.5) и, согласно лемме 4.2, являются квадратичными невычетами. Критерий Эйлера доказан.

Третье утверждение леммы, очевидно, вытекает из второго и не требует отдельного доказательства.

Критерий Эйлера позволяет доказать и четвертое утверждение леммы. Действительно, если $a = bc$, то

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv \left(b^{\frac{p-1}{2}}\right) \cdot \left(c^{\frac{p-1}{2}}\right) \equiv \left(\frac{b}{p}\right) \left(\frac{c}{p}\right) \pmod{p}.$$

Из четвертого утверждения леммы следует, что в числителе символа Лежандра можно отбросить любой квадратный множитель, то есть выполнено равенство

$$\left(\frac{a^2 b}{p} \right) = \left(\frac{b}{p} \right).$$

□

Для доказательства двух последних утверждений леммы нам потребуются дополнительные усилия. Из достаточно обширного списка опубликованных на русском языке доказательств квадратичного закона взаимности, мы остановимся на классическом доказательстве, изложенном в книге [10]. Это третье доказательство квадратичного закона взаимности из шести, данных Гауссом, последняя его часть принадлежит Кронекеру. Нам потребуется еще одна лемма.

Лемма 4.4 (Гаусс). *Пусть p нечетное простое число, a целое число, взаимно простое с p , $\text{НОД}(a, p) = 1$, тогда для символа Лежандра $\left(\frac{a}{p} \right)$ выполнено равенство*

$$\left(\frac{a}{p} \right) = (-1)^\mu,$$

где μ число отрицательных абсолютно-наименьших вычетов по модулю p (см. определение 2.4) среди чисел $a, 2a, \dots, \frac{p-1}{2}a$.

Доказательство. Обозначим символами

$$a_1, a_2, \dots, a_\lambda, -b_1, -b_2, \dots, -b_\mu, \quad (4.6)$$

абсолютно наименьшие вычеты чисел $a, 2a, \dots, \frac{p-1}{2}a$ по модулю p , то есть для всех $i = 1, \dots, \lambda, j = 1, \dots, \mu$ выполнено

$$-\frac{p-1}{2} \leq a_i \leq \frac{p-1}{2}, \quad -\frac{p-1}{2} \leq -b_j \leq \frac{p-1}{2}.$$

Мы считаем, что все a_i, b_j положительны, поэтому в (4.6) содержится λ положительных чисел и μ отрицательных и $\lambda + \mu = \frac{p-1}{2}$. Все числа

$$a_1, a_2, \dots, a_\lambda, b_1, b_2, \dots, b_\mu,$$

целые, положительные, различные по модулю p и меньшие, чем $\frac{p}{2}$, следовательно, ими исчерпывается множество всех целых чисел от 1 до $\frac{p-1}{2}$. Перемножая их, получим равенство

$$a_1 a_2 \cdots a_\lambda b_1 b_2 \cdots b_\mu = \left(\frac{p-1}{2} \right)!. \quad (4.7)$$

Каждое из чисел (4.6) сравнимо только с одним произведением ka , где $k = 1, \dots, \frac{p-1}{2}$, таким образом, с учетом равенства (4.7) получаем сравнение

$$\begin{aligned} \left(\frac{p-1}{2} \right)! a^{\frac{p-1}{2}} &= a \cdot 2a \cdots \frac{p-1}{2} \equiv a_1 a_2 \cdots a_\lambda b_1 b_2 \cdots b_\mu (-1)^\mu \equiv \\ &\equiv \left(\frac{p-1}{2} \right)! (-1)^\mu \pmod{p}. \end{aligned}$$

Сокращая обе части сравнения на множитель $\left(\frac{p-1}{2} \right)!$ получаем сравнение

$$(-1)^\mu \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p} \right) \pmod{p},$$

которое выполнено в силу критерия Эйлера, см. утверждение 2 леммы 4.3. Учитывая, что в правой и левой частях приведенного сравнения стоят числа, не превосходящие по абсолютной величине единицы, то разность между ними, по абсолютной величине, не превосходит двух и меньше любого нечетного простого числа p . Следовательно, мы можем заменить знак сравнения на знак равенства. Лемма доказана. \square

Завершение доказательства леммы 4.3. Рассмотрим оставшиеся утверждения. Для этого зафиксируем множество чисел $a, 2a, \dots, \frac{p-1}{2}a$ и разделим каждое из них с остатком на p

$$\begin{cases} a = q_1 p + r_1, \\ 2a = q_2 p + r_2, \\ \dots \\ \frac{p-1}{2}a = q_{\frac{p-1}{2}} p + r_{\frac{p-1}{2}}, \end{cases} \quad (4.8)$$

где $0 \leq r_k < p$, $1 \leq k \leq \frac{p-1}{2}$. В обозначениях леммы Гаусса (лемма 4.4) получаем, что остатки r_k совпадают со множеством чисел

$$a_1, a_2, \dots, a_\lambda, p - b_1, p - b_2, \dots, p - b_\mu,$$

следовательно, можно записать равенство

$$\sum_{k=1}^{\frac{p-1}{2}} r_k = A - B + \mu p, \quad A = a_1 + \dots + a_\lambda, \quad B = b_1 + \dots + b_\mu.$$

Сложим почленно все равенства в (4.8) и, учитывая равенство¹

$$1 + 2 + \dots + \frac{p-1}{2} = \left(1 + \frac{p-1}{2}\right) \frac{p-1}{4} = \frac{p^2-1}{8},$$

получим

$$a \left(\frac{p^2-1}{8} \right) = p \sum_{k=1}^{\frac{p-1}{2}} q_k + A - B + \mu p. \quad (4.9)$$

Из доказательства леммы Гаусса следует, что все числа a_1, \dots, a_λ и b_1, \dots, b_μ суть числа от 1 до $\frac{p-1}{2}$. Следовательно,

$$A + B = 1 + 2 + \dots + \frac{p-1}{2} = \frac{p^2-1}{8}, \quad \text{или} \quad A = \frac{p^2-1}{8} - B.$$

Подставляя в (4.9) полученные равенства и перенося $\frac{p^2-1}{8}$ в правую часть, получим

$$\frac{p^2-1}{8}(a-1) = p \sum_{k=1}^{\frac{p-1}{2}} q_k - 2B + \mu p. \quad (4.10)$$

Поскольку p нечетное число, то выполнено сравнение $p \equiv 1 \pmod{2}$. Пусть $a = 2$, тогда равенство (4.10) может быть записано в виде сравнения

$$\frac{p^2-1}{8} \equiv \sum_{k=1}^{\frac{p-1}{2}} q_k + \mu \pmod{2}.$$

Заметим, что при $a = 2$ значения всех q_k , $1 \leq k \leq \frac{p-1}{2}$, определяемых равенствами (4.8), равны нулю. Это, очевидно, следует из того, что все числа вида ka при всех $1 \leq k \leq \frac{p-1}{2}$ не превосходят величины p . Таким образом,

$$\frac{p^2-1}{8} \equiv \mu \pmod{2}$$

¹Мы используем равенство $1 + 2 + \dots + m = \frac{m(m+1)}{2}$, при $m = \frac{p-1}{2}$.

и, учитывая лемму Гаусса, мы завершаем доказательство пятого утверждения леммы

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

Перейдем к доказательству последнего, шестого утверждения леммы – квадратичного закона взаимности Гаусса. Пусть a нечетное простое число, отличное от p . Тогда равенство (4.10) может быть записано в виде сравнения

$$0 \equiv \sum_{k=1}^{\frac{p-1}{2}} q_k + \mu \pmod{2} \quad \text{или} \quad \sum_{k=1}^{\frac{p-1}{2}} q_k \equiv \mu \pmod{2}.$$

В силу определения, выполнено равенство $q_k = \left\lfloor \frac{ka}{p} \right\rfloor$ и $\mu \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor$, откуда, по лемме Гаусса, получаем

$$\left(\frac{a}{p}\right) = (-1)^\mu = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor}.$$

Аналогичными рассуждениями получаем равенство $\left(\frac{p}{a}\right) = (-1)^{\sum_{s=1}^{\frac{a-1}{2}} \left\lfloor \frac{sp}{a} \right\rfloor}$, следовательно,

$$\left(\frac{a}{p}\right) \left(\frac{p}{a}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{s=1}^{\frac{a-1}{2}} \left\lfloor \frac{sp}{a} \right\rfloor}.$$

Нам осталось вычислить сумму, образующую степень, в которую возводится -1 , и показать, что выполнено равенство

$$S_1 + S_2 = \frac{(p-1)(a-1)}{4}, \quad \text{где} \quad S_1 = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor, \quad S_2 = \sum_{s=1}^{\frac{a-1}{2}} \left\lfloor \frac{sp}{a} \right\rfloor.$$

Воспользуемся геометрическими рассуждениями и покажем, что искаемая сумма равна количеству точек с целыми координатами, расположенными внутри некоторого прямоугольника.

