ТЧ экз

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

Основные множества:

1. Множество натуральных чисел $\mathbb{N} = \{1, 2, 3, 4, \dots\}$, если число n принадлежит этому множеству, то и число n+1 также будет принадлежать ему.
2. Множество целых чисел $\mathbb{Z} = -\mathbb{N} \cup 0 \cup \mathbb{N}$.

Непустое множество $\mathbb{M}$ называется **группой**, если:

1. Задана бинарная операция $\varphi(a, b) \to \mathbb{M}, \forall a, b \in \mathbb{M}$
2. Эта операция ассоциативна $\varphi(\varphi(a, b), c) = \varphi(a, \varphi(b, c))$
3. $\exists e$ - нейтральный элемент множества $\mathbb{M}$:

   $$\varphi(a, e) = \varphi(e, a) = a, \forall a \in \mathbb{M}$$
4. $\forall a \;\; \exists a^{-1} \in \mathbb{M} : \varphi(a, a^{-1}) = e$

Группа M называется **коммутативной или абелевой**, если операция φ коммутативна, то есть $\varphi(a, b) = \varphi(b, a)$.

Непустое множество M называется **кольцом**, если:

1. Заданы две бинарные операции $\varphi(a, b) \to \mathbb{M}\ и\ \lambda(a, b) \to \mathbb{M}, \forall a, b \in \mathbb{M}$.
2. Относительно операции φ M образует коммутативную группу.
3. Операция λ - ассоциативна.
4. Эти операции дистрибутивны. $\lambda(a, \varphi(b, c)) = \varphi(\lambda(a, b), \lambda(a, c))$

Кольцо M называется **кольцом с единицей**, если M содержит нейтральный элемент, относительно операции λ. Такой элемент называется **единичным элементом.**

Кольцо M называется **полем**, если относительно операции λ множество ненулевых элементов M образует коммутативную группу.

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

Коммутативное кольцо U называется **целостным**, если $a \cdot b = 0 \Rightarrow$, либо $a = 0$, либо $b = 0$.

Теорема о погружении целостного кольца в поле. Пусть U - целостное кольцо с единицей. Тогда найдётся поле F такое, что $F \supset U$.

Опр.: Отношение эквивалентность ~.

1. $a \sim a$
2. $a \sim b \Rightarrow b \sim a$
3. $a \sim b, b \sim c \Rightarrow a \sim c$

Док-во.

Рассмотрим множество упорядоченных пар (a, b) элементов из U таких, что $b \neq 0$ и введем отношение эквивалентности двух пар:

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

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) ~ (c, d) или ad = bc.

Множество классов будем обозначать F. Определим операции сложения и умножения классов эквивалентности.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Приведенные определения корректно определены, поскольку для $b \neq 0, d \neq 0$ и кольцо U - целостное, то величина $bd \neq 0$, а также данные определения не зависят от выбора представителя классов. Пусть $(a_1, b_1) \sim (a, b)$ или $a_1 b = a b_1$. Тогда:

$$\frac{a_1}{b_1} + \frac{c}{d} = \frac{a_1 d + c b_1}{b_1 d} = \frac{(a_1 d + c b_1) b}{b_1 d b} = \frac{a_1 d b + c b_1 b}{b_1 d b} = \frac{a b_1 d + c b_1 b}{b_1 d} = \frac{ad + cb}{bd} = \frac{a}{b} + \frac{c}{d}$$

$$\frac{a_1}{b_1} \cdot \frac{c}{d} = \frac{a_1 c}{b_1 d} = \frac{a_1 c b}{b_1 d b} = \frac{a b_1 c}{b_1 d b} = \frac{ac}{bd} = \frac{a}{b} \cdot \frac{c}{d}$$

Нейтральными элементами для этих операций являются $\frac{0}{1}$ и $\frac{1}{1}$.

$$\frac{a}{b} + \frac{0}{1} = \frac{1a + 0b}{1b} = \frac{a}{b}$$

$$\frac{a}{b} \cdot \frac{1}{1} = \frac{1a}{1b} = \frac{a}{b}$$

Обратный элемент для операции +: $\frac{-a}{b}$

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab - ab}{bb} = \frac{0}{bb} = \frac{0}{b}$$

Обратный элемент для операции $\cdot$: $\frac{b}{a}$

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}$$

Эти операции ассоциативны:

$$(\frac{a}{b} + \frac{c}{d}) + \frac{e}{f} = \frac{ad+cb}{bd} + \frac{e}{f} = \frac{adf+cbf+ebd}{bdf} = \frac{afd+b(cf+ed)}{bfd} =$$

$$= \frac{a}{b} + \frac{cf+ed}{fd} = \frac{a}{b} + (\frac{c}{d} + \frac{e}{f})$$

$$(\frac{a}{b} \cdot \frac{c}{d}) \cdot \frac{e}{f} = \frac{ac}{bd} \cdot \frac{e}{f} = \frac{ace}{bdf} = \frac{a}{b} \cdot \frac{ce}{df} = \frac{a}{b} \cdot (\frac{c}{d} \cdot \frac{e}{f})$$

И коммутативны:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd} = \frac{cb+ad}{db} = \frac{c}{d} + \frac{a}{b}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \cdot \frac{a}{b}$$

Таким образом, F - поле.

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

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

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

$$\frac{cb}{b} = \frac{c_1b_1}{b_1} \Rightarrow cbb_1 = c_1b_1b \Rightarrow c = c_1$$

Следовательно элементам кольца U однозначно сопоставляются элементы поля F.

Поскольку

$$\frac{cb}{b} + \frac{c_1b_1}{b_1} = \frac{(c+c_1)bb_1}{bb_1}$$

$$\frac{cb}{b} \cdot \frac{c_1b_1}{b_1} = \frac{(cc_1)bb_1}{bb_1}$$

то операции сложения и умножения оставляют множество $\{\frac{cb}{b}\}$ замкнутым, т.е не выводят за его пределы и образуют кольцо U. Таким образом $U \subset F$. ЧТД

3. Понятие евклидова кольца. Теорема о том, что кольцо целых чисел - евклидово.

Определение: отображение N: $\mathbb{U} \rightarrow \mathbb{N}_0$ называется **нормой**, если выполнены следующие условия:

1. $N(0) = 0$
2. $\exists a : N(a) \neq 0$
3. Если $a \neq 0$ *и* $a|b \Rightarrow N(a) \leq N(b)$

Мультипликативная норма: $N(ab) = N(a) \cdot N(b)$

Аддитивная норма: $N(ab) = N(a) + N(b)$

Определение: U - коммутативное кольцо, в котором задана норма N,, тогда U - **евклидово кольцо**, если N обладает следующим условием. $\forall a, b \in U, \text{где } a \neq 0$ найдутся элементы $q, r \in U$:

$$b = aq + r, \text{где } 0 \leq N(r) < N(a) \text{ или } r = 0$$

Теорема: Кольцо целых чисел $\mathbb{Z}$ - евклидово. $N(a) = |a|$. То есть для любой пары чисел a, b, таких, что $a \neq 0$, найдутся целые q, r, такие, что:

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

Аксиома 1 (Архимеда): $\forall a, b \, \exists c \; ac > b$

Аксиома 2: M - конечное подмножество Z $\Rightarrow$ существует минимальный и максимальным элемент M.

Док-во теоремы:

Предположим, что a,b неотрицательные целые числа и $a \neq 0$, тогда $\exists c : ac > b \Rightarrow c \geq 0 \Rightarrow \exists c - min$

Для c - min: $ac > b \geq a(c-1)$

Обозначим $q = c - 1, r = b - a(c-1)$. Тогда:

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

Докажем единственность q и r. Пусть найдутся q_1, r_1 такие, что

$$aq + r = aq_1 + r_1, \; a > r_1 \geq 0.a(q - q_1) = r_1 - r$$

Так как $a > |r_1 - r| \geq 0$ и левая часть кратна a, то равенство возможно только если $r_1 - r = 0b > 0, a > 0 \; r_1 = r, q_1 = q$. Для случая $b > a > 0$ теорема доказана.

Пусть выполнено равенство $|b| = |a|q + r$. Тогда:

$$b < 0, a > 0 \Rightarrow b = -|b| = -|a|q - r + |a| - |a| = a(-q-1) + r_0, r_0 = |a| - r, |a| > r_0 > 0$$

$$b < 0, a < 0 \Rightarrow b = -|b| = -|a|q - r + |a| - |a| = -|a|(q+1) + r_0 = a(q+1) + r_0$$

$$b \geq 0, a < 0 \Rightarrow b = |b| = |a|q + r = -|a|(-q) + r = a(-q) + r$$

Таким образом, для любого $a, b \; a \neq 0$ найдутся $q, r : b = aq + r, |a| > r \geq 0$.
Следовательно Z - евклидово кольцо.

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

Определение: Пусть a, b элементы Евклидового кольца U. Элемент $d \in U, d \neq 0$, называется **наибольшим общим делителем**($НОД(a, b)$), если

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

Теорема. Пусть U - евклидово кольцо, $a, b \in U$, одновременно не равные нулю, тогда $НОД(a, b)$ существует и он единственен с точностью до ассоциированных значений.

Доказательство. Рассмотрим множество $D = \{au + bv : u, v \in U\}$.

Выберем в этом множестве элемент d отличный от 0 с наименьшей нормой, поскольку хотя бы один из элементов a, b отличен от 0, то найдётся хотя бы один d, отличный от нуля.

Предположим, что $d \nmid a$, тогда $a = dq + r, \; N(d) > N(r), \; r \neq 0$. r удовлетворяет равенству: $r = a - dq = a - (au + bv)q = a(1 - u) - bvq$, следовательно $r \in D$, и так как $N(d) > N(r)$, это противоречит условию тому, что у d наименьшая норма. Следовательно $d|a$.

Аналогично с b. Пусть
$d \nmid a \Rightarrow b = dq + r, N(d) > N(r), r \neq 0 \Rightarrow r = b - dq = b - (au + bv)q = b(1 - v) - auq \Rightarrow r \in D.$
Так как $N(d) > N(r)$, это противоречит условию тому, что у d наименьшая норма. Следовательно $d|b$.

Так как $d|a$ и $d|b$, то d - общий делитель a, b.

Пусть $\exists \delta : \delta|a, \delta|b$, тогда $a = s\delta, b = t\delta$.

$d = au + bv = s\delta u + t\delta v = \delta(su + tv) \Rightarrow \delta|d$

Покажем, что d - единственен с точностью до ассоциирования. Пусть найдётся d_1 - другой $НОД(a, b)$. Так как d_2 - общий делитель, а d - НОД, то $d_2|d$. Так как d - общий делитель, а d_2 - НОД, то $d|d_2$. Получаем $d_2 \sim d$, чтд.