Рассмотрим сумму S_1 . При фиксированном индексе k из интервала $1 \leq k \leq \frac{p-1}{2}$ величина $\left\lfloor \frac{ka}{p} \right\rfloor$ есть количество целых чисел y , удовлетворяющих неравенству $0 \leq y < \frac{ka}{p}$. Заметим, что мы можем не учитывать нулевые значения величины y , поскольку они не изменяют величину S_1 .

Подставляя первое неравенство во второе и замечая, что интервал $(\frac{p-1}{2}, \frac{p}{2})$ не содержит целых точек, мы получаем, что S_1 есть число всех точек (k, y) , с целыми координатами, удовлетворяющими неравенствам

$$0 < k < \frac{p}{2}, \quad 0 < y < \frac{a}{2}, \quad py - ak < 0.$$

Аналогичным способом получаем, что S_2 есть количество точек (k, y) , с целыми координатами, удовлетворяющими неравенствам

$$0 < k < \frac{p}{2}, \quad 0 < y < \frac{a}{2}, \quad py - ak > 0.$$

Поскольку в указанных границах не найдется ни одной пары целых чисел таких, что $py = ak$, то мы получаем, что сумма $S_1 + S_2$ есть количество точек с целыми координатами, расположенными внутри прямоугольника со сторонами $\frac{p}{2}$ и $\frac{a}{2}$. Поскольку числа p и a нечетны, то $S_1 + S_2 = \frac{p-1}{2} \cdot \frac{a-1}{2}$. Лемма доказана. \square

21. Схема асимметричного шифрования Рабина-Вильямса и ее связь с квадратичными вычетами.

Схема шифрования RSA является самой известной, но не единственной схемой, криптографическая стойкость которой основывается на задаче факторизации целых чисел. В 1979 году Микаэль Рабин (Michael Rabin) предложил следующую схему шифрования [?].

Пусть $m = pq > 0$ нечетное составное число, являющееся произведением двух простых чисел p и q . Данное число является открытым ключом абонента, который хочет получать сообщения. Секретным ключом являются значения простых чисел p и q .

Процесс зашифрования сообщения выглядит следующим образом. Пусть сообщение s удовлетворяет неравенствам $1 < s < m - 1$ и выполнено условие $\text{НОД}(s, m) = 1$. Тогда для зашифрования сообщения s необходимо вычислить

$$c \equiv s^2 \pmod{m}.$$

Процесс расшифрования сообщения, то есть определения числа s по заданным значениям c и m , выглядит следующим образом. Получатель сообщения, абонент которому известно разложение числа m на множители, вычисляет значения x_p, x_q такие, что

$$x_p^2 \equiv c \pmod{p}, \quad x_q^2 \equiv c \pmod{q}.$$

В предыдущих лекциях мы подробно рассмотрели алгоритм Тонелли-Шенкса вычисления квадратного корня по модулю простого числа, алгоритм 4.2. Для упрощения вычислений при генерации числа m рекомендуется выбирать $p \equiv q \equiv 3 \pmod{4}$. В этом случае задача вычисления квадратного корня, как мы показали ранее, сводится к модульному возведению в степень, то есть

$$x_p \equiv c^{\frac{p+1}{4}} \pmod{p}, \quad x_q \equiv c^{\frac{q+1}{4}} \pmod{q}.$$

Найденные значения x_p, x_q используются для вычисления множества, состоящего из четырех значений s_1, s_2, s_3, s_4 таких, что $s_i^2 \equiv c \pmod{m}$. Это можно сделать, например, с помощью китайской теоремы об остатках, теорема 2.3.

Другой подход заключается в следующем. Используя расширенный алгоритм Эвклида, алгоритм 2.1, вычислим u, v такие, что

$$up + vq = 1,$$

и определим

$$\begin{aligned}s_1 &\equiv upx_q + vqx_p \pmod{m}, \\ s_2 &= m - s_1, \\ s_3 &\equiv upx_q - vqx_p \pmod{m}, \\ s_4 &= m - s_3.\end{aligned}$$

Заметим, что вычисление значений u и v можно произвести заранее, например, сразу после генерации простых чисел p и q .

Подобный подход избавляет нас от необходимости решать четыре различных системы сравнений. Получателю остается сделать выбор какое же из четырех полученных им значений было ему отправлено.

22. Алгоритм нахождения корней многочленов по простому модулю

Найденные значения x_p, x_q используются для вычисления множества, состоящего из четырех значений s_1, s_2, s_3, s_4 таких, что $s_i^2 \equiv c \pmod{m}$. Это можно сделать, например, с помощью китайской теоремы об остатках, теорема 2.3.

Другой подход заключается в следующем. Используя расширенный алгоритм Эвклида, алгоритм 2.1, вычислим u, v такие, что

$$up + vq = 1,$$

Схема шифрования RSA является самой известной, но не единственной схемой, криптографическая стойкость которой основывается на задаче факторизации целых чисел. В 1979 году Микаэль Рабин (Michael Rabin) предложил следующую схему шифрования [?].

Пусть $m = pq > 0$ нечетное составное число, являющееся произведением двух простых чисел p и q . Данное число является открытым ключом абонента, который хочет получать сообщения. Секретным ключом являются значения простых чисел p и q .

Процесс зашифрования сообщения выглядит следующим образом. Пусть сообщение s удовлетворяет неравенствам $1 < s < m - 1$ и выполнено условие $\text{НОД}(s, m) = 1$. Тогда для зашифрования сообщения s необходимо вычислить

$$c \equiv s^2 \pmod{m}.$$

Процесс расшифрования сообщения, то есть определения числа s по заданным значениям c и m , выглядит следующим образом. Получатель сообщения, абонент которому известно разложение числа m на множители, вычисляет значения x_p, x_q такие, что

$$x_p^2 \equiv c \pmod{p}, \quad x_q^2 \equiv c \pmod{q}.$$

В предыдущих лекциях мы подробно рассмотрели алгоритм Тонелли-Шенкса вычисления квадратного корня по модулю простого числа, алгоритм 4.2. Для упрощения вычислений при генерации числа m рекомендуется выбирать $p \equiv q \equiv 3 \pmod{4}$. В этом случае задача вычисления квадратного корня, как мы показали ранее, сводится к модульному возведению в степень, то есть

$$x_p \equiv c^{\frac{p+1}{4}} \pmod{p}, \quad x_q \equiv c^{\frac{q+1}{4}} \pmod{q}.$$

и определим

$$\begin{aligned}s_1 &\equiv upx_q + vqx_p \pmod{m}, \\ s_2 &= m - s_1, \\ s_3 &\equiv upx_q - vqx_p \pmod{m}, \\ s_4 &= m - s_3.\end{aligned}$$

Заметим, что вычисление значений u и v можно произвести заранее, например, сразу после генерации простых чисел p и q .

Подобный подход избавляет нас от необходимости решать четыре различных системы сравнений. Получателю остается сделать выбор какое же из четырех полученных им значений было ему отправлено.

Алгоритм 4.3 (Вычисление случайного корня многочлена)

Вход: Нечетное простое число p и многочлен $h(x) \equiv \prod_{k=1}^r (x - e_k) \pmod{p}$, раскладывающийся на линейные множители в $\mathbb{F}_p[x]$ с неизвестными значениями e_1, \dots, e_r .

Выход: Корень многочлена – одно из значений e_1, \dots, e_r .

1. Выбрать случайное значение $c \in \mathbb{F}_p$. Если $h(c) \equiv 0 \pmod{p}$, то закончить алгоритм и вернуть значение c в качестве корня многочлена $h(x)$.
2. Вычислить многочлен $d(x) \in \mathbb{F}_p[x]$

$$d(x) = \text{НОД} \left(h(x), (x - c)^{\frac{p-1}{2}} - 1 \right).$$

3. Если $\deg d(x) < 1$ или $\deg d(x) = \deg h(x)$, то вернуться на шаг 1).
 4. Если $\deg d(x) = 1$, то закончить алгоритм и вернуть в качестве корня значение свободного члена многочлена $d(x)$.
 5. Определить $f(x) = d(x)$ и вернуться на шаг 1). □
-

Алгоритм 4.4 (Вычисление всех корней многочлена)

Вход: Простое нечетное число p и многочлен $f(x) = \sum_{k=0}^n a_k x^k$ такой, что $a_n \not\equiv 0 \pmod{p}$.

Выход: Значения $e_1, \dots, e_r, \alpha_1, \dots, \alpha_r$ и многочлен $u(x) \in \mathbb{F}_p[x]$ такие, что выполнено сравнение $f(x) \equiv a_n(x - e_1)^{\alpha_1} \cdots (x - e_r)^{\alpha_r} u(x) \pmod{p}$.

1. Если $a_n \not\equiv 1 \pmod{p}$, то сделать многочлен $f(x)$ унитарным, то есть определить $f(x) \equiv a_n^{-1} f(x) \pmod{p}$.
 2. Определить многочлены $u(x) = f(x)$ и $h(x) = \text{НОД}(x^p - x, f(x))$.
 3. Если $\deg h(x) = 0$, то закончить алгоритм.
 4. Используя алгоритм 4.3 вычислить $e \in \mathbb{F}_p$ такой, что $h(e) \equiv 0 \pmod{p}$ и определить $\alpha = 0$.
 5. Пока $f(x) \equiv 0 \pmod{x - e}$ выполнить
 - 5.1. Определить $f(x) = \frac{f(x)}{(x - e)}$ и вычислить $\alpha = \alpha + 1$.
 6. Вычислить $u(x) = \frac{u(x)}{(x - e)^\alpha}$ и $h(x) = \frac{h(x)}{(x - e)}$.
 7. Добавить пару e, α в список корней и их кратностей и перейти на шаг 3. □
-

23. Двоичный алгоритм возведения в степень и области его применения

24. Понятия показателя и первообразного корня. Их свойства.

Рассмотрим вопросы, связанные с понятием первообразного корня целого числа.

Определение 2.7. Пусть a и $m > 0$ целые взаимно простые числа. Мы будем называть показателем числа a по модулю m минимальное из целых чисел q таких, что $a^q \equiv 1 \pmod{m}$, и использовать обозначение

$$\text{ord}_m a = \min \{q \in \mathbb{Z}, q > 0 : a^q \equiv 1 \pmod{m}\}.$$

Из теоремы Эйлера (теорема 2.6) следует, что показатель числа a существует всегда, например, им может являться значение функции Эйлера.

Лемма 2.4. Пусть $a, m > 0$ целые числа такие, что $\text{НОД}(a, m) = 1$, и показатель числа a по модулю m равен q . Тогда выполнены следующие условия

1. Числа $1, a, a^2, \dots, a^{q-1}$ не сравнимы друг с другом по модулю m .
2. Если выполнено сравнение $a^k \equiv a^l \pmod{m}$, то $k \equiv l \pmod{q}$.
3. Пусть s натуральное число такое, что $a^s \equiv 1 \pmod{m}$, тогда $q|s$. В частности, показатель q делит значение $\varphi(m)$ функции Эйлера.

Доказательство. Докажем первое утверждение леммы. Пусть найдутся такие показатели k и l , $0 \leq k < l < q$, что $a^k \equiv a^l \pmod{m}$. Тогда из сравнения $a^{l-k} \equiv 1 \pmod{m}$ и неравенства $l - k < q$ получаем, что q не является показателем числа a и противоречие условию леммы.

Для доказательства второго утверждения леммы, используя деление с остатком (см. лемму 1.1), получим представления $k = k_1q + r_1$, где $0 \leq r_1 < q$ и $l = l_1q + r_2$, где $0 \leq r_2 < q$.

Из сравнения $a^k \equiv a^l \pmod{m}$ следует, что

$$a^{r_1} \equiv (a_1^k)^q a^{r_1} \equiv (a_1^l)^q a^{r_2} \equiv a^{r_2} \pmod{m}.$$

Поскольку $r_1 < q$, $r_2 < q$, то из первого утверждения леммы следует равенство $r_1 = r_2$ и доказательство второго утверждения.

Третье утверждение леммы является частным случаем второго. Действительно из сравнения

$$a^s \equiv 1 \equiv a^0 \pmod{m},$$

получаем, что $s \equiv 0 \pmod{q}$ и $s = cq$, при некотором значении числа c , то есть $q|s$. \square

Из утверждения леммы следует, что для каждого целого числа a его показатель по модулю числа t является делителем значения функции Эйлера $\varphi(m)$. Таким образом, множество всех возможных делителей числа $\varphi(m)$ образует множество всех возможных значений показателей. Следующее определение задает класс чисел, имеющих максимально возможное значение показателя.

Определение 2.8. Пусть $a, t > 0$ целые взаимно простые числа. Число a называется первообразным корнем по модулю t , если показатель a по модулю t равен $\varphi(t)$, то есть $\text{ord}_t a = \varphi(t)$.

Сделаем следующее замечание. В отечественной учебной литературе по криптографии термины «показатель числа» и «первообразный корень» не прижились. Обычно они заменяются их алгебраическими синонимами: «порядок элемента» и «примитивный элемент», вводимыми в случае, когда модуль t является простым числом.

Определение 2.9. Пусть p нечетное простое число и a целое число такое, что $\text{НОД}(a, p) = 1$. Тогда порядком числа a по модулю p называется показатель числа a по модулю p , то есть минимальное из чисел q таких, что $a^q \equiv 1 \pmod{p}$

$$\text{ord}_p a = \min_{q>0} \{a^q \equiv 1 \pmod{p}\}.$$

Соответственно, a называется примитивным элементом по модулю p , если показатель числа a равняется $p - 1$, то есть a является первообразным корнем по модулю простого числа p .

Вопрос о существовании первообразных корней зависит от того, какой модуль t мы рассматриваем. Далее мы покажем, что первообразные корни существуют по модулю $t = p^\alpha$ для некоторого нечетного простого числа p и $\alpha \geq 1$.

25. Теорема о существовании первообразного корня по простому модулю

Вначале мы сформулируем следующий результат.

Теорема 2.8. *Пусть p нечетное простое число, тогда найдется целое число a , являющееся первообразным корнем по модулю p .*

Перед доказательством теоремы мы исследуем ряд свойств первообразных корней по модулю простого числа p .

Лемма 2.5. *Пусть a, b целые числа, p простое число.*

1. *Если показатель числа a по модулю p равен xy , $\text{ord}_p a = xy$, то выполнено $\text{ord}_p a^x = y$.*
2. *Если $\text{ord}_p a = x$, $\text{ord}_p b = y$ и $\text{НОД}(x, y) = 1$, то $\text{ord}_p(ab) = xy$.*

Доказательство. Докажем первое утверждение леммы. Предположим, что показатель числа a^x равен t , тогда $(a^x)^t \equiv a^{xt} \equiv 1 \pmod{p}$. Тогда, согласно второму утверждению леммы 2.4, выполнено $xt \equiv xy \pmod{p}$ или $xt = yx + c$ при некотором целом c . Сокращая на x , получим, что $y|t$.

С другой стороны, из сравнения $1 \equiv a^{xy} \equiv (a^x)^y \pmod{p}$ следует, что $y \equiv t \pmod{t}$, следовательно, $t|y$. Таким образом, $y = t$ и первое утверждение леммы доказано.

Пусть показатель элемента ab равен t , тогда

$$1 \equiv ((ab)^t)^x \equiv a^{tx}b^{tx} \equiv b^{tx} \pmod{p}.$$

Используя второе утверждение леммы 2.4, получим, что $tx \equiv y \pmod{p}$ или $tx = yx + c$ при некотором целом c . Поскольку $\text{НОД}(x, y) = 1$, то из леммы 1.4 получаем, что $y|t$. Аналогично, заменяя в предыдущей цепочке сравнений x на y , получаем, что $x|t$ и $xy|t$.

С другой стороны, из второго утверждения леммы 2.4 и сравнения

$$(ab)^{xy} \equiv 1 \pmod{p}$$

получаем, что $ab \equiv t \pmod{p}$ и $t|xy$, следовательно, $xy = t$. □

Введем понятие наименьшего общего кратного и докажем несколько свойств, которым оно удовлетворяет.

Определение 2.10. Пусть a, b натуральные, отличные от нуля числа. Наименьшим общим кратным мы будем называть наименьшее натуральное число t такое, что $a|t$, $b|t$. Для обозначения наименьшего общего кратного мы будем использовать символ

$$\text{НОК}(a, b) = \min\{m \in \mathbb{N} : a|m, b|m\}.$$

Данное определение может быть обобщено на несколько целых чисел

$$\text{НОК}(a_1, \dots, a_k) = \min\{m \in \mathbb{N} : a_1|m, \dots, a_k|m\}.$$

Лемма 2.6. Верны следующие утверждения:

1. Любое общее кратное нескольких чисел a_1, \dots, a_k делится на их наименьшее общее кратное.
2. Наименьшее общее кратное взаимно простых чисел a_1, \dots, a_k равно их произведению, то есть $\text{НОК}(a_1, \dots, a_k) = \prod_{i=1}^k a_i$.
3. Если число b делится на каждое из попарно взаимно простых чисел a_1, \dots, a_k , то оно делится и на их произведение.