Следствие (Соотношение Безу). Пусть a, b элементы Евклидового кольца U. Тогда найдутся элементы $u, v \in U$ такие, что $au + bv \sim НОД(a, b)$

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

Свойства НОД:

1. $НОД(a, b) = НОД(b, a)$
2. $НОД(a, \varepsilon) = 1, если \; \varepsilon \in U^*$

3. $НОД(a, 0) = a$
4. $c \neq 0,\ НОД(ac, bc) = НОД(a, b) \cdot c$
5. $НОД(a, b) = НОД(a, b \pm a)$
6. $НОД(a, b) = НОД(a, r), b = aq + r$
7. $НОД(a, c) = 1 \Rightarrow НОД(a, bc) = НОД(a, b)$
   Док-во шестого свойства.
   $d = НОД(a, b),\ \delta = НОД(a, r = b - aq)$

$$\begin{matrix} \delta | a \\ \delta | r \end{matrix} \Rightarrow \begin{matrix} a = s\delta \\ r = t\delta \end{matrix} \Rightarrow b = aq + r = s\delta q + t\delta = \delta(sq + t) \Rightarrow \delta | b \Rightarrow \delta | НОД(a, b)$$

$$\begin{matrix} d | a \\ d | b \end{matrix} \Rightarrow \begin{matrix} a = pd \\ b = hd \end{matrix} \Rightarrow r = b - aq = hd - pdq = d(h - pq) \Rightarrow d | r \Rightarrow d | НОД(a, r)$$

Таким образом, $\delta \sim d \Rightarrow НОД(a, b) = НОД(a, r)$ чтд
Алгоритм Евклида. a, b оба отличны от 0, $b = q_0 a + r_0,\ N(r_0) < N(a)$

$$\begin{aligned} a &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-1} &= q_{n+1} r_n + r_{n+1} \end{aligned}$$

$N(a) > N(r_0) > \cdots > N(r_n) > N(r_{n+1})$
$N(a), N(r_0), \ldots$ - убывающая последовательность целых чисел, ограниченная снизу нулём, в силу определения нормы, следовательно, найдётся $N(r_{n+1}) = 0 \Rightarrow r_{n+1} = 0$.
Из свойств НОД получаем:
$НОД(a, r_0) = НОД(r_0, r_1) = \cdots = НОД(r_{n-1}, r_n) = НОД(r_n, r_{n+1}) = НОД(r_n, 0) = r_n$

6. Теорема Ламэ.

Теорема Ламэ. Пусть $a, b \in Z$, и $b \geq a > 0$ $\exists c : n \leq 1 + c \log_2 b$, тогда $\exists c : n \leq 1 + c \log_z b$, где n - количество делений с остатком в Алгоритме Евклида.

Определение. Последовательностью чисел Фибоначчи называется рекуррентная последовательность целых чисел:

$$A_0 = 0,\ A_1 = 1,\ A_{n+1} = A_n + A_{n-1}$$

Лемма. Пусть $z = \frac{1+\sqrt{5}}{2}$ - действительный положительный корень уравнения $z^2 = z + 1$. Тогда для последовательности Фибоначчи при всех натуральных n выполнено $A_{n+1} \geq z^{n-1}$.
Доказательство леммы. По мат индукции. При n = 1 очевидно, тк $A_2 = 1 = z^0$. Пусть условие леммы выполнено для всех индексов меньших или равных n, тогда:

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

ЧТД.
Доказательство теоремы Ламэ.

1. Докажем, что $r_{k-1} \geq A_{n+1-k}$
   При $k = n$. $A_{n+1-n} = A_1 = 1$, что меньше r_{n-1}, так как $r_{n-1} > r_n$, а r_n минимум равна 1. Для $k = n$ доказано.
   Предположим, что для всех $n, n-1, \ldots, k+1, k$ неравенство выполнено. Тогда:
   $$r_{k-1} = r_k q_{k+1} + r_{k+1} \geq r_k + r_{k+1} \geq A_{n-k} + A_{n-(k+1)} = A_{n+1-k}$$
2. Из доказанного неравенства и леммы, при $k = 0$ получаем.
   $$b \geq a = r_{-1} \geq A_{n+1} \geq z^{n-1} \Rightarrow \log_z b \geq \log_z z^{n-1} = n - 1 \Rightarrow$$
   $$\Rightarrow n \leq 1 + \log_z b = 1 + \frac{1}{\log_2 z} \log_2 b = 1 + c \log_2 b \text{ ЧТД}$$

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

Определение. Множество делителей элемента $a \in U$. $\{\varepsilon, a\epsilon : \varepsilon \in U^*\}$ определенное для всех возможных обратимых элементов кольца U (ε - обратимый элемент U, если $\exists \varepsilon^{-1} : \varepsilon\varepsilon^{-1} = 1$), 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. Если элемент a кольца U имеет только несобственные делители, то a является **неразложимым**.

Неразложимые положительные числа в кольце целых чисел Z принято называть **простыми**.

Так как в кольце целых чисел для любого числа n множество несобственных делителей будет состоять из $\{-1, 1, -n, n\}$, то положительное целое число n будет простым, если оно делится только на $1, -1, n, -n$.

Теорема. Пусть U - кольцо, содержащее хотя бы один необратимый элемент. 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 $p_1, \ldots, p_k$ для некоторого натурального k.

Определим элемент $p = p_1 \cdot \ldots \cdot p_k + \varepsilon,\ \varepsilon \in U^*$, являющийся произведением всех неразложимых элементах кольца, к которому прибавлен обратимый элемент ε. $p \in U$ так как операции сложения и умножения не выводят за пределы кольца.

Проверим, что $p \neq 0$. Если $p = 0 \Rightarrow p_1 p_2 \cdot \ldots \cdot p_k + \varepsilon = 0 \Rightarrow -p_1 p_2 \cdot \ldots \cdot p_k \varepsilon^{-1} = 1$ так как p_i - неразложимые, то они не могут быть обратимыми, следовательно равенство $p = 0$ не выполняется.

Теперь предположим, что найдётся такой индекс i, что $i \in \{1, 2, \dots, k\}$ и $p_i = p$, тогда выполнено равенство:

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

Из этого равенства вытекает противоречие с тем, что элементы $p_1, \dots, p_k$ необратимы, следовательно все элементы $p_1, \dots, p_k$ отличны от p.

Если p - неразложимый, то мы в явном виде предъявили новый неразложимый элемент, опровергнув наше изначальное предположение.

Если p - разложимый и необратимый, то существует неразложимый собственный делитель v элемента p.

Поскольку для любого индекса $i \in \{1, 2, \dots, k\}$ выполнено равенство

$$p = q_i p_i + \varepsilon, \;\; q_i = p_1 \cdot \ldots \cdot p_{i-1} p_{i+1} \cdot \ldots \cdot p_k, \;\; \varepsilon \neq 0$$

то ни один из элементов $p_1, \dots, p_k$ не делит элемент p и, следовательно, отличен от v. Противоречие. Теорема доказана.

Доп теорема, если спросят. Пусть U – евклидово кольцо, содержащее хотя бы один необратимый элемент a. Тогда в кольце U найдется хотя бы один неразложимый элемент p и p|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 $N(p_1) \leqslant N(p_2) \leqslant \dots \leqslant N(p_k)$. Без ограничения общности считаем, что элемент $p = p_1$ 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 $N(v) \geqslant N(p1)$. Вместе с тем, из того, что $v|p_1$ 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.

8. Основная теорема арифметики.

Лемма: Если $НОД(a, b) = 1$ и $au = bv$, тогда $a|v, b|u$

Доказательство. Согласно соотношению Безу $\exists s, t : as + bt = 1 \Rightarrow bt = 1 - as$.

$$\begin{gathered} au = bv \\ atu = btv \\ atu = (1 - as)v \\ atu = v - asv \\ a(tu + sv) = v \Rightarrow a|v \end{gathered}$$

Аналогично с $b|u$. ЧТД

Основная теорема арифметики. U - евклидовое кольцо. a - произвольный, отличный от нуля элемент, тогда

1. a можно представить в виде произведения: $a = \varepsilon_1 \cdot \ldots \cdot \varepsilon_s \cdot p_1 \cdot \ldots \cdot p_k$, где $\varepsilon_1, \ldots, \varepsilon_s \in U, p_1, \ldots p_k$ - неразложимые.
2. Это разложение единственно, с точностью до ассоциированности и перестановки.
   Доказательство.
   Доказательство существования.
   Если a - неразложим, то можем представить $a = p_1$ ЧТД
   Если a - обратимый, то $a = \varepsilon,\ \varepsilon \in U^*$ ЧТД
   Если a - разложим, то найдётся неразложимый элемент $p_1 \in U : p_1|a$ и $a = p_1 a_1,\ a_1 \in U$. При этом будет выполнено $N(a_1) \leq N(a)$.
   Применим аналогичные рассуждения к a_1 и получим цепочку равенств:

$$\begin{gathered} a = p_1 a_1, \qquad\qquad N(a_1) \leq N(a) \\ a = p_1 p_1 a_2,\ N(a_2) \leq N(a_1) \leq N(a) \\ \vdots \\ a = p_1 p_2 \cdot \ldots \cdot p_k a_k,\ N(a_k) \leq \ldots \leq N(a) \end{gathered}$$

Поскольку $N(a_i)$ принимают неотрицательные значения и убывают, то на каком-то шаге k a_k будет неразложимым, обозначим его за p_{k+1}, Таким образом $a = p_1 p_2 \cdot \ldots \cdot p_k p_{k+1}$.
$p_i = \varepsilon \pi_i$, где $\varepsilon \in U^*,\ \pi_i$ - ассоциированный с p_i элемент, тогда π_i также неразложимый.
Таким образом выполнено равенство:
$a = \varepsilon_1 \cdot \ldots \cdot \varepsilon_s \pi_1 \cdot \ldots \cdot \pi_s p_{s+1} \cdot \ldots \cdot p_k$, где $\varepsilon_1, \ldots, \varepsilon_s \in U, \pi_1, \ldots, \pi_s, p_s + 1, \ldots, p_k$ - неразложимые. ЧТД.
Существование доказано.
Доказательство единственности.
Пусть существует два разложения числа a.

$$\lambda q_1 \cdot \ldots \cdot q_s = a = \varepsilon p_1 \cdot \ldots \cdot p_k$$

где $\lambda, \varepsilon \in U^*$ - произведения λ_i и ε_i, соответственно, $q_1, \ldots, q_e, p_1, \ldots, p_k$ - неразложимые. Кроме того будет считать, что $s \leq k$.
$q_1 \cdot \ldots \cdot q_s = \varepsilon \lambda^{-1} p_1 \cdot \ldots \cdot p_k = \varepsilon' p_1 \cdot \ldots \cdot p_k$

1. Если $q_i \sim p_i \Rightarrow q_i = \phi_i p_i, \phi_i \in U^*$
2. Если $q_i \nsim p_i \Rightarrow \text{НОД}(q_i, p_i) = 1$, так как они не разложимы.
   $q_i u = p_i v = a \Rightarrow q_i | v \Rightarrow \exists j\ p_j \sim q_i$, что возвращает нас к первому пункту.
   Таким образом.
   $\phi_1 q_1 \cdot \ldots \cdot \phi_s q_s = \varepsilon' p_1 \cdot \ldots \cdot p_k$
   Если $s = k$, то

$$\phi_1 \cdot \ldots \cdot \phi_k = \varepsilon'$$

Мы получили, что $p_i \sim q_i, \forall i = 1, \dots, k$, в этом случае теорема доказана.
Если $s < k$, то

$$\phi_1 \cdot \ldots \cdot \phi_s = \varepsilon' p_{s+1} \cdot \ldots \cdot p_k 1 = \varepsilon' \phi_1^{-1} \cdot \ldots \cdot \phi_s^{-1} p_{s+1} \cdot \ldots \cdot p_k$$

Следовательно $p_{s+1} \cdot \ldots \cdot p_k$ - обратимые, что противоречит тому, что они неразложимы, следовательно $s = k$, а для $s = k$ единственность доказана.
Теорема доказана.

9. Решето Эратосфена в кольце целых чисел.