Доказательство. Начнем доказательство с первого утверждения леммы. Обозначим символом $t = \text{НОК}(a_1, \dots, a_k)$, а символом s – какое-нибудь произвольное общее кратное чисел a_1, \dots, a_k . Поскольку t наименьшее общее кратное, мы можем записать равенство

$$s = mq + r, \quad 0 \leq r < m,$$

где q, r некоторые натуральные числа. В силу определения общего делителя, находим, что $r = s - mq$ делится на каждое из чисел a_1, \dots, a_k и, следовательно, является их общим делителем. Но поскольку мы предположили, что $r < m$ и m – наименьший общий делитель, то данное свойство возможно только при $r = 0$. Первое утверждение доказано.

Согласно основной теореме арифметики, см. теорему 1.4, разложим a_1 в произведение простых чисел $a_1 = \prod_{i=1}^{k_1} p_i^{\alpha_i}$. Каждое $p_i^{\alpha_i}$ из этого произведения делит **НОК** (a_1, \dots, a_k), в силу определения наименьшего общего кратного, но не делит остальные a_i при $i > 1$, в силу их взаимной простоты. Аналогичное свойство выполняется для всех a_i , $i = 2, \dots, k$.

Таким образом, $\prod_i^k a_i$ делит **НОК** (a_1, \dots, a_k). Поскольку $\prod_i^k a_i$ также является общим кратным чисел a_1, \dots, a_k , то второе утверждение леммы выполнено.

Третье утверждение леммы тривиально следует из двух первых. Действительно, из первого утверждения леммы следует, что b делится на **НОК** (a_1, \dots, a_k), а в силу второго утверждения следует утверждение, поскольку **НОК** (a_1, \dots, a_k) = $\prod_i^k a_i$. \square

Доказательство теоремы 2.8. Для доказательства теоремы нам достаточно предъявить число a , показатель которого по модулю p равняется $p - 1$.

Пусть $\{t_1, \dots, t_k\}$ множество различных показателей, которым принадлежат числа $1, 2, \dots, p - 1$. Определим $\tau = \text{НОК}(t_1, \dots, t_k)$ и разложим его в произведение простых делителей

$$\tau = q_1^{\alpha_1} \cdots q_r^{\alpha_r}.$$

В силу определения наименьшего общего кратного для множителя $q_1^{\alpha_1}$ найдется некоторый показатель t_i , $1 \leq i \leq k$, такой, что $q_1^{\alpha_1} | t_i$ или, что равносильно, $t_i = c_1 q_1^{\alpha_1}$ для некоторого целого c_1 . Пусть a_1 целое число, показатель которого равен t_i . Тогда из первого утверждения леммы 2.5 получаем, что показатель числа $b_1 \equiv a_1^{c_1} \pmod{p}$ равен $q_1^{\alpha_1}$.

Выполняя аналогичные рассуждения далее, мы найдем для каждого простого делителя q_i числа τ число b_i такое, что $\text{ord}_p b_i = q_i^{\alpha_i}$ для всех $i = 1, \dots, r$.

Тогда, согласно второму утверждению леммы 2.5, показатель элемента $b \equiv b_1 \cdots b_r \pmod{p}$ равен τ . Из третьего утверждения леммы 2.4, получаем $\tau | \varphi(p) = p - 1$.

С другой стороны, в силу построения τ , для любого индекса i выполнено $t_i | \tau$, следовательно, для каждого целого b из интервала $1, \dots, p - 1$ найдется индекс i такой, что $\text{ord } b = t_i$ и $b^\tau \equiv 1 \pmod{p}$. Отсюда мы выводим, что $p - 1 | \tau$ и завершаем доказательство теоремы. \square

26. Схема Диффи-Хеллмана выработка общего ключа и ее связь с первообразными корнями

Описание алгоритма [\[2\]](#) [править | править код]

Предположим, существует два абонента: Алиса и Боб. Обоим абонентам известны некоторые два числа g и p , которые не являются секретными и могут быть известны также другим заинтересованным лицам. Для того, чтобы создать неизвестный более никому секретный ключ, оба абонента генерируют большие случайные числа: Алиса — число a , Боб — число b . Затем Алиса вычисляет остаток от деления^[3] (1):

$$A = g^a \bmod p \quad (1)$$

и пересыпает его Бобу, а Боб вычисляет остаток от деления (2):

$$B = g^b \bmod p \quad (2)$$

и передаёт Алисе. Предполагается, что злоумышленник может получить оба этих значения, но не модифицировать их (то есть, у него нет возможности вмешаться в процесс передачи).

На втором этапе Алиса на основе имеющегося у неё a и полученного по сети B вычисляет значение (3):

$$B^a \bmod p = g^{ab} \bmod p \quad (3)$$

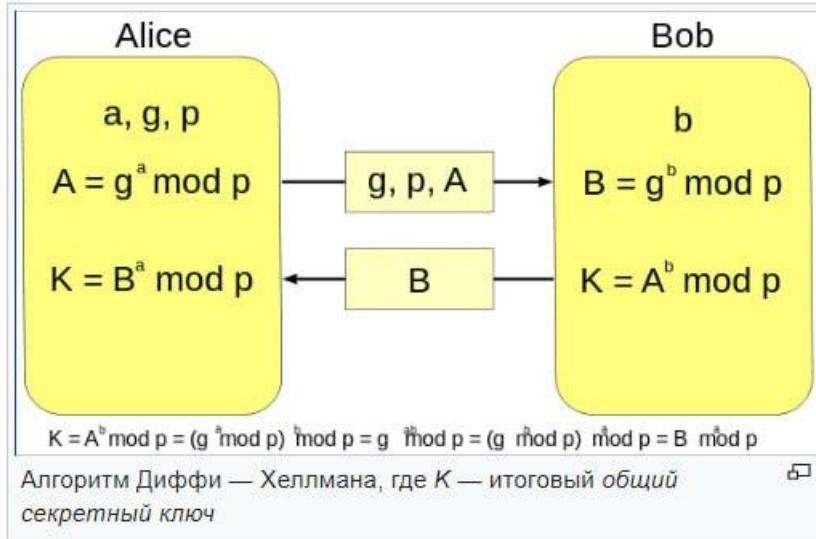
Боб на основе имеющегося у него b и полученного по сети A вычисляет значение (4):

$$A^b \bmod p = g^{ab} \bmod p \quad (4)$$

Как нетрудно видеть, у Алисы и Боба получилось одно и то же число (5):

$$K = g^{ab} \bmod p \quad (5)$$

Его они и могут использовать в качестве секретного ключа, поскольку здесь злоумышленник встретится с практически неразрешимой (за разумное время) проблемой вычисления (3) или (4) по перехваченным $g^a \bmod p$ и $g^b \bmod p$, если числа p, a, b выбраны достаточно большими. Работа алгоритма показана на рисунке^[4].



При работе алгоритма каждая сторона:

1. генерирует случайное **натуральное число a — закрытый ключ**
2. совместно с удалённой стороной устанавливает **открытые параметры p и g** (обычно значения p и g генерируются на одной стороне и передаются другой), где
 - p является **случайным простым числом**
 - $(p-1)/2$ также должно быть **случайным простым числом** (для повышения безопасности)^[5]
 - g является **первообразным корнем по модулю p** (*также является простым числом*)
3. вычисляет **открытый ключ A** , используя преобразование над **закрытым ключом**
4. обменивается **открытыми ключами** с удалённой стороной
5. вычисляет **общий секретный ключ K** , используя открытый ключ удаленной стороны B и свой закрытый ключ a

$$K = B^a \bmod p$$

K получается равным с обеих сторон, потому что:

$$B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p = (g^a \bmod p)^b \bmod p = A^b \bmod p$$

В практических реализациях для a и b используются числа порядка 10^{100} и p порядка 10^{300} . Число g не обязано быть большим и обычно имеет значение в пределах первого десятка.

27. Понятие систематической дроби. Периодичность систематической дроби

Начнем с того, что определим основной объект исследования этой главы – бесконечную систематическую дробь.