Лемма. U - евклидово кольцо, m - разложимый, тогда $\exists a | m$:

1. $N(a)^2 \leq N(m)$, если N - мультипликативна.
2. $2N(a) \leq N(m)$, если N - аддитивна.
   Доказательство.
   $m = \varepsilon_1 \cdot \ldots \cdot \varepsilon_k a_1 \cdot \ldots \cdot a_l, \varepsilon_i \in U^*, a_1, \ldots, a_l$ - неразложимые.
   Предположим, что $N(a_1) \leq \ldots \leq N(a_e)$. Это предположение не нарушает общность.
   Предположим, что утверждение леммы не выполнено.
   N - мультипликативна.
   $N^2(a_1) > N(m) = N(\varepsilon_1 \cdot \ldots \cdot \varepsilon_k a_1 \cdot \ldots \cdot a_l) = N(\varepsilon_1) \cdot \ldots \cdot N(\varepsilon_k) N(a_1) \cdot \ldots \cdot N(a_l) = N(a_1) \cdot \ldots \cdot N(a_l$
   $N^2(a_1) > N^l(a_1)$ - противоречие при $l \geq 2$. А если $l = 1$, то m - неразложимое.
   N - аддитивна.
   $2N(a_1) > N(m) = N(\varepsilon_1 \cdot \ldots \cdot \varepsilon_k a_1 \cdot \ldots \cdot a_l) = N(\varepsilon_1) + \ldots + N(\varepsilon_k) + N(a_1) + \ldots + N(a_l) = N(a_1) +$
   $2N(a_1) > lN(a_1)$ - противоречие при $l \geq 2$. А если $l = 1$, то m - неразложимое.
   Лемма доказана.
   Решето Эратосфена.
   Из доказанной леммы следует, что у разложимого m всегда найдётся неразложимый делитель p, норма которого ограничена нормой m. Решето Эратосфена - алгоритм для поиска всех неразложимых элементов кольца U, норма которых ограничена сверху некоторым натуральным значением b.
   Для кольца целых чисел решето Эратосфена состоит в следующем.
   Выпишем все натуральные целые числа от 2 до максимального значения b, упорядочив их по возрастанию норм, т.е

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, \ldots, b-1, b$$

   Первое число в этой последовательности будет иметь минимально возможную норму для необратимого элемента, поэтому оно не может быть разделено на какой-либо другой необратимый элемент с меньшей нормой. Следовательно оно неразложимо.
   Отметим двойку в качестве неразложимого, вычеркнем все элементы, делящиеся на 2, и получим следующую последовательность.

$$[2], 3, 5, 7, 9, 11, 13, 15, 17, \ldots, b$$

Рассмотрим следующее неотмеченное число с наименьшей нормой, те тройку. Данное число не делится на ранее отмеченный элемент с наименьшей нормой, следовательно также является неразложимым элементом кольца. Отметим тройку и вычеркнем все числа, делящиеся на 3.

$$[2],[3],5,7,11,13,17,19,\dots,b$$

Далее применим ту же процедуру к следующему неотмеченному элементу с минимальной нормой, те к пятёрке, затем к 7 и так далее до тех пор, пока мы не отметим элемент p, такой, что $N^2(p)>N(b)$. При этом может оказаться, что b будет вычеркнуто на каком-то шаге. Оставшиеся числа окажутся неразложимыми, согласно утверждению доказанной выше леммы. Добавив к этим элементам ассоциированные получим все неразложимые элементы кольца целых чисел.

$$\pm2,\pm3,\pm5,\pm7,\pm11,\pm13,\pm17,\dots$$

10. Понятие класса вычетов. Свойства классов вычетов.

Определение. Пусть U - евклидово кольцо, $a,b,m\in U$ элементы этого кольца и $m\neq0$. Мы будем говорить, что элементы a и b сравнимы по модулю m и записывать $b\equiv a(mod\,m)$, если $m|(b-a)$, т.е. элемент m делит разность $b-a$.

Лемма 1. Пусть U - евклидово кольцо, $m\neq0, a\equiv b(mod\,m)$, тогда

1. $b\equiv a(m)$
2. $\forall c\in U,\quad a\pm c\equiv b\pm c(mod\,m)$
3. Если $НОД(a,b)=d,\ d|m$, то $\frac{a}{d}\equiv\frac{b}{d}(mod\,\frac{m}{d})$
4. Если $НОД(a,b)=d,\ НОД(d,m)=1$, то $\frac{a}{d}\equiv\frac{b}{d}(mod\,m)$
5. Если $\exists c: c|a,\ c|m$, то $c|b$

Доказательство.

1. $a\equiv b(mod\,m)\Rightarrow m|(b-a)\Rightarrow mk=b-a\Rightarrow m(-k)=a-b\Rightarrow m|(a-b)\Rightarrow b\equiv a(mod\,m)$ ЧТД
2. $a\equiv b(mod\,m)\Rightarrow m|(b-a)\Rightarrow mk=b-a\Rightarrow mk=a\pm c-(b\pm c)\Rightarrow m|(a\pm c-(b\pm c))\Rightarrow$ $\Rightarrow a\pm c\equiv b\pm c(mod\,m)$ ЧТД
3. $a\equiv b(mod\,m)\Rightarrow m|(b-a)\Rightarrow\exists k: mk=b-a$
   $НОД(a,b)=d\Rightarrow\begin{matrix}d|b\\d|a\end{matrix}\Rightarrow\begin{matrix}b=db_1\\a=da_1\end{matrix}$
   $mk=d(b_1-a_1);\ d|m\Rightarrow m=dm_1$
   $dm_1k=d(b_1-a_1)\Rightarrow m_1k=b_1-a_1\Rightarrow m_1|(b_1-a_1)\Rightarrow b_1=a_1(mod\,m_1)$ ЧТД
4. $a\equiv b(mod\,m)\Rightarrow m|(b-a)\Rightarrow\exists k: mk=b-a$
   $НОД(a,b)=d\Rightarrow\begin{matrix}d|b\\d|a\end{matrix}\Rightarrow\begin{matrix}b=db_1\\a=da_1\end{matrix}\Rightarrow mk=d(b_1-a_1)$

$\begin{matrix} НОД(m,d)=1 \\ mk=d(b_1-a_1) \end{matrix} \Rightarrow d|k \Rightarrow k=dk_1 \Rightarrow mdk_1=d(b_1-a_1)$
$\Rightarrow mk_1=b_1-a_1 \Rightarrow m|(b_1-a_1) \Rightarrow\Rightarrow b_1 \equiv a_1(mod\, m)$ ЧТД

5. $\begin{matrix} c|a \\ c|m \end{matrix} \Rightarrow \begin{matrix} a=ca_1 \\ m=cm_1 \end{matrix}$
   $a \equiv b(mod\, m) \Rightarrow m|(b-a) \Rightarrow mk=b-a \Rightarrow cm_1k=b-ca_1$
   Так как с делит левую часть уравнения, то с должно делить и правую часть уравнения, следовательно $c|(b-ca_1)$. Так как $c|ca_1$, то $c|b$ ЧТД

Определение. Пусть m - отличный от нуля элемент евклидового кольца U. $\forall a \quad \overline{a}_m=\{a+km, k\in U\}$ - класс вычетов по модулю m, элементы этого множества - вычеты по модулю m, a - представитель класса вычетов $\overline{a}_m$.

Лемма. Пусть $\overline{a}_m, \overline{b}_m$ - классы вычетов по модулю m.

1. Если $a\in\overline{b}_m$ и $b\in\overline{a}_m$, тогда $\overline{a}_m=\overline{b}_m$
2. Если $c\in\overline{b}_m$ и $c\in\overline{a}_m$, тогда $\overline{a}_m=\overline{b}_m$

Доказательство.

1. $a\in\overline{b} \Rightarrow a=b+km$ и $b\in\overline{a}\Rightarrow b=a+lm$
   $a=b+km=a+(l+k)m \Rightarrow \overline{a}\subset\overline{b}$
   $b=a+lm=b+(l+k)m \Rightarrow \overline{b}\subset\overline{a}$
   Таким образом, $\overline{a}=\overline{b}$
2. $\overline{a}=\{a+km\},\ \overline{b}=\{b+lm\}$
   $c\in\overline{a}\Rightarrow c=a+km$
   $c\in\overline{b}\Rightarrow c=b+lm$
   $a+km=b+lm \Rightarrow m(k-l)=b-a \Rightarrow m|(b-a) \Rightarrow a\equiv b(mod\, m)$
   Таким образом a, b - представители одного класса вычетов, следовательно $\overline{a}=\overline{b}$.
   Лемма доказана.

11. Теорема о кольце классов вычетов.

Теорема. Пусть U - евклидово кольцо и m - отличный от нуля элемент U. Множество классов вычетов $U/(m)$ образует кольцо.

Доказательство. Определим операции.

$$\overline{c}=\overline{a}+\overline{b},\ \ \overline{d}=\overline{a}\cdot\overline{b}$$

Где представители классов $\overline{c}, \overline{d}$ определяются условиями:

$$c\equiv a+b(mod\, m),\ \ d\equiv a\cdot b(mod\, m)$$

Рассмотрим операцию сложения.

1. Надо доказать, что $(\overline{a}+\overline{b})+\overline{c}=\overline{a}+(\overline{b}+\overline{c})$.
   Пусть $\overline{d}=(\overline{a}+\overline{b})+\overline{c}$, тогда

$d \equiv (a+b)+c\ (mod\, m) \equiv a+(b+c)\ (mod\, m) \Rightarrow \overline{d} = \overline{a}+(\overline{b}+\overline{c})$
Таким образом $(\overline{a}+\overline{b})+\overline{c} = \overline{d} = \overline{a}+(\overline{b}+\overline{c})$ ЧТД

2. Надо доказать, что $\overline{a}+\overline{b} = \overline{b}+\overline{a}$
   Пусть $\overline{d} = \overline{a}+\overline{b}$, тогда $d \equiv a+b\ (mod\, m) \equiv b+a\ (mod\, m) \Rightarrow \overline{d} = \overline{b}+\overline{a}$
   Таким образом $\overline{a}+\overline{b} = \overline{d} = \overline{b}+\overline{a}$ ЧТД
3. $\exists\overline{0}$ - нулевой элемент. Это такой класс вычетов по модулю m, что $\overline{0} = \{cm, c \in U\}$ и его представитель - 0.
   Проверим, что $\overline{a}+\overline{0} = \overline{0}+\overline{a} = \overline{a}$.
   Пусть $\overline{d} = \overline{a}+\overline{0}$, тогда $d \equiv a+0\ (mod\, m) \equiv 0+a\ (mod\, m) \equiv a(mod\, m) \Rightarrow \overline{d} = \overline{0}+\overline{a}$ и $\overline{d} = \overline{a}$
   Таким образом $\overline{a}+\overline{0} = \overline{d} = \overline{0}+\overline{a} = \overline{d} = \overline{a}$ ЧТД
4. $\forall\overline{a}\ \exists\overline{(-a)}$ - противоположный элемент. Это такой класс вычетов, что по модулю m, что $\overline{(-a)} = \{-a+km, k \in U\}$ и его представитель - $(-a)$.
   Проверим, что $\overline{a}+\overline{-a} = \overline{0}$.
   Пусть $\overline{d} = \overline{a}+\overline{-a}$, тогда $d \equiv a+(-a)\ (mod\, m) \equiv 0\ (mod\, m) \Rightarrow \overline{d} = \overline{0}$
   Таким образом $\overline{a}+\overline{-a} = \overline{d} = \overline{0}$ ЧТД
   Таким образом относительно операции сложения $U/(m)$ - коммутативная группа.

Рассмотрим операцию умножения.

1. Надо доказать, что $(\overline{a}\cdot\overline{b})\cdot\overline{c} = \overline{a}\cdot(\overline{b}\cdot\overline{c})$
   Пусть $\overline{d} = (\overline{a}\cdot\overline{b})\cdot\overline{c}$, тогда $d \equiv (a\cdot b)\cdot c\ (mod\, m) \equiv a\cdot(b\cdot c)\ (mod\, m) \Rightarrow \overline{d} = \overline{a}\cdot(\overline{b}\cdot\overline{c})$
   Таким образом $(\overline{a}\cdot\overline{b})\cdot\overline{c} = \overline{d} = \overline{a}\cdot(\overline{b}\cdot\overline{c})$ ЧТД
2. Надо доказать, что $\overline{a}\cdot(\overline{b}+\overline{c}) = \overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}$.
   Пусть $\overline{d} = \overline{a}\cdot(\overline{b}+\overline{c})$, тогда
   $d \equiv a\cdot(b+c)\ (mod\, m) \equiv a\cdot b+a\cdot c\ (mod\, m) \Rightarrow \overline{d} = \overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}$
   Таким образом $\overline{a}\cdot(\overline{b}+\overline{c}) = \overline{d} = \overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}$ ЧТД
   Таким образом $U/(m)$ - кольцо.
   Теорема доказана.