Определение 6.1. Пусть $b > 1$ натуральное число, которое мы будем называть основанием системы счисления. Пусть $\sigma \in \{-1, 1\}$ и t некоторое целое число. Мы будем называть систематической дробью α ряд

$$\alpha = \sigma \sum_{n=-m}^{\infty} a_n b^{-n} = \sigma \left(a_{-k} b^{-k} + \cdots + a_1 b + a_0 + \frac{a_1}{b} + \frac{a_2}{b^2} + \cdots \right), \quad (6.1)$$

где $a_n \in \mathbb{N}_0$ и $0 \leq a_n < b$ для $n = -m, -m+1, \dots$

Величину

$$a = \sigma \sum_{k=-m}^0 a_k b^{-k} = \sigma (a_{-k} b^{-k} + \cdots + a_1 b + a_0)$$

мы будем называть целой частью систематической дроби. Для любого $k \in \mathbb{N}_0$ мы будем называть величину

$$s_k(\alpha) = \sigma \sum_{n=-m}^k a_n b^{-n} \in \mathbb{Q}, \quad (6.2)$$

конечной суммой систематической дроби (6.1).

Мы будем говорить, что систематическая дробь конечна, если найдется индекс $n_0 \in \mathbb{N}$ такой, что для всех индексов $n \geq n_0$ выполнено равенство $a_n = 0$. Это же условие равносильно тому, что

$$s_n(\alpha) = s_{n_0}(\alpha), \quad n \geq n_0.$$

Мы будем говорить, что систематическая дробь периодична, если найдется индекс $\lambda \in \mathbb{N}$ и натуральное число $\tau \geq 1$ такие, что всех индексов $n \geq \lambda$ выполнено равенство

$$a_{n+\tau} = a_n, \quad n = \lambda, \lambda + 1, \dots$$

Величину τ мы будем называть периодом систематической дроби, а величину λ – длиной подхода к периоду.

Для записи систематических дробей и их конечных сумм также можно использовать обозначения, более привычные, чем суммы (6.1) или (6.2),

$$\begin{aligned}\alpha &= \pm a_{-m} a_{-m+1} \dots a_0, a_1 a_2 \dots, \\ s_k(\alpha) &= \pm a_{-m} a_{-m+1} \dots a_0, a_1 a_2 \dots a_{k_b}.\end{aligned}$$

Для периодических систематических дробей может использоваться обозначение

$$\alpha = \pm a_{-m} a_{-m+1} \dots a_0, a_1 a_2 \dots (a_\lambda \dots a_{\lambda+\tau-1})_b,$$

в котором элементы $a_\lambda, \dots, a_{\lambda+\tau-1}$ образуют период последовательности коэффициентов систематической дроби. В случаях, когда это ясно из контекста изложения, символ b может быть опущен.

Определение 6.2. Мы будем говорить, что систематическая дробь сходится к числу α , если сходится последовательность его конечных сумм $(s_k)_{k=0}^{\infty}$, то есть $\alpha = \lim_{k \rightarrow \infty} s_k$.

Любая систематическая дробь сходится к некоторой величине. Для доказательства этого утверждения нам потребуется следующая лемма.

Теорема 6.2. Сходящаяся к числу α систематическая дробь конечна или периодична тогда и только тогда, когда α рациональное число.

Доказательство. Покажем, что всякая конечная или периодическая систематическая дробь определяет рациональное число. Рассмотрим систематическую дробь

$$\alpha = \sigma \sum_{n=0}^{\infty} a_n b^{-n}.$$

Если данная дробь конечна, тогда найдется индекс $k \in \mathbb{N}_0$ такой, что $a_n = 0$ при $n > k$ и

$$\alpha = \sigma \sum_{n=0}^k a_n b^{-n} = \frac{\sigma}{b^k} (a_0 b^k + a_1 b^{k-1} + \cdots + a_k) \in \mathbb{Q},$$

т.е. α рациональное число.

Пусть теперь систематическая дробь периодична, тогда найдется натуральное число $\tau \geq 1$ и индекс $\lambda \in \mathbb{N}_0$ такой, что $a_{n+\tau} = a_n$ при $n \geq \lambda$. Обозначим

$$\begin{aligned} a_\lambda b^{-\lambda} + a_{\lambda+1} b^{-\lambda-1} + \cdots + a_{\lambda+\tau-1} b^{-\lambda-\tau+1} &= \\ &= b^{-\lambda} (a_\lambda + a_{\lambda+1} b^{-1} + \cdots + a_{\lambda+\tau-1} b^{-\tau+1}) = \\ &= b^{-\lambda} \cdot b^{-\tau+1} (a_\lambda b^{\tau-1} + a_{\lambda+1} b^{\tau-2} + \cdots + a_{\lambda+\tau-1}) = b^{-\lambda} \frac{A}{b^\tau}, \end{aligned}$$

где $A \in \mathbb{Z}$ и $0 \leq A < b^\tau$. Тогда, учитывая (6.2), (6.3), получим равенство

$$\begin{aligned} \alpha \sigma^{-1} &= \sum_{n=0}^{\infty} a_n b^{-n} = \\ &= \sum_{n=0}^{\lambda-1} a_n b^{-n} + \sum_{n=\lambda}^{\lambda+\tau-1} a_n b^{-n} + \sum_{n=\lambda+\tau}^{\lambda+2\tau-1} a_n b^{-n} + \sum_{n=\lambda+2\tau}^{\lambda+3\tau-1} a_n b^{-n} + \cdots = \\ &= s_{\lambda-1} + b^{-\lambda} \left(\frac{A}{b^\tau} + \frac{A}{b^{2\tau}} + \frac{A}{b^{3\tau}} + \cdots \right) = s_{\lambda-1} + \frac{A}{b^\lambda} \sum_{n=1}^{\infty} (b^\tau)^{-n} = \\ &= s_{\lambda-1} + \frac{A}{b^\lambda} \cdot \frac{1}{b^\tau - 1} \in \mathbb{Q}, \end{aligned}$$

из которого следует, что α является рациональным числом.

Теперь докажем теорему в обратную сторону и рассмотрим произвольное рациональное число $\frac{r}{q}$, где $q > 0$ и **НОД**(r, q) = 1. Используя операцию деления с остатком запишем $|r| = a_0 q + p$, тогда

$$\frac{r}{q} = \sigma \left(a_0 + \frac{p}{q} \right), \quad \text{где } 0 \leq p < q, \quad \sigma = \frac{r}{|r|}, \quad (6.5)$$

и нам достаточно в явном виде предъявить систематическую дробь для $\frac{p}{q}$.

Определим **НОД**(q, b) = d и для $d > 1$ обозначим $\nu_d(b) \in \mathbb{N}_0$ максимальную степень, в которой число d входит в разложение числа b , иначе положим $\nu_1(b) = 0$. Аналогично определим величину $\nu_d(q)$. Тогда

$$q = d^{\nu_d(q)} q_1, \quad b = d^{\nu_d(b)} b_1, \quad \text{НОД}(b, b_1) = \text{НОД}(q, q_1) = \text{НОД}(b_1, q_1) = 1.$$

Определим

$$\nu_d(q) = s\nu_d(b) + t, \quad 0 \leq t < \nu_d(b)$$

и запишем равенства

$$q = d^{\nu_d(q)} q_1 = d^t \cdot \left(d^{\nu_d(b)} \right)^s q_1 = d^t \left(\frac{b}{b_1} \right)^s q_1$$

и

$$\frac{p}{q} = \frac{d^t p b_1^s}{b^s q_1} = \frac{1}{b^s} \cdot \left(c_0 + \frac{p_1}{q_1} \right), \quad (6.6)$$

где $d^t p b_1^s = c_0 q_1 + p_1$ и $0 \leq p_1 < q_1$. Если $p_1 = 0$, то мы получаем точное равенство

$$\frac{p}{q} = \frac{c_0}{b^s},$$

в противном случае $p_1 > 0$ и **НОД**(p_1, q_1) = 1.

Из равенства (6.6) следует, что любая рациональная дробь может быть представлена в виде произведения величины, обратно пропорциональной некоторой степени b и дроби, знаменатель которой взаимно прост с основанием системы счисления b .

Поскольку $p < q$, то $c_0 < b^s$, следовательно, воспользуемся леммой 5.1 и запишем

$$c_0 = a_s + a_{s-1}b + \cdots + a_1b^{s-1}, \quad (6.7)$$

тогда из (6.6) следует равенство

$$\frac{p}{q} = a_1 b^{-1} + a_2 b^{-2} + \cdots + a_s b^{-s} + \frac{1}{b^s} \cdot \frac{p_1}{q_1}.$$

Если $p_1 = 0$, то мы получили конечную систематическую дробь для $\frac{p}{q}$ и утверждение теоремы. Теперь нам осталось построить систематическую дробь для рационального числа $\frac{p_1}{q_1}$ при $0 < p_1 < q_1$. Для этого рассмотрим последовательность целых чисел

$$b, b^2, \dots, b^\tau, b^{\tau+1}, \dots$$

и выберем из них то, у которого остаток от деления на q_1 будет равен 1, т.е.

$$b^\tau = cq_1 + 1 \quad (6.8)$$

при некотором натуральном c и минимально возможном значении $\tau > 1$. Поскольку $b^\tau > cq_1 > cp_1$, мы можем снова воспользоваться леммой 5.1 и записать

$$cp_1 = a_{\tau+s} + a_{\tau+s-1}b + \cdots + a_{s+1}b^{\tau-1}, \quad (6.9)$$

тогда

$$\begin{aligned} \frac{p_1}{q_1} &= \frac{cp_1}{cq_1} = cp_1 \cdot \frac{1}{b^\tau - 1} = cp_1 \sum_{n=1}^{\infty} (b^\tau)^{-n} = \\ &= (a_{\tau+s} + a_{\tau+s-1}b + \cdots + a_{s+1}b^{\tau-1}) \sum_{n=1}^{\infty} (b^\tau)^{-n} = \\ &= a_{s+1}b^{-1} + \cdots + a_{s+\tau}b^{-\tau} + a_{s+1}b^{-\tau-1} + \cdots + a_{s+\tau}b^{-2\tau} + \cdots, \end{aligned}$$

т.е. дробь $\frac{p_1}{q_1}$ является пределом систематической дроби с периодом $a_{s+1}, \dots, a_{s+\tau}$. Теперь, учитывая (6.5) и (6.6), запишем окончательное равенство

$$\begin{aligned} \frac{r}{q} &= \sigma \left(a_0 + \frac{p}{q} \right) = \sigma \left(a_0 + \sum_{n=1}^s a_n b^{-n} + \frac{1}{b^s} \cdot \frac{p_1}{q_1} \right) = \\ &= \sigma \left(a_0 + \sum_{n=1}^s a_n b^{-n} + \sum_{n=s+1}^{\infty} a_n b^{-n} \right) = \sigma \sum_{n=0}^{\infty} a_n b^{-n}, \end{aligned}$$

в котором коэффициент a_0 определен равенством (6.5), коэффициенты a_1, \dots, a_s равенством (6.7), а образующие период коэффициенты $a_{s+1}, \dots, a_{s+\tau}$ определены равенством (6.9). \square

28. Понятие цепной дроби. Подходящие дроби и их свойства.

Рассмотрим непрерывные дроби действительных чисел.

Определение 7.1. Пусть α действительное число. Мы будем называть целой частью α , которую мы обозначаем символом $\lfloor \alpha \rfloor$, наибольшее целое число, меньшее, либо равное α . В частном случае: целая часть целого числа совпадает с ним.

Отметим, что α может быть как отрицательным, так и положительным числом. Например $\lfloor \sqrt{13} \rfloor = 3$, в то время как $\lfloor -\sqrt{13} \rfloor = -4$. В любом случае выполнено неравенство $\lfloor \alpha \rfloor \leq \alpha$.

Пусть α_0 действительное число и $\alpha_0 \neq 0$. Определим последовательность действительных чисел $\alpha_1, \alpha_2, \dots$ следующим рекуррентным соотношением

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n}, \quad \text{где } a_n = \lfloor \alpha_n \rfloor. \quad (7.1)$$

В случае, если α_n является целым числом, то есть выполнено равенство $a_n = \alpha_n$, мы будем считать, что последовательность (7.1) обрывается.

Записав равенство (7.1) в виде $\alpha_n = a_n + \frac{1}{\alpha_{n+1}}$, мы можем выразить число α_0 в виде

$$\alpha_0 = a_0 + \frac{1}{\alpha_1} = a_0 + \frac{1}{a_1 + \frac{1}{\alpha_2}} = \dots$$

или, в общем виде,

$$\alpha_0 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots + \cfrac{1}{\alpha_n}}}}, \quad (7.2)$$

для произвольного индекса n .

Для упрощенной записи равенства (7.2) мы будем использовать обозначение $\alpha_0 = [a_0, a_1, \dots, a_{n-1}, \alpha_n]$.

Определение 7.2. Пусть $\alpha_0 \neq 0$ действительное число. Мы будем называть представление (7.2)

$$\alpha_0 = [a_0, a_1, \dots, a_{n-1}, \alpha_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots + \cfrac{1}{\alpha_n}}}},$$

$n = 1, 2, \dots$ непрерывной или цепной дробью числа α_0 . Элементы последовательности a_0, a_1, \dots мы будем называть неполными частными, а элементы последовательности $\alpha_1, \alpha_2, \dots$ полными частными.

Для каждого индекса n мы можем рассмотреть рациональную дробь $\frac{P_n}{Q_n}$, определяемую равенством

$$\frac{P_n}{Q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots + \cfrac{1}{a_n}}}} = [a_0, a_1, \dots, a_{n-1}, a_n]. \quad (7.5)$$

Определение 7.3. Пусть $\alpha_0 \neq 0$ действительное число. Дробь $\frac{P_n}{Q_n}$, определяемая равенством (7.5), называется подходящей дробью к числу α_0 .

Нам потребуются следующие леммы, описывающие свойства числиелей и знаменателей подходящих дробей.

Лемма 7.2. Пусть $\alpha_0 \neq 0$ действительное число. Для числителей P_n и знаменателей Q_n подходящих дробей числа α_0 выполнены следующие рекуррентные соотношения

$$\begin{aligned} P_{n+1} &= a_{n+1}P_n + P_{n-1}, \\ Q_{n+1} &= a_{n+1}Q_n + Q_{n-1}, \end{aligned} \quad (7.6)$$

где $P_{-1} = 1, Q_{-1} = 0, P_0 = a_0, Q_0 = 1$.

Доказательство. Из определения 7.3 следуют равенства

$$\frac{P_0}{Q_0} = a_0, \quad \frac{P_1}{Q_1} = a_0 + \frac{1}{a_1} = \frac{a_1 a_0 + 1}{a_1},$$

которые задают начальные значения для соотношений (7.6).

Проведем доказательство по индукции. Предположим, что утверждение леммы выполнено для всех индексов равных или меньших n , то есть выполнено равенство

$$\frac{P_n}{Q_n} = [a_0, a_1, \dots, a_n] = \frac{a_n P_{n-1} + P_{n-2}}{a_n Q_{n-1} + Q_{n-2}}.$$

Тогда утверждение леммы следует из следующего равенства

$$\begin{aligned} \frac{P_{n+1}}{Q_{n+1}} &= [a_0, a_1, \dots, a_n, a_{n+1}] = \\ &= \left[a_0, a_1, \dots, a_n + \frac{1}{a_{n+1}} \right] = \frac{\left(a_n + \frac{1}{a_{n+1}} \right) P_{n-1} + P_{n-2}}{\left(a_n + \frac{1}{a_{n+1}} \right) Q_{n-1} + Q_{n-2}} = \\ &= \frac{a_{n+1} (a_n P_{n-1} + P_{n-2}) + P_{n-1}}{a_{n+1} (a_n Q_{n-1} + Q_{n-2}) + Q_{n-1}} = \frac{a_{n+1} P_n + P_{n-1}}{a_{n+1} Q_n + Q_{n-1}}. \end{aligned}$$

□

Основываясь на доказательстве леммы 7.2, легко заметить, что из равенства

$$[a_0, \dots, a_n] = \frac{a_n P_{n-1} + P_{n-2}}{a_n Q_{n-1} + Q_{n-2}},$$

следует равенство

$$\alpha_0 = [a_0, \dots, \alpha_{n+1}] = \frac{\alpha_{n+1} P_n + P_{n-1}}{\alpha_{n+1} Q_n + Q_{n-1}}. \quad (7.7)$$

Отметим, что неравенство (7.3) и формулы (7.6) позволяют заключить, что числители и знаменатели подходящих дробей удовлетворяют неравенствам

$$P_n > 0, \quad Q_n > 0.$$

Далее мы будем считать, что действительное число α является как рациональным, так и иррациональным.

Лемма 7.3. При всех индексах $n = 0, 1, \dots$ для числителей P_n и знаменателей Q_n подходящих дробей выполнено следующее соотношение

$$P_{n+1}Q_n - Q_{n+1}P_n = (-1)^n. \quad (7.8)$$

Доказательство. Используя равенства (7.6), получим следующие равенства

$$\begin{aligned} P_{n+1}Q_n - Q_{n+1}P_n &= (a_{n+1}P_n + P_{n-1})Q_n - (a_{n+1}Q_n + Q_{n-1})P_n = \\ &= -(P_nQ_{n-1} - Q_nP_{n-1}) = (-1)^2(P_{n-1}Q_{n-2} - Q_{n-1}P_{n-2}) = \dots \\ &= (-1)^k(P_{n-k+1}Q_{n-k} - Q_{n-k+1}P_{n-k}), \end{aligned}$$

для любого $k = 1, 2, \dots$

Подставляя в полученные равенства $k = n+1$ и начальные значения $P_{-1} = 1, P_0 = a_0, Q_{-1} = 0, Q_0 = 1$ из (7.6), получим равенство

$$P_{n+1}Q_n - Q_{n+1}P_n = (-1)^{n+2},$$

которое равносильно утверждению леммы. \square

Следствие 7.0.А. Для любого индекса $n = 0, 1, \dots$ подходящая дробь $\frac{P_n}{Q_n}$ несократима.