12. Теорема о числе решений уравнения ax = b (mod m).

Теорема. Пусть U - евклидовое кольцо и a, b, m - элементы кольца U такие, что a, m отличны от нуля. Тогда количество классов вычетов, удовлетворяющих сравнению $ax \equiv b\ (mod\, m)$, равно

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

Доказательство. Начнём с первого утверждения теоремы. Пусть $\text{НОД}(a, m) = 1$ и покажем, что в этом случае найдётся только один класс вычетов, удовлетворяющий условию.

Воспользуемся соотношением Безу и найдём $u, v \in U$ такие, что

$$au + mv = \text{НОД}(a, m)$$

Учитывая, что $\text{НОД}(a, m) = 1$, найдётся $\varepsilon \in U^*$, такой, что

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

Следовательно, $au\varepsilon^{-1} \equiv 1 (mod\, m) \Rightarrow aub\varepsilon^{-1} \equiv b(mod\, m)$. Следовательно класс вычетов, представителем которого является $ub\varepsilon^{-1}$, удовлетворяет сравнению.

Предположим, что есть два класса вычета, удовлетворяющий этому условию.

$$\overline{x_1} = \{x_1 + k_1 m,\ k_1 \in U\},\ \overline{x_2} = \{x_2 + k_2 m,\ k_2 \in U\}$$

$$ax_1 \equiv b \equiv ax_2(mod\, m)$$
$$m|(ax_1 - ax_2) = a(x_1 - x_2)$$
$$mu = a(x_1 - x_2)$$

Так как $\text{НОД}(m, a) = 1$, то $m|(x_1 - x_2)$

$$mv = x_1 - x_2 \Rightarrow x_1 = x_2 + vm$$

Тогда x_1 принадлежит классу вычетов $\overline{x_2}$ по модулю m и является его представителем, следовательно эти классы вычетов совпадают. Таким образом первый пункт теоремы доказан.

Пусть $\text{НОД}(a, m) = d$, тогда из свойств сравнений должно выполняться $d|b$ иначе изначальное сравнение неразрешимо.

Будем считать, что $d|b$. Тогда

$$a = a_1 d,\ b = b_1 d,\ m = m_1 d$$

и тогда $a_1 x \equiv b_1(mod\, m_1)$, из свойства сравнений. Поскольку $\text{НОД}(a_1, m_1) = 1$, то в силу первого утверждения теоремы сравнение $a_1 x \equiv b_1(mod\, m_1)$ разрешимо и имеет единственное решение $\overline{x_1}$ - класс вычетов по модулю m_1.

$$\overline{x_1} = \{x + lm_1, l \in U\}$$

Выберем произвольный элемент l и зафиксирует $x_l = x + lm$.

$$\exists k \in U : a_1 x_l = b_1 + km_1 a x_l = a_1 d x_l = a_1 d(x + lm_1) = da_1 x + da_1 lm_1 =$$

$$= d(b_1 + km_1) + a_1 lm_1 d = b + km + a_1 lm = b + (k + la_1)m$$

те выполнено сравнение $ax_l \equiv b(mod\, m)$ и x_l является представителем класса вычетов, удовлетворяющего изначальному сравнению.

Осталось определить сколько различных классов вычетов по модулю m содержится в множестве $\overline{x_1}$.

В силу свойств кольца U найдётся натуральное число n и конечное число элементов $r_1, \ldots, r_n \in U$, являющимися остатками от деления на d и представителями различных классов вычетов по модулю d, те $r_i \not\equiv r_j (mod\, d)$ при $i \neq j$. $\forall l \;\; \exists q, r_i \in U$, удовлетворяющие равенству $l = qd + r_i, 0 \leq N(r_i) < N(d)$. Следовательно для любого элемента $x_l \in \overline{x_1}$ выполняется равенство

$$x_l = x + lm_1 = x + (qd + r_i)m_1 = (x + r_i m_1) + qm, x_l \equiv x + r_i m_1 (mod\, m)$$

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

$$x + r_i m_1 = x + r_j m_1 (mod\, m) r_i m_1 \equiv r_j m_1 (mod\, m) r_i \equiv r_j (mod\, m)$$

Это противоречит выбору остатков $r_1, \ldots, r_n$. Следовательно, все велечины $x + r_i m_1, i = 1, \ldots, n$ принадлежат различным классам вычета по модулю m. Следовательно кол-во классов вычетов, удовлетворяющих условию равно n, те количеству классов вычетов по модулю d. Что требовалось доказать.

Теорема доказана.

13. Расширенный алгоритм Эвклида и его приложения.

U - евклидовое кольцо, $a, b, m \in U$ и $m \neq 0$. Поиск классов вычетов, удовлетворяющих сравнению $ax \equiv b (mod\, m)$ сводится к решению соотношения Безу, те поиску элементов $u, v \in U$, таких, что

$$a_1 u + m_1 v = НОД(a_1, m_1) \quad и a_1 = \frac{a}{d},\; m_1 = \frac{m}{d},\; d = НОД(a, m)$$

Пусть a, m произвольные элементы евклидового кольца и $r_{-1}, r_0, \ldots$ последовательность удовлетворяющая равенствам $r_{-1} = m, r_0 = a$ и

$$\begin{gathered} r_{-1} = r_0 q_1 + r_1, \\ r_0 = r_1 q_2 + r_2, \\ r_1 = r_2 q_3 + r_3, \\ \vdots \\ r_{n-1} = r_n q_{n+1},\; r_{n+1} = 0, n \in \mathbb{N}_0 \end{gathered}$$

r_n - $НОД(a, m)$. Определим две последовательности элементов $u_{-1}, u_0, \ldots$ и $v_{-1}, v_0, \ldots$ равенствами.

$$\begin{gathered} u_{-1} = 0, u_0 = 1, \\ v_{-1} = 1, v_0 = 0, \\ u_{k+1} = u_{k-1} - q_k u_k, \\ v_{k+1} = v_{k-1} - q_k v_k \end{gathered}$$

Теорема. Пусть a, m - элементы евклидового кольца U, $r_{-1}, r_0, \ldots, r_n$, $u_{-1}, u_0, \ldots, u_n$ и $v_{-1}, v_0, \ldots, v_n$ последовательности, определённые расширенным алгоритмом Евклида. Тогда выполняется равенство

$$au_k + mv_k = r_k, k = -1, 0, 1, \ldots, n$$

В частности $au_n + mv_n = НОД(a, m)$.

Доказательство. По мат индукции.

Для $k = -1$: $au_{-1} + mv_{-1} = a \cdot 0 + m \cdot 1 = m = r_{-1}$ Выполняется.

Предположим, что равенство выполняется для всех значений $-1, 0, 1, \dots, k$

$$au_{k+1} + mv_{k+1} = a(u_{k-1} - q_k u_k) + m(v_{k-1} - q_k v_k) = au_{k-1} + mv_{k-1} - q_k(au_k + mv_k) =$$
$$= r_{k-1} - q_k r_k = r_{k+1}$$

Теорема доказана.

14. Китайская теорема об остатках.

Рассмотрим систему сравнений:

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

где элементы $a_1, \dots, a_k$ и $m_1, \dots, m_k$ принадлежат евклидовому пространству U, а кроме того, $НОД(m_i, m_j) = 1$, при $i \neq j$, те элементы $m_1, \dots, m_k$ попарно простые. Решение системы - множество элементов U, удовлетворяющих всем сравнениям системы.

Теорема(Китайская теорема об остатках). Пусть U - евклидово кольцо. $m_1, \dots m_k \in U$ - необратимые и взаимно-простые, $a_1, \dots, a_k$ - произвольные элементы U. $\exists!$ решение по модулю.

$M = \prod\limits_{i=1}^{k} m_i$

$** b_i = \frac{M}{m_i} = m_1, m_2, \dots, m_{i-1}, m_{i+1}, \dots, m_k **$

$c_i \equiv b_i^{-1} (mod\, m_i)$

$c_i b_i \equiv 1 (mod\, m_i)$

$x \equiv \sum\limits_{i=1}^{k} a_i b_i c_i (mod\, m)$ - решение.

Доказательство.

Рассмотрим i-ый индекс.

$a_i b_i c_i \equiv a_i (mod\, m_i)$, так как b_i, c_i - обратные по модулю m_i

$a_i b_i c_i \equiv 0 (mod\, m_j), \forall j \neq i$, так как $m_i | b_i$

Из этого следует, что x удовлетворяет системе уравнений.

Доказательство единственности.

Пусть существуют x, y: $\begin{matrix} x(mod\, M) \\ y(mod\, M) \end{matrix}$ - решения.

$$\begin{gathered} x-y \equiv a_1 - a_1 = 0(mod\, m_1) \Rightarrow \\ \Rightarrow x-y = m_1\gamma_1,\ \gamma_1 \in U \\ x-y \equiv a_2 - a_2 = 0(mod\, m_2) \Rightarrow \\ \Rightarrow x-y = m_2\gamma_2,\ \gamma_2 \in U \\ \dots \\ x-y \equiv a_k - a_k = 0(mod\, m_k) \Rightarrow \\ \Rightarrow x-y = m_k\gamma_k,\ \gamma_k \in U \end{gathered}$$

Таким образом $x-y = m_1\gamma_1 = m_2\gamma_2 = \ldots = m_k\gamma_k$. Так как m_i - взаимно-простые, то $m_i | \gamma_j,\ \forall j \neq i$.

$x - y = m_i\gamma_j \equiv 0(mod\, M) \Rightarrow x \equiv y(mod\, M)$

Таким образом x и y принадлежат одним классам вычетов - решение единственно.

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

Определение. Функция Эйлера $\varphi(m)$ - функция от натурального аргумента m, возвращающая количество взаимно-простых чисел в m на интервале $[1, \ldots, m]$.

Теорема. Пусть $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k},\ p_i$ - простое, α_i - натуральное. Тогда $\varphi(m) = \prod\limits_{i=1}^{k}(p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = \prod\limits_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)$

Доказательство.

1. $m = p$ - простое. $1, 2, 3, \ldots, p$
   Все числа кроме p - взаимно-простые с m, следовательно $\varphi(m) = p - 1$
2. $m = p^\alpha$
   $1, 2, 3, \ldots, p, \ldots, p^1, \ldots, p^2, \ldots, p^\alpha$
   Все числа $p^j,\ j = 1, \ldots, \alpha$ - не взаимно-простые с m. Таких чисел $\frac{p^\alpha}{p} = p^{\alpha-1}$. А остальные числа взаимно простые. Таким образом $\varphi(m) = p^\alpha - p^{\alpha-1}$.

Для доказательства основного утверждения надо доказать, что функция Эйлера мультипликативна для взаимно-простых чисел, те $\varphi(ab) = \varphi(a)\varphi(b)$.

Рассмотрим систему сравнений

$$\begin{cases} x \equiv c_1(mod\, a) \\ x \equiv c_2(mod\, b) \end{cases}$$

$x \equiv d(mod\, ab)$ - её единственное решение (из КТО).

Если $\begin{matrix} НОД(c_1,a)=1 \\ НОД(c_2,b)=1 \end{matrix}$, то $\begin{matrix} НОД(d,a)=1 \\ НОД(d,b)=1 \end{matrix}$ по свойству НОД, так как c_1, c_2 - остатки от деления d на a, b, соответственно. А из этого следует, что $НОД(d, ab) = 1$, также по свойству НОД(7ое св-во). В противном случае если $НОД(c_1, a) > 1$ или $НОД(c_2, b) > 1$, тогда $НОД(d, ab) > 1$, по тем же свойствам НОД.