Доказательство. Следствие очевидным образом следует из равенства (7.8). Если предположить обратное, то найдется целое число d_n такое, что $\text{НОД}(P_n, Q_n) = d_n > 1$ и $d_n | (-1)^{n+1}$. Последнее условие невыполнимо. \square

Докажем еще одно следствие, которое может быть использовано для решения сравнений первой степени.

Следствие 7.0.В. Пусть a и m взаимно простые целые числа и $\frac{P_0}{Q_0}, \dots, \frac{P_n}{Q_n}$ последовательность подходящих дробей к числу $\alpha = \frac{m}{a}$. Тогда решение уравнения $ax \equiv b \pmod{m}$ удовлетворяет сравнению

$$x \equiv (-1)^n b P_{n-1} \pmod{m}$$

для некоторого натурального индекса n .

Доказательство. Разложим число $\alpha = \frac{m}{a}$ в непрерывную дробь и определим последовательность подходящих дробей $\frac{P_0}{Q_0}, \dots, \frac{P_n}{Q_n}$. Поскольку α рациональное число, то согласно лемме 7.1, непрерывная дробь конечна и найдется индекс n такой, что $\frac{P_n}{Q_n} = \frac{m}{a}$.

Поскольку дробь $\frac{P_n}{Q_n}$ несократима, а числа m, a взаимно просты, то выполнены равенства $P_n = m, Q_n = a$. Тогда, из равенства (7.8) следует, что

$$mQ_{n-1} - aP_{n-1} = (-1)^{n-1}, \quad \text{или} \quad aP_{n-1} = (-1)^n + mQ_{n-1}.$$

Последнее равенство позволяет нам записать сравнение $aP_{n-1} \equiv (-1)^n \pmod{m}$ или, домножая на $(-1)^n b$, сравнение $a(-1)^n b P_{n-1} \equiv b \pmod{m}$. Последнее сравнение в явном виде определяет значение неизвестного x , а именно, $x \equiv (-1)^n b P_{n-1} \pmod{m}$. Следствие доказано. \square

Лемма 7.4. При всех индексах $n = 0, 1, \dots$ для числителей P_n и знаменателей Q_n подходящих дробей выполнено следующее соотношение

$$P_{n+1}Q_{n-1} - Q_{n+1}P_{n-1} = a_{n+1}(-1)^{n+1}. \quad (7.9)$$

Доказательство. Для доказательства леммы домножим первое равенство в (7.6) на Q_{n-1} и вычтем из полученного второе равенство из (7.6), домноженное на P_{n-1} . Учитывая предыдущую лемму, получаем, с точностью до показателя степени при -1 , искомое равенство

$$P_{n+1}Q_{n-1} - Q_{n+1}P_{n-1} = a_{n+1}(P_nQ_{n-1} - Q_nP_{n-1}) = a_{n+1}(-1)^{n-1}.$$

\square

Лемма 7.5. Для всех индексов $n = 1, 2, \dots$ знаменатели Q_n подходящих дробей удовлетворяют неравенству $Q_{n+1} > 2^{\lceil \frac{n}{2} \rceil}$ или, что равносильно

$$\begin{cases} Q_{n+1} \geq 2^{\frac{n}{2}}, & \text{при четном } n, \\ Q_{n+1} \geq 2^{\frac{n+1}{2}}, & \text{при нечетном } n. \end{cases} \quad (7.11)$$

Доказательство. Из соотношений (7.3) и (7.6) следует неравенство

$$Q_{n+1} = a_{n+1}Q_n + Q_{n-1} \geq Q_n + Q_{n-1} \geq 2Q_{n-1} + Q_{n-2} \geq 2Q_{n-1},$$

из которого следует утверждение леммы – при нечетном n выполнено неравенство $Q_{n+1} \geq 2^{\frac{n+1}{2}}Q_0 = 2^{\frac{n+1}{2}}$, а при четном n – выполнено неравенство $Q_{n+1} \geq 2^{\frac{n}{2}}Q_1 \geq 2^{\frac{n}{2}}$. \square

Теперь мы можем доказать теорему о приближении числа α_0 последовательностью подходящих дробей.

29. Теорема о сходимости подходящих дробей

Теорема 7.1. Пусть $\alpha_0 \neq 0$ действительное число. Тогда последовательность подходящих дробей сходится к α_0 , то есть выполнено условие

$$\alpha_0 = \lim_{n \rightarrow \infty} \frac{P_n}{Q_n}.$$

Доказательство. Сначала мы покажем, что последовательность подходящих дробей сходится. Действительно, из леммы 7.3 получаем равенство

$$\left| \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} \right| = \frac{1}{Q_n Q_{n+1}} |P_{n+1}Q_n - Q_{n+1}P_n| = \frac{1}{Q_n Q_{n+1}}.$$

Из этого равенства и из утверждения леммы 7.5 следует, что последовательность подходящих дробей сходится, то есть

$$\lim_{n \rightarrow \infty} \left| \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} \right| = 0.$$

Нам осталось выяснить чему равен предел последовательности подходящих дробей. Учитывая равенство (7.7) и утверждение леммы 7.3, получим следующее равенство

$$\begin{aligned} \alpha_0 - \frac{P_n}{Q_n} &= \frac{1}{Q_n} (\alpha_0 Q_n - P_n) = \\ &= \frac{1}{Q_n} \left(Q_n \frac{\alpha_{n+1} P_n + P_{n-1}}{\alpha_{n+1} Q_n + Q_{n-1}} - P_n \right) = \\ &= \frac{1}{Q_n} \left(\frac{Q_n P_{n-1} - P_n Q_{n-1}}{\alpha_{n+1} Q_n + Q_{n-1}} \right) = \frac{(-1)^n}{Q_n (\alpha_{n+1} Q_n + Q_{n-1})}. \end{aligned} \quad (7.12)$$

Вспоминая, что α_n и Q_n положительны при всех $n \geq 1$, получаем неравенство

$$\begin{aligned} \left| \alpha_0 - \frac{P_n}{Q_n} \right| &= \frac{1}{Q_n (\alpha_{n+1} Q_n + Q_{n-1})} \leqslant \\ &\leqslant \frac{1}{Q_n (a_{n+1} Q_n + Q_{n-1})} = \frac{1}{Q_{n+1} Q_n}, \end{aligned} \quad (7.13)$$

из которого вытекает утверждение теоремы. \square

(Доказательство лемм 7.3 и 7.5 в 28 вопросе)

Лемма 7.3. При всех индексах $n = 0, 1, \dots$ для числителей P_n и знаменателей Q_n подходящих дробей выполнено следующее соотношение

$$P_{n+1}Q_n - Q_{n+1}P_n = (-1)^n. \quad (7.8)$$

Лемма 7.5. Для всех индексов $n = 1, 2, \dots$ знаменатели Q_n подходящих дробей удовлетворяют неравенству $Q_{n+1} > 2^{\lceil \frac{n}{2} \rceil}$ или, что равносильно

$$\begin{cases} Q_{n+1} \geq 2^{\frac{n}{2}}, & \text{при четном } n, \\ Q_{n+1} \geq 2^{\frac{n+1}{2}}, & \text{при нечетном } n. \end{cases} \quad (7.11)$$

30. Квадратичные иррациональности. Приведенные квадратичные иррациональности и теорема о периодичности квадратичных иррациональностей

Напомним, что целое число D называется полным квадратом, если найдется целое число d такое, что $D = d^2$.

Определение 7.4. Действительное число α называется квадратичной иррациональностью, если найдутся такие целые, взаимно простые числа $u > 0, v, w$, что значение $v^2 - 4uw > 0$ не является полным квадратом, а α является одним из корней многочлена $f(x) = ux^2 + vx + w$, то есть $f(\alpha) = 0$.

Величина $D = v^2 - 4uw$ называется дискриминантом квадратичной иррациональности α .