Всего вариантов вычетов c_1 по модулю a - a, а вычетов c_2 по модулю b - b. Следовательно всего вариантов вычетов d - ab, так как все значения d по формуле ответа КТО различны, если различны вычеты c_1 или c_2.

Всего вариантов вычетов c_1 и c_2 таких, что они взаимно-просты с a, b, соответственно, $\varphi(a)$ и $\varphi(b)$. Таким образом у нас всего $\varphi(a) \cdot \varphi(b)$ систем с такими c_1, c_2. Следовательно у нас всего $\varphi(a) \cdot \varphi(b)$ решений d взаимно-простых с (ab).

А вычетов d , таких, что $НОД(d, ab) = 1$, всего $\varphi(ab)$.

Таким образом $\varphi(ab) = \varphi(a) \cdot \varphi(b)$, если a и b - взаимно-простые.

1. $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$

   Так как p_i - простые, то они взаимно просты. Следовательно

   $$\varphi(m) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k}) = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$$

   ЧТД

Теорема Эйлера. Пусть $a, m > 0$, $НОД(a, m) = 1$. Тогда $a^{\varphi(m)} \equiv 1 (mod\, m)$.

Доказательство. Рассмотри систему вычетов по модулю m, где каждый вычет взаимно-прост с m: $c_1, \ldots, c_{\varphi(m)}$. Она состоит из $\varphi(m)$ вычетов по определению функции Эйлера.

Домножим каждый вычет на a и получим систему вычетов по модулю m:
$ac_1, ac_2, \ldots, ac_{\varphi(m)}$
Необходимо доказать, что все ac_i являются представителями тех же вычетов по модулю m, что и c_i.

1. Докажем, что $НОД(ac_i, m) = 1$
   Так как $НОД(a, m) = 1$, то $НОД(ac_i, m) = НОД(c_i, m) = 1$
2. Докажем, что если $ac_i \not\equiv ac_j (mod\, m)$, при $i \neq j$
   Допустим, что $ac_i \equiv ac_j (mod\, m)$, тогда $c_i \equiv c_j (mod\, m)$, что выполняется только при $i = j$, так как c_i, c_j - различные вычеты по модулю m, при $i \neq j$. Возникает противоречие с тем, что $i \neq j$. Следовательно $ac_i \not\equiv ac_j (mod\, m)$ при $i \neq j$.

В итоге получаем, что все вычеты ac_i по модулю m различны и взаимно-просты с m. Так как их количество равно $\varphi(m)$, то эта система совпадает с системой c_i.

Следовательно получаем

$$c_1 \cdot \ldots \cdot c_{\varphi(m)} \equiv ac_1 \cdot \ldots \cdot ac_{\varphi(m)} (mod\, m)$$
$$1 \equiv a^{\varphi(m)} (mod\, m)$$

Таким образом теорема доказана.

Малая теорема Ферма. Пусть p - простое, a - целое, больше нуля, взаимно-простое с m. Тогда $a^{p-1} \equiv 1(mod\, m)$

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

Схема ассиметричного шифрования RSA(Rivest, Shamir, Adleman, 1977г)

Введём обозначения:

S - открытый текст, который необходимо зашифровать.

c - зашифрованный текст.

e - открытый ключ, он известен всем.

d - закрытый ключ, он есть только у получателя.

$m = pq$ - произведение случайных простых чисел q и p. Значение m известно, значения p, q - нет.

Подготавливаем все значения:

1. $m = pq$
2. находим d через $ed \equiv 1(mod\, \varphi(m))$ и **храним его в секрете.**

Зашифрование:

Получаем зашифрованный текст c через $S^e \equiv c(mod\, m)$

Расшифрование:

Для ясности преобразований выпишем равенства:

$ed = 1 + k\varphi(m)$, так как из подготовки значений имеем $ed \equiv 1(mod\, \varphi(m))$

$a^{\varphi(m)} \equiv 1(mod\, m)$ по тореме Эйлера

Применяем наш секреный ключ

$c^d \equiv (S^e)^d \equiv S^{ed} \equiv S^{1+k\varphi(m)} \equiv S \cdot S^{k\varphi(m)} \equiv S \cdot 1^k \equiv S(mod\, m)$

Как взломать? Раскладываем m на множители p и q. Теперь можно узнать $\varphi(m) = \varphi(p)\varphi(q) = (p-1)(q-1)$

Теперь можем узнать ключ d через расширенный алгоритм Евклида из $ed \equiv 1(mod\, \varphi(m))$

17. Теорема о числе корней многочлена по простому модулю.

Теорема. Пусть p - простое число и $f(x) \equiv 0(mod\, p)$, $f(x) = \sum\limits_{i=0}^{n} a_i x^i$. Тогда количество корней многочлена $f(x)$ не превосходит $n = deg f(x)$.

Доказательство.

1. e - корень по модулю $p \Rightarrow (x-e)|f(x)$

   $f(x) = q(x)(x-e) + r \; deg(r) = 0 \Rightarrow r \in \mathbb{Z}/(p)$

   Так как e - корень, то $f(e) \equiv 0(mod\, p) \Rightarrow q(e)(e-e) + r = 0(mod\, p) \Rightarrow 0 + r \equiv 0(mod\, p) \Rightarrow r \equiv 0(mod\, p)$
2. $e_1, \ldots, e_k$ - все корни по модулю p

   $f(x) = (x-e_1)(x-e_2)\cdot \ldots \cdot (x-e_k)u(x) \quad (mod\, p)$

   у $u(x)$ нет корней по модулю p

   $deg(f(x)) = n = k + deg(u(x)) \Rightarrow k \leq n$

ЧТД

18. Теорема о числе корней многочлена по составному модулю.

Теорема. Если $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, то x - корень многочлена $f(x)$ по модулю m будет удовлетворять системе сравнений

$$\begin{cases} f(x) \equiv 0(mod\, p_1^{\alpha_1}) \\ \ldots \\ f(x) \equiv 0(mod\, p_k^{\alpha_k}) \end{cases}$$

и наоборот.

А также $N(m)$ - количество решений $f(x) \equiv 0(mod\, m)$. $N(p_i^{a_i})$ - количество решений $f(x) \equiv 0(mod\, p_i^{\alpha_i})$. Тогда $N(m) = N(p_1^{\alpha_1}) \cdot \ldots \cdot N(p_k^{\alpha_k})$

Доказательство.

1. Доказательство совпадения решения системы и изначального сравнения.
   Пусть e - корень
   $f(x) \Rightarrow f(e) \equiv 0(mod\, m) \Rightarrow \exists c: f(e) = 0 + cm = cp_1^{\alpha_1} \cdot \ldots \cdot p_1^{\alpha_1} \Rightarrow p_i^{\alpha_i} | f(e)\ \forall i \Rightarrow f(e) \equiv$
   $\equiv 0(mod\, p_i^{\alpha_i})$
   Пусть e - решение системы. Тогда $f(e) \equiv 0(mod\, p_i^{\alpha_i})\ \forall i \Rightarrow p_i^{\alpha_i} | f(e)$.
   Так как $f(e)$ делится на все $p_i^{\alpha_i}$ и p_i - взаимно-простые, то $f(e)$ делится
   $p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} = m \Rightarrow f(e) \equiv 0(mod\, m)$
   Таким образом решение системы совпадает с решением $f(x) \equiv 0(mod\, m)$.
2. Доказательство количества решений.
   Пусть у нас есть набор сравнений со свои набором решений.

$$f(x) \equiv 0(mod\, p_1^{\alpha_1}),\ решения\ a_1, \ldots, a_{r_1}$$
$$\ldots$$
$$f(x) \equiv 0(mod\, p_k^{\alpha_k}),\ решения\ b_1, \ldots, b_{r_k}$$

   В каждом наборе содержится $N(p_i^{\alpha_i})$ решений.
   Чтобы решить систему вида.

$$\begin{cases} f(x) \equiv 0(mod\, p_1^{\alpha_1}) \\ \ldots \\ f(x) \equiv 0(mod\, p_k^{\alpha_k}) \end{cases} (1)$$

   Нужно найти такое e, чтобы $f(e)$, удовлетворяло всем сравнениям.
   Найдём e для конкретного набора $a_1, \ldots, b_1$.
   Получаются следующие верные сравнения

$$\begin{cases} f(a_1) \equiv 0(mod\, p_1^{\alpha_1}) \\ \ldots \\ f(b_1) \equiv 0(mod\, p_k^{\alpha_k}) \end{cases} (2)$$

   Таким образом, e должно удовлетворять системе

$$\begin{cases} e \equiv a_1(mod\, p_1^{\alpha_1}) \\ \ldots \\ e \equiv b_1(mod\, p_k^{\alpha_k}) \end{cases} (3)$$

   С помощью КТО находим $E(mod\, p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} = m)$ - вычет по модулю m, решение системы (3).
   Проверим, что E удовлетворяет системе (2).

$$f(E) = f(a_1 + c_1 p_1^{\alpha_1}) \equiv 0(mod\, p_1^{\alpha_1})$$
$$\ldots$$
$$f(E) = f(b_1 + c_k p_k^{\alpha_k}) \equiv 0(mod\, p_k^{\alpha_k})$$

   Следовательно, полученное решение E удовлетворяет системе (2), а следовательно и системе (1).
   Для каждого набора $a_i, \ldots, b_j$ будет своя система (3) и из КТО будет своё решение E_i.

Всего можно составить $N(p_1^{\alpha_1})\cdot\ldots\cdot N(p_k^{\alpha_k})$ систем (2), а следовательно всего будет столько же решений E_i, а следовательно и решений системы (1).

Таким образом, $N(m) = N(p_1^{\alpha_1})\cdot\ldots\cdot N(p_k^{\alpha_k})$, так как $N(m)$ - количество решений системы (1).

Теорема доказана.

19. Теорема о подъеме решения.

$f(x) = \sum\limits_{i=0}^{n} a_i x^i$

$f(x+c) = \sum\limits_{i=0}^{n} a_i (x+c)^i = \sum\limits_{i=0}^{n} a_i \sum\limits_{j=0}^{i} C_i^j x^{i-j} c^j = f(x) + cf'(x) + c^2 f''(x) + \ldots$

$f(x+c) \equiv f(x) + cf'(x) (mod\, c^2)$

Теорема. Пусть $e : f(e) \equiv 0 (mod\, p)$ и $f'(e) \not\equiv 0 (mod\, p)$.

Тогда $\exists e_\alpha : \begin{matrix} 1) f(e_\alpha) \equiv 0 (mod\, p^\alpha) \\ 2) e_\alpha \equiv e (mod\, p) \end{matrix}$

Доказательство. По индукции.

При $\alpha = 1$:

$f(e_1) \equiv 0 (mod\, p^1 = p) \Rightarrow e_1 = e$, следовательно e_1 существует и очевидно выполняется второе утверждение теоремы. Для $\alpha = 1$ доказано.

Пусть для всех $\alpha = 1, 2, \ldots, \alpha - 1$ выполняется.

Представим e_α в виде: $e_\alpha = e_{\alpha-1} + t \cdot p^{\alpha-1}, 0 \le t < p$

При таком выборе e_α второй пункт теоремы выполняется, так как $e_\alpha \equiv e_{\alpha-1} \equiv e (mod\, p)$

Тогда $f(e_\alpha) = f(e_{\alpha-1} + tp^{\alpha-1}) \equiv f(e_{\alpha-1}) + tp^{\alpha-1} f'(e_{\alpha-1})\ (mod\, t^2 p^{2(\alpha-1)})$

$f(e_\alpha) \equiv f(e_{\alpha-1}) + tp^{\alpha-1} f'(e_{\alpha-1}) (mod\, p^\alpha)$

$f(e_{\alpha-1}) + tp^{\alpha-1} f'(e_{\alpha-1}) - f(e_\alpha) \equiv 0 (mod\, p^\alpha)$

Если e_α - корень, то $f(e_\alpha) \equiv 0 (mod\, p^\alpha)$ тогда выполнится

$$f(e_{\alpha-1}) + tp^{\alpha-1} f'(e_{\alpha-1}) - f(e_\alpha) \equiv 0 (mod\, p^\alpha)$$
$$f(e_{\alpha-1}) + tp^{\alpha-1} f'(e_{\alpha-1}) - 0 \equiv 0 (mod\, p^\alpha)$$
$$f(e_{\alpha-1}) + tp^{\alpha-1} f'(e_{\alpha-1}) = hp^\alpha$$
$$0 = f(e_{\alpha-1}) + tp^{\alpha-1} f'(e_{\alpha-1}) + h'p^\alpha$$
$$t = -\frac{f(e_{\alpha-1}) + h'p^\alpha}{p^{\alpha-1} f'(e_{\alpha-1})}$$
$$t \equiv -\frac{f(e_{\alpha-1})}{p^{\alpha-1} f'(e_{\alpha-1})} (mod\, p)$$

Почему $f'(e_{\alpha-1}) \not\equiv 0(mod\, p)$?

Так как $e_{\alpha-1} \equiv e(mod\, p) \Rightarrow e_{\alpha-1} = e + \xi p$

$f'(e_{\alpha-1}) = f'(e+\xi p) = f'(e) + \xi p f''(e_{\alpha-1}) + \xi^2 p^2 \dots$

$f'(e_{\alpha-1}) \equiv f'(e)(mod\, p)$

Таким образом, мы нашли t, при котором e_α обладает нужными свойствами. Следовательно e_α существует. Теорема доказана.

20. Квадратичные вычеты. Понятие символа Лежандра. Критерий Эйлера.

Определение. Пусть p - нечётное, простое. $D \not\equiv 0(mod\, p)$. D - **квадратичный вычет** по модулю p, если $\exists x : x^2 \equiv D(mod\, p)$, иначе D - **квадратичный невычет**.

Лемма. Число квадратных вычетов по модулю $p =$ числу квадратных невычетов $= \frac{p-1}{2}$.

Доказательство.

$k = 1, 2, \dots, (p-1)$ - вычеты по модулю p. Среди них квадратными вычетами будут те, что сравнимы с $1^2, 2^2, \dots, (\frac{p-1}{2})^2$ - числа (1) по модулю p.

При $k : 1 \le k \le \frac{p-1}{2}$, k^2 очевидно входят в числа (1)

Остальные вычеты при $\frac{p-1}{2} < k \le p-1,\, k = p - l,\ l < \frac{p-1}{2}$ выполнено

$$k^2 \equiv (p-l)^2 \equiv l^2(mod\, p) \le (\frac{p-1}{2})^2$$

Таким образом все вычеты k при возведении в квадрат будут находится в числах (1), следовательно все квадратичные вычеты по модулю p сравнимы с числами (1).

Проверим, что числа (1) несравнимы друг с другом. Пусть среди чисел (1) найдётся хоть одна пара совпадающих, те $i^2 \equiv j^2(mod\, p),\ 1 \le i < j \le \frac{p-1}{2}$

Тогда сравнению $x^2 \equiv j^2(mod\, p)$ удовлетворяют четыре решения $i, -i, j, -j$, что невозможно, так как $deg(x^2) < 4$. Следовательно, числа (1) попарно несравнимы, а это значит, что всего квадратичных вычетов $\frac{p-1}{2}$

Поскольку всего вычетов $p-1$, а квадратичных вычетов из них $\frac{p-1}{2}$, то квадратичных невычетов $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$

ЧТД

Определение. Пусть p - нечётное простое, $D \not\equiv 0(mod\, p)$

$(\frac{D}{p})$ - символ Лежандра. $(\frac{D}{p}) = \begin{cases} 1,\ \textit{если } D - \textit{квадратичный вычет} \\ -1,\ \textit{если } D - \textit{квадратичный невычет} \end{cases}$

Лемма. Пусть p - нечётное простое, a - целое взаимно-простое с p. Тогда:

1. Если $a \equiv b(mod\, p)$, то $(\frac{a}{p}) = (\frac{b}{p})$
2. $(\frac{a}{p}) = a^{\frac{p-1}{2}}(mod\, p)$ Критерий Эйлера
3. $(\frac{1}{p}) = 1,\ (\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$
4. $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$
5. $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$
6. Если a - простое, тогда $(\frac{a}{p}) = (-1)^{\frac{p-1}{2}\frac{a-1}{2}}(\frac{p}{a})$ Квадратичный закон взнаимности Гаусса.

Доказательство.

1. Если $a \equiv b(mod\, p)$, то $(\frac{a}{p}) = (\frac{b}{p})$

   Это утверждение следует из того, что разрешимость сравнения $x^2 \equiv a(mod\, p)$ не зависит от выбора представителя класса вычета.
2. **Критерий Эйлера.** $(\frac{a}{p}) = a^{\frac{p-1}{2}}(mod\, p)$, p - нечётное простое, $\forall a \in \mathbb{Z} : НОД(a,p) = 1 \Rightarrow a \neq 0$

   Вспомним малую теорему Ферма: $\forall a : НОД(a,p) = 1$, p - простое выполняется $a^{p-1} \equiv 1(mod\, p)$

   Рассмотрим сравнение из МТФ.

   $a^{p-1} \equiv 1(mod\, p) \Rightarrow a^{p-1} - 1 \equiv 0(mod\, p)$, так как $p-1$ - чётное это сравнение приобретает вид.

   $$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0(mod\, p)$$

   $\exists k : (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) = kp$

   $\forall a, НОД(a,p) = 1$, выполняется одно из сравнений

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

   Пусть a - квадратичный вычет, тогда $\exists z : z^2 \equiv a(mod\, p)$
   $a^{\frac{p-1}{2}} \equiv (z^2)^{\frac{p-1}{2}} \equiv z^{p-1} \equiv 1(mod\, p)$ это удовлетворяет сравнению (1) и подтверждает, что все квадратные вычеты удовлетворяют сравнению (1)
   Рассмотрим многочлен $x^{\frac{p-1}{2}} - 1$ и найдём его решения по модулю p:

   $$x^{\frac{p-1}{2}} - 1 \equiv 0(mod\, p)\ (3)$$

   У этого многочлена не более $\frac{p-1}{2}$ решений, что равно числу квадратных вычетов, все из которых удовлетворяют этому сравнению. Следовательно решением

сравнения (3) будут только квадратные вычеты.
Осталось $\frac{p-1}{2}$ квадратных невычетов. Только они удовлетворяют сравнению (2), так как квадратный вычет не может быть решением сравнения (2).
Таким образом доказано, что соответствие символа Лежандра с квадратичным вычетом и невычетом отвечает Критерию Эйлера.

3. $(\frac{1}{p}) = 1,\ (\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$

   По Критерию Эйлера, так как $НОД(1,p) = 1$ и $НОД(-1,p) = 1$

   $(\frac{1}{p}) = 1^{\frac{p-1}{2}} = 1$

   $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$
4. $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$

   По критерию Эйлера. Если $a = bc$, то

   $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \equiv (b^{\frac{p-1}{2}})(c^{\frac{p-1}{2}}) \equiv (\frac{b}{p})(\frac{c}{p})\ (mod\, p)$

Доказательство 5ого и 6ого свойство требует доказательства леммы Гаусса, а это другой билет.

21. Квадратичный закон взаимности. Лемма Гаусса.

Лемма Гаусса. Пусть p - нечётное простое число, $a \in \mathbb{Z} : НОД(a,p) = 1$. Тогда для символа Лежандра выполнено равенство

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

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

$a, 2a, \ldots, \frac{p-1}{2}a$ - это множество $\{ka : 1 \leq k \leq \frac{p-1}{2}\}$

$ka = pq + r$

$0 \leq N(r) \leq N(p)$

$0 \leq |r| \leq |p|$

$-\frac{p-1}{2}$ $\qquad$ 0 $\qquad$ $\frac{p-1}{2}$ $\qquad$ p

```
|________|________________|____________|
```

Абсолютно-наименьший остаток должен находиться от $-\frac{p-1}{2}$ до $\frac{p-1}{2}$.
В случае если, $0 < r \leq \frac{p-1}{2}$, r - абсолютно-наименьший остаток.
Рассмотри случай, когда $\frac{p-1}{2} < r < p \Rightarrow -\frac{p+1}{2} < r - p < 0$, $r - p$ - абсолютно-

наименьший остаток

$ka = pq_k - r_k$

$-\frac{p+1}{2} < r_k \leq \frac{p-1}{2}$

$-\frac{p-1}{2} \leq r_k \leq \frac{p-1}{2}$

Для любого числа можно найти абсолютно-наименьший остаток

Доказательство. Обозначим символами

$$a_1, a_2, \ldots, a_\lambda, -b_1, -b_2, \ldots, -b_\mu \quad (2)$$

абсолютно-наименьшие вычеты чисел (1) по модулю p, то есть для всех $i = 1, \ldots, \lambda, \;\; j = 1, \ldots, \mu$ выполнено

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

Считаем, что все a_i, b_j - положительные, поэтому в (2) λ положительных и μ отрицательных чисел и $\lambda + \mu = \frac{p-1}{2}$.

Предположим, что $a_i = b_j \Rightarrow r_i \equiv -r_j \; (mod\, p) \Leftrightarrow r_i + r_j \equiv 0 (mod\, p)$

Так как и r_i , и r_j - остатки от деления на ka на p, то $r_i = k_1 a - q_1 p$, $r_j = k_2 a - q_2 p$

$r_i + r_j = k_1 a - q_1 p + k_2 a - q_2 p \equiv (k_1 + k_2) a \not\equiv 0 \; (mod\, p)$, так как $НОД(a,p) = 1$ и $p \nmid (k_1 + k_2)$, так как $2 \leq (k_1 + k_2) \leq p - 1$ и равенство достигается только при одинаковых k, чего быть не может.

Таким образом все числа

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

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

$$a_1 a_2 \cdot \ldots \cdot a_\lambda b_1 b_2 \cdot \ldots \cdot b_\mu = (\frac{p-1}{2})! \quad (3)$$

Каждое из чисел (2) сравнимо только с одним произведением ka, где $k = 1, 2, \ldots, \frac{p-1}{2}$, таким образом, с учётом равенства (3) получаем сравнение

$$(\frac{p-1}{2})! a^{\frac{p-1}{2}} = a \cdot 2a \cdot \ldots \cdot \frac{p-1}{2} a \equiv a_1 \cdot \ldots \cdot a_\lambda b_1 \cdot \ldots \cdot b_\mu (-1)^\mu \equiv (\frac{p-1}{2})! (-1) \mu \;\; (mod\, p)$$

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

$$(-1)^\mu \equiv a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \; (mod\, p)$$

Так как $|(\frac{a}{p})| = 1$, $|(-1)^\mu| = 1$ и $p \geq 3$ то мы можем перейти от сравнения к равно.
Таким образом, $(\frac{a}{p}) = (-1)^\mu$ ЧТД

22. Квадратичный закон взаимности. Доказательство основной теоремы.

Перед тем, как доказывать КЗВГ. Докажем, что $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$
Для этого зафиксируем множество чисел $a, 2a, \ldots, \frac{p-1}{2}a$ (1) и разделим каждое их них с остатком на p.