Из определения 7.4 следует, что любая квадратичная иррациональность может быть представлена в виде

$$\alpha = \frac{A + \sqrt{D}}{B}, \quad (7.14)$$

где A, B, D – целые числа, $D = v^2 - 4uw$ не является полным квадратом и

$$\begin{cases} A = -v, B = 2u, & \text{либо} \\ A = v, B = -2u, & \end{cases} \quad (7.15)$$

в зависимости от того, какой из двух корней многочлена $f(x)$ выбирается. Если величина D удовлетворяет сравнению $D \equiv 0 \pmod{4}$, то из равенства $v^2 = D + 4uv$ следует, что величина v четна. Тогда равенства (7.15) принимают вид

$$A = \mp v, B = \pm u. \quad (7.16)$$

Возникает вопрос: единственны ли указанное представление? Для ответа на него предположим, что равенство (7.14) не единственны, то есть найдется еще одна пара целых чисел C, E таких, что $\alpha = \frac{C + \sqrt{D}}{E}$. Тогда выполнено равенство

$$E(A + \sqrt{D}) = B(C + \sqrt{D}),$$

откуда

$$EA - BC = (B - E)\sqrt{D}. \quad (7.17)$$



В левой части равенства (7.17), в силу выбора значений A, B, C, E , находится целое число. В правой части – произведение целого числа на корень из N , не являющегося полным квадратом, то есть действительное число. Таким образом, равенство (7.17) может быть выполнено только в том случае, если в обеих его частях находятся нули. Из этого следует, что $B = E$, $A = C$ и представление (7.17) единственno.

Определение 7.5. Пусть $\alpha = \frac{A + \sqrt{D}}{B}$ квадратичная иррациональность – корень многочлена $f(x) = ux^2 + vx + w$. Тогда второй корень этого многочлена

$$\hat{\alpha} = \frac{A - \sqrt{D}}{B}$$

называется квадратичной иррациональностью, сопряженной с α .

Теорема 7.2. Пусть $\alpha = \frac{A + \sqrt{D}}{B}$ квадратичная иррациональность. Тогда ее непрерывная дробь периодична.

Доказательство. Вначале предположим, что α_0 приведенная квадратичная иррациональность, то есть

$$\alpha_0 > 1, \quad a_0 \geq 1, \quad -1 < \hat{\alpha}_0 < 0.$$

Тогда из (7.8) следует, что $\alpha_1 > 1$. Далее, следуя равенству (7.24), получим

$$\frac{1}{\hat{\alpha}_1} = \hat{\alpha}_0 - a_0 < 0 - a_0 \leq -1,$$

следовательно, $-1 < \hat{\alpha}_1 < 0$ и α_1 является приведенной квадратичной иррациональностью.

Продолжая далее, мы получим, что α_2 и все остальные полные частные $\alpha_n = \frac{A_n + \sqrt{D}}{B_n}$ являются приведенными квадратичными иррациональностями. Из леммы 7.7 следует, что значения A_n, B_n неотрицательны, ограничены сверху и бесконечная последовательность пар A_n, B_n принимает значения на конечном множестве. Следовательно, найдется некоторый индекс n_0 такой, что $A_0 = A_{n_0}$, $B_0 = B_{n_0}$ и последовательность α_n зациклится или, другими словами, периодична.

Для завершения доказательства теоремы нам осталось показать, что для любой квадратичной иррациональности α_0 найдется такой индекс n_0 , что α_{n_0} является приведенной квадратичной иррациональностью.

Вначале рассмотрим частный случай. Пусть

$$\alpha_0 = A_0 + \sqrt{D}$$

и α_0 не является приведенной. Тогда $a_0 = A_0 + \lfloor \sqrt{D} \rfloor$ и равенство (7.24) позволяет записать неравенства

$$-1 < \hat{\alpha}_1 = \frac{1}{\hat{\alpha}_0 - a_0} = \frac{-1}{\sqrt{D} + \lfloor \sqrt{D} \rfloor} < 0.$$

Следовательно, α_1 приведенная квадратичная иррациональность.

Теперь перейдем к общему случаю. Рассмотрим равенство (7.25) и, учитывая равенство (7.12), полученное в ходе доказательства теоремы 7.1, при $n \geq 1$, получим

$$\begin{aligned} \hat{\alpha}_{n+1} &= -\frac{\hat{\alpha}_0 Q_{n-1} - P_{n-1}}{\hat{\alpha}_0 Q_n - P_n} = \\ &= -\frac{Q_{n-1}}{Q_n} \left(\frac{\hat{\alpha}_0 - \frac{P_{n-1}}{Q_{n-1}}}{\hat{\alpha}_0 - \frac{P_n}{Q_n}} \right) = -\frac{Q_{n-1}(1 + \omega_{n+1})}{Q_n}, \end{aligned} \quad (7.26)$$

где точное значение ω_{n+1} определено равенством

$$\omega_{n+1} = \frac{\left(\frac{(-1)^{n-1}}{Q_{n-1}(\alpha_n Q_{n-1} + Q_{n-2})} - \frac{(-1)^n}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})} \right)}{\hat{\alpha}_0 - \alpha_0 + \frac{(-1)^n}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})}}. \quad (7.27)$$

Равенство (7.26) позволяет сделать следующее заключение. Если величина ω_{n+1} удовлетворяет неравенствам

$$-1 < \omega_{n+1} < \frac{Q_n}{Q_{n-1}} - 1, \quad (7.28)$$

то, при $n \geq 1$, из (7.26) вытекают неравенства $-1 < \hat{\alpha}_{n+1} < 0$. Следовательно, α_{n+1} приведенная квадратичная иррациональность и, как мы доказали ранее, ее разложение в непрерывную дробь периодично. Следовательно, периодично разложение для α_0 .

Нам осталось показать, что найдется индекс $n \geq 1$, для которого выполнены неравенства (7.28). Рассмотрим равенство (7.27) более подробно и обозначим символом δ_{n+1} числитель дроби, то есть

$$\delta_{n+1} = (-1)^{n-1} \left(\frac{1}{Q_{n-1}(\alpha_n Q_{n-1} + Q_{n-2})} + \frac{1}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})} \right).$$

Поскольку α_n и Q_n положительные целые числа, то выполнено $|\delta_{n+1}| < 1$. Более того

$$\begin{aligned} |\delta_{n+1}| &= \frac{1}{Q_{n-1}(\alpha_n Q_{n-1} + Q_{n-2})} + \frac{1}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})} \leq \\ &\leq \frac{1}{Q_{n-1}(a_n Q_{n-1} + Q_{n-2})} + \frac{1}{Q_n(a_{n+1} Q_n + Q_{n-1})} = \\ &= \frac{1}{Q_n Q_{n-1}} + \frac{1}{Q_{n+1} Q_n} = \frac{1}{Q_n} \left(\frac{1}{Q_{n+1}} + \frac{1}{Q_{n-1}} \right). \end{aligned} \quad (7.29)$$

Обозначим $\gamma = \hat{\alpha}_0 - \alpha_0$ и рассмотрим знаменатель дроби (7.27), тогда

$$\begin{aligned} \left| \hat{\alpha}_0 - \alpha_0 + \frac{(-1)^n}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})} \right| &\geq \\ |\gamma| - \frac{1}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})} &\geq |\gamma| - \frac{1}{Q_{n+1} Q_n}. \end{aligned}$$

С учетом (7.29), мы получили следующее неравенство

$$\begin{aligned} |\omega_{n+1}| &\leq \frac{|\delta_{n+1}|}{|\gamma| - \frac{1}{Q_{n+1} Q_n}} \leq \\ &\leq \left(\frac{1}{Q_{n+1}} + \frac{1}{Q_{n-1}} \right) \frac{Q_{n+1}}{Q_{n+1} Q_n |\gamma| - 1} = \\ &= \frac{Q_{n+1} + Q_{n-1}}{Q_{n+1} Q_n Q_{n-1} |\gamma| - Q_{n-1}}. \end{aligned}$$

Полученное неравенство позволяет нам сделать вывод о том, что всегда найдется индекс n , при котором будут выполнены ограничения на ω_{n+1} , то есть неравенства (7.28). Если $|\gamma|$ принимает большие значения, например $|\gamma| > 1$, то выполнение неравенств (7.28) очевидно. Более тонким является случай, когда значения $|\gamma|$ близки к нулю.

Предположим, что $|\gamma|$ ограничен снизу величиной

$$|\gamma| > \frac{3}{Q_n Q_{n-1}} = \frac{3Q_{n+1}}{Q_{n+1} Q_n Q_{n-1}} > \frac{Q_{n+1} + 2Q_{n-1}}{Q_{n+1} Q_n Q_{n-1}},$$

тогда выполнено $|\omega_{n+1}| < 1$.

В силу того, что Q_n образуют монотонно возрастающую последовательность, замечаем, что для сколь угодно малого значения $\gamma = \hat{\alpha}_0 - \alpha_0$ найдется такой индекс n , что будет выполнено неравенство $|\gamma| > \frac{3}{Q_n Q_{n-1}}$ и, следовательно, $|\omega_{n+1}| < 1$. \square