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

где $0 \leq r_k \leq p, 1 \leq k \leq \frac{p-1}{2}$.
Обозначим символами

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

абсолютно-наименьшие вычеты чисел (1) по модулю p, то есть для всех $i = 1, \ldots, \lambda, \;\; j = 1, \ldots, \mu$ выполнено

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

Тогда остатки r_k совпадают с множеством

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

Следовательно, можно записать равенства $(-b_j = r_j - p \Rightarrow r_j = p - b_j)$

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

Сложим почленно все равенства (2) и учитывая, что

$$1 + 2 + \ldots + \frac{p-1}{2} = (1 + \frac{p-1}{2})\frac{p-1}{2 \cdot 2} = \frac{p-1}{4} + \frac{(p-1)^2}{8} = \frac{p^2 - 2p + 1 + 2p - 2}{8} = \frac{p^2-1}{8}$$

Получаем

$$a(\frac{p^2-1}{8}) = p\sum_{k=1}^{\frac{p-1}{2}} q_k + \sum_{k=1}^{\frac{p-1}{2}} r_k = p\sum_{k=1}^{\frac{p-1}{2}} q_k + A - B + \mu p \quad (3)$$

Из доказательства Лемы Гаусса все числа $a_1, \ldots, a_\lambda, b_1, \ldots, b_\mu$ - различные числа от 1 до $\frac{p-1}{2}$. Следовательно

$$A + B = 1 + 2 + \ldots + \frac{p-1}{2} = \frac{p^2-1}{8} \Rightarrow A = \frac{p^2-1}{8} - B$$

Подставляя в (3) имеем

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

$$\frac{p^2-1}{8}(a-1) = p\sum_{k=1}^{\frac{p-1}{2}} q_k - 2B + \mu p \ \ (4)$$

Поскольку p - нечётное $p \equiv 1(mod\, 2)$. Пусть $a = 2$, тогда равенство (4) может быть записано в виде сравнения.

$$\frac{p^2-1}{8} = \sum_{k=1}^{\frac{p-1}{2}} q_k + \mu\ (mod\, 2)$$

При $a = 2$ все $q_k = 0$ это следует из того, что $2 \leq 2k \leq p-1$ те все ka не превосходят величины p. Таким образом,

$$\frac{p^2-1}{8} \equiv \mu\ (mod\, 2)$$

И учитывая лемму Гаусса

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

ЧТД

Квадратичный закон взаимности Гаусса.

Пусть a - нечётное простое, тогда $(\frac{p^2-1}{8})(a-1)$ - чётное. Тогда равенство (4) можно записать в виде сравнения

$$0 \equiv \sum_{k=1}^{\frac{p-1}{2}} q_k + \mu\ (mod\, 2)$$

$$\sum_{k=1}^{\frac{p-1}{2}} q_k \equiv \mu\ (mod\, 2)$$

Так как $q_k = \lfloor \frac{ka}{p} \rfloor$, то $\mu \equiv \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor\ (mod\, 2)$, откуда по лемме Гаусса получаем

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

Аналогично $(\frac{p}{a}) = (-1)^{\sum_{s=1}^{\frac{a-1}{2}} \lfloor \frac{sp}{a} \rfloor}$

Обозначим $\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor = S_1$ и $\sum_{s=1}^{\frac{a-1}{2}} \lfloor \frac{sp}{a} \rfloor = S_2$

Рассмотрим $S_1 = \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor$. $q_k = \lfloor \frac{ka}{p} \rfloor < \frac{ka}{p}$

$0 < k < \frac{p}{2}$ расположим целые k на оси x, каждому k соответствует своё q_k, расположим их на оси y. Так как $k < \frac{p}{2}$, то $q_k < \frac{a}{2}$

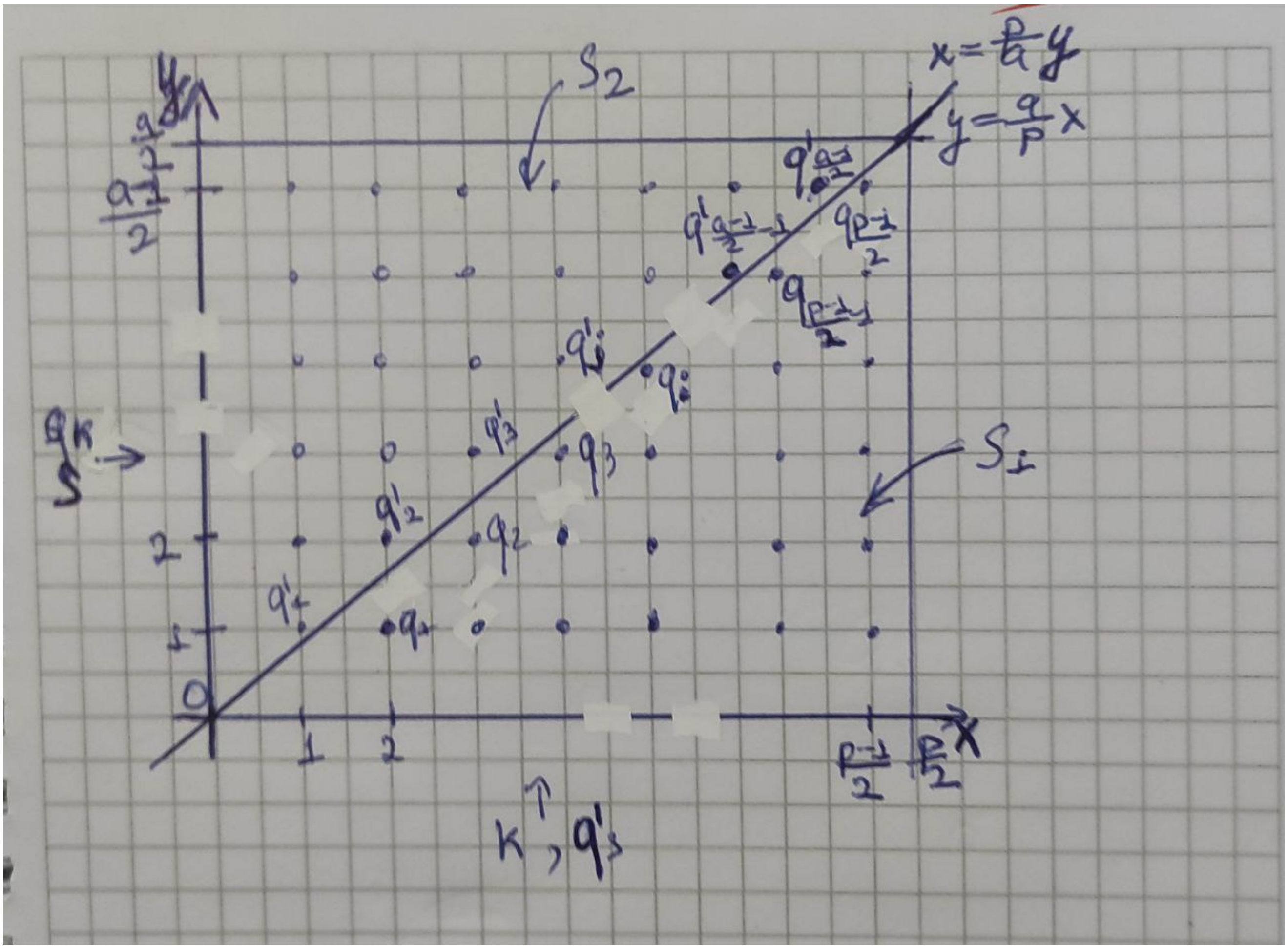
$q_k < \frac{ka}{p} \Rightarrow$ значения q_k находятся ниже прямой $y = \frac{a}{p}x$, причём максимально близко к ней. Таким образом каждое q_k равно количеству целых точек от точки $(k, 0)$ не включая её до точки $(k, \frac{ka}{p})$. Следовательно S_1 равен количеству всех целых точек ниже прямой $y = \frac{a}{p}x$, выше прямой $y = 0$ и левее $x = \frac{p}{2}$.

Рассмотрим $S_2 = \sum\limits_{s=1}^{\frac{a-1}{2}} \lfloor \frac{sp}{a} \rfloor$. $q'_s = \lfloor \frac{sp}{a} \rfloor < \frac{sp}{a}$

$0 < s < \frac{a}{2}$ расположим целые s на оси y, каждому s соответствует своё q'_s, расположим их на оси x. Так как $s < \frac{a}{2}$, то $q'_s < \frac{p}{2}$

$q'_s < \frac{sp}{a} \Rightarrow$ значения q'_s находятся левее прямой $x = \frac{p}{a}y$ она же прямая $y = \frac{a}{p}x$, причём максимально близко к ней. Таким образом каждое q'_s равно количеству целых точек от точки $(0, s)$ не включая её до точки $(\frac{sa}{p}, s)$. Следовательно S_2 равен количеству всех целых точек левее прямой $y = \frac{a}{p}x$, ниже прямой $y = \frac{a}{2}$ и правее $x = 0$.

Таким образом $S_1 + S_2$ равно количеству целых точек в квадрате с координатами его точек $(1, 1), (1, \frac{a-1}{2}), (\frac{p-1}{2}, \frac{a-1}{2}), (\frac{p-1}{2}, 1)$ (на прямой $y = \frac{a}{p}x$ нет целых точек входящих в наш квадрат, так как при $x : 1 \leq x < \frac{p-1}{2}$, $НОД(ax, p) = 1$). Всего целых точек в этом квадрате $(\frac{p-1}{2})(\frac{a-1}{2})$



Получаем

$$(\frac{a}{p})(\frac{p}{a}) = (-1)^{S_1+S_2} = (-1)^{(\frac{p-1}{2})(\frac{a-1}{2})} \ \ (1.1)$$
$$(\frac{a}{p}) = (-1)^{(\frac{p-1}{2})(\frac{a-1}{2})}(\frac{p}{a}) \ \ (1.2)$$

Из (1.1) можно перейти к (1.2) умножением левой и правой части на $(\frac{p}{a})$, так как $(\frac{p}{a})(\frac{p}{a}) = 1$

ЧТД

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

Пусть $m = pq > 0$ - нечетное составное число, p, q-простые

m - известно, открытый ключ p, q - неизвестны, закрытый ключ. Есть только у получателя

s - шифруемое сообщение

c - зашифрованное сообщение

Зашифрование:

Абонент А предоставляет s такое, что $1 < s < m - 1, НОД(s, m) = 1$

Вычисляем зашифрованное сообщение $c \equiv s^2(m)$

Расшифрование:

У получателя есть c, m, p, q.

Вычисляем значения $x_p^2 \equiv c(p)$ *и* $x_q^2 \equiv c(q)$
Найденные значения используются для поиска s_1, s_2, s_3, s_4 таких, что $s_i^2 \equiv c(m)$

Наличие нескольких вариантов расшифрования сообщения снижает практическую применимость данной схемы. Поэтому для однозначного определения s необходимо добавить код целостности. Это и поможет определить единственное значение s, и защитит от атак, основанных на изменении передаваемого значения.

Упрощение поиска квадратного корня:
Для упрощения вычислений x_p и x_q рекомендуется выбирать при генерации m выбирать $p \equiv q \equiv 3(4)$. В таком случае можно вспомнить лемму о поиске квадратного корня:
Лемма. p - нечетное простое, a - целое, $НОД(a, p) = 1$. Если сравнение $x^2 \equiv a(p)$ разрешимо (то есть а - квадратный вычет, это стоит помнить), то выполнены следующие утверждения:

1. $p \equiv 3(4) \Rightarrow x \equiv a^{\frac{p+1}{4}}(p)$ **нам нужен этот пункт**
2. $p \equiv 5(8) \Rightarrow$
   1. $a^{\frac{p-1}{4}} \equiv 1(p) \Rightarrow x \equiv a^{\frac{p+3}{8}}(p)$
   2. $a^{\frac{p-1}{4}} \equiv -1(p) \Rightarrow x \equiv 2a(4a)^{\frac{p-5}{8}}(p)$

   Тогда поиск x_q и x_p сводится к

$$x_p \equiv c^{\frac{p+1}{4}}(p)$$
$$x_p \equiv c^{\frac{q+1}{4}}(q)$$

24. Алгоритм нахождения корней многочленов по простому модулю.

Лемма 1. Для каждого простого p справедливо сравнение
$x^p - x \equiv x(x-1)(x-2) \cdot \ldots \cdot (x-p+1) \equiv \prod_{k=0}^{p-1}(x-k) \ \ (mod\, p)$

Доказательство. По Малой Теореме Ферма для каждого целого $e : 0 \leq e < p$ выполнено $e^{p-1} \equiv 1\ (mod\, p) \Rightarrow e^p \equiv e(mod\, p) \Rightarrow e^p - e \equiv 0(mod\, p)$ Следовательно все числа e_i являются корнями многочлена $x^p - x$. Следовательно $(x - e_1)|(x^p - x)$ и таким образом многочлен стоящий в правой части сравнения делит нацело многочлен, стоящий слева.

Поскольку степени обоих многочленов совпадают, а также совпадают коэффициенты при старших степенях, то можно сделать вывод о том, что сравнение леммы выполнено. ЧТД

Лемма 2. Пусть $f(x)$ произвольный многочлен из $\mathbb{F}_p[x]$. $h(x) = НОД(x^p - x, f(x))$
Тогда каждый корень многочлена $h(x)$ является корнем многочлена $f(x)$ и наоборот.

Доказательство.
$f(x)$ можно представить в виде $f(x) = a_n(x-e_1)^{\alpha_1}\cdot\ldots\cdot(x-e_r)^{\alpha_r}u(x)$, где e_i - различные корни многочлена $f(x)$, а многочлен $u(x)$ не имеет корней.

Так как согласно предыдущей лемме многочлен $x^p - x$ раскладывается на произведение p различных линейных множителей, следовательно

$$h(x) = \text{\textit{НОД}}(x^p - x, f(x)) = (x-e_1)\cdot\ldots\cdot(x-e_r)$$

Из чего следует, что e_i также корни $h(x)$ ЧТД

Вероятностный алгоритм нахождения корней.
Вход: простое число p и многочлен $f(x)$
Выход: Корень многочлена $f(x)$

1. Находим многочлен $h(x) = \text{\textit{НОД}}(x^p - x, f(x))$
2. Берём случайное $c \in \mathbb{F}_p$
   Если $h(c) \equiv 0 (mod\, p)$, то возвращаем c - искомый корень
   Иначе считаем $d(x) = \text{\textit{НОД}}(h(x), v(x)),\ v(x) = (x-c)^{\frac{p-1}{2}} - 1$
   И определяем $h(x)$ равным $d(x)$.
3. Если $deg\, h(x) = 1 \Rightarrow h(x) = ax + b \Rightarrow e \equiv -\frac{b}{a} (mod\, p)$
   Иначе возвращаемся на шаг 2.

25. Двоичный алгоритм возведения в степень и области его применения.

Двоичный алгоритм возведения в степень.

Любое натуральное число n можно перевести в двоичную систему счисления и представить в виде
$n = \overline{(m_k m_{k-1} \ldots m_1 m_0)}_2 = \sum\limits_{i=0}^{k}(m_i \cdot 2^i) = ((\ldots((m_k 2 + m_{k-1})2 + m_{k-2})2 + \ldots)2 + m_1)2 + m_0$
Тогда $x^n = x^{((\ldots((m_k 2 + m_{k-1})2 + m_{k-2})2 + \ldots)2 + m_1)2 + m_0} = ((\ldots((x^{m_k})^2 \cdot x^{m_{k-1}})^2 \cdot \ldots)^2 \cdot x^{m_1})^2 \cdot x^{m_0}$

Алгоритм.
Вход: $x, n \in \mathbb{N}$
Выход: x^n

1. Находим двоичное представление числа n.
   $n = \overline{(m_k m_{k-1} \ldots m_1 m_0)}_2 = \sum\limits_{i=0}^{k}(m_i \cdot 2^i)$
2. Берём $d = x$, $i = k - 1$
3. Если $m_i = 1$ то d возводим в квадрат и умножаем на x.
   Иначе d просто возводим в квадрат.
4. Если $i > 0$ уменьшаем i на 1 и возвращаемся к шагу 3.
   Иначе возвращаем d.

Алгоритм быстрого возведения в степень получил широкое распространение в криптографических системах. В частности, алгоритм применяется в протоколе RSA, схеме Эль-Гамля и других криптографических алгоритмах.

26. Понятия показателя и первообразного корня. Их свойства.

Определение. Пусть a, m - положительные взаимно-простые целые числа.
Показателем числа a по модулю m называется минимальное натуральное t, такое что $a^t \equiv 1 (mod\, m)$
Обозначение $ord_m a$.

$$ord_m a = min\{t \in \mathbb{N} : a^t \equiv 1 (mod\, m)\}$$

Из теоремы Эйлера следует, что показатель всегда существует.
Лемма(Свойства показателя). $НОД(a, m) = 1,\ t = ord_m a$

1. Числа $a^1, a^2, \ldots, a^t$ попарно не сравнимы между собой.
2. Если $a^k \equiv a^l (mod\, m)$, то $k \equiv l (mod\, t)$
3. Если $a^s \equiv 1 (mod\, m)$, то $t|s$, в частности $t|\varphi(m)$
   Доказательство.
4. Пусть существуют $i, j, 1 \le i < j \le t$ такие, что $a^j \equiv a^i (mod\, m)$
   $a^j \equiv a^i (mod\, m) \Rightarrow a^{j-i} \equiv 1 (mod\, m)\ \ (1)$
   $j - i < t\ \ (2)$
   Из (1) и (2) следует, что t - не показатель, что противоречит условиям.
   Следовательно не существует таких $i, j, 1 \le i < j \le t$, что $a^j \equiv a^i (mod\, m)$ ЧТД
5. Пусть $a^k \equiv a^l (mod\, m)$ и пусть $l > k$
   $1 \equiv a^{l-k} (mod\, m)$
   $l - k = qt + r,\ \ 0 \le r < t$
   $1 \equiv a^{l-k} \equiv a^{qt+r} \equiv a^r (a^t)^q \equiv a^r\ (mod\, m) \Rightarrow r = 0 \Rightarrow l - k = qt \Rightarrow l \equiv k (mod\, t)$ ЧТД
6. $a^s \equiv 1 \equiv a^0 (mod\, m)$ из второго следует, что $s \equiv 0\ (mod\, t) \Rightarrow t|s$ ЧТД
   Определение. a - первообразный корень, если $ord_m a = \varphi(m)$.
   Лемма(Свойства показателя по простому модулю). Пусть a,b - целые числа, p - простое.
7. Если $ord_p a = xy$, то $ord_p a^x = y$.
8. Если $ord_p a = x,\ ord_p b = y$ и $НОД(x, y) = 1$, то $ord_p (ab) = xy$.
   Доказательство.
9. Обозначим
   $ord_p a^x = t \Rightarrow (a^x)^t \equiv 1 (mod\, p) \Rightarrow a^{xt} \equiv 1 (mod\, p) \Rightarrow ord_p a | xt \Rightarrow xy | xt \Rightarrow y | t$
   $ord_p a = xy \Rightarrow a^{xy} \equiv 1 (mod\, p) \Rightarrow (a^x)^y \equiv 1 (mod\, p) \Rightarrow ord_p a^x | y \Rightarrow t | y$
   Так как $t|y$ и $y|t$, следовательно $y = t$.
10. Обозначим $ord_p ab = t \Rightarrow (ab)^t \equiv 1 (mod\, p)$
    $$\begin{matrix} a^x \equiv 1 (mod\, p) \Rightarrow (a^x)^y \equiv 1 (mod\, p) \\ b^y \equiv 1 (mod\, p) \Rightarrow (b^y)^x \equiv 1 (mod\, p) \end{matrix} \Rightarrow (ab)^{xy} \equiv 1 (mod\, p) \Rightarrow t | xy$$

$(ab)^t \equiv 1(mod\, p) \Rightarrow (ab)^{tx} \equiv 1(mod\, p) \Rightarrow a^{tx}b^{tx} \equiv 1(mod\, p) \Rightarrow$
$\Rightarrow b^{tx} \equiv 1(mod\, p) \Rightarrow y|tx \Rightarrow \exists c : yc = tx$
Так как $НОД(y, x) = 1 \Rightarrow y|t$
$(ab)^t \equiv 1(mod\, p) \Rightarrow (ab)^{ty} \equiv 1(mod\, p) \Rightarrow a^{ty}b^{ty} \equiv 1(mod\, p) \Rightarrow$
$\Rightarrow a^{ty} \equiv 1(mod\, p) \Rightarrow x|ty \Rightarrow \exists k : xk = ty$
Так как $НОД(y, x) = 1 \Rightarrow x|t$

$$\begin{matrix} x|t \\ y|t \\ НОД(x,y) = 1 \end{matrix} \Rightarrow xy|t$$

Так как $xy|t$ и $t|xy$, то $xy = t$ ЧТД

27. Теорема о существовании первообразного корня по простому модулю.

Определение. Пусть $t_1, \ldots t_n$ - натуральные. Наименьшим общим кратным называется натуральное число k такое, что $t_i|k, \ \forall i = 1, \ldots, n$.

$$НОК(t_1, \ldots, t_n) = min\{k \in \mathbb{N} : t_i|k \ \forall i = 1, 2, \ldots, n\}$$

Лемма(свойства НОК). $НОК(t_1, \ldots, t_n) = k$

1. Если $\exists m : t_i|m \ \forall i = 1, \ldots, n$, то $k|m$. Те НОК делит ОК
2. $НОК(t_1, \ldots, t_n) = p_1^{\alpha_1} \cdot \ldots \cdot p_m^{\alpha_m}$, p_i - простое, α_i - натуральное. Тогда $\exists i, j : p_i^{\alpha_1}|t_j$ в точности, то есть $p_i^{\alpha_i+1} \not| \ t_j$
3. Если $НОД(t_i, t_j) = 1 \ \forall i, j \Rightarrow НОК(t_1, \ldots, t_n) = \prod_{i=1}^{n} t_i$

   Доказательство.
4. $k - НОК$, m - общее кратное(ОК).
   $m = qk + r \Rightarrow r = m - qk$

$$\begin{matrix} t_i|m \\ t_i|k \end{matrix} \Rightarrow t_i|m - qk = r \Rightarrow r - OK$$

   Так как r - остаток, $0 \leq r \leq k$, так как $k - НОК$, то $r = 0 \Rightarrow k|m$ ЧТД
5. $t_1 = p_{i_1}^{\alpha_{i_1}} \cdot \ldots \cdot p_{i_{s_1}}^{\alpha_{i_{s_1}}} \Rightarrow p_{i_1}^{\alpha_{i_1}}|t_1|k$

$$\left.\begin{matrix} p_{i_1}^{\alpha_{i_1}}|k \\ t_2 = p_{i_1}^{\beta_{i_1}} \cdot \ldots \Rightarrow p_{i_1}^{\beta_{i_1}}|k \\ \vdots \\ t_n = p_{i_1}^{\gamma_{i_1}} \cdot \ldots \Rightarrow p_{i_1}^{\gamma_{i_1}}|k \end{matrix}\right\} \Rightarrow p_{i_1}^{c}|k, \ c = max\{\alpha_{i_1}, \beta_{i_1}, \ldots, \gamma_{i_1}\}$$

   Таким образом $p_{i_1}^c$ будет в разложении k и так как $c = max\{\alpha_{i_1}, \beta_{i_1}, \ldots, \gamma_{i_1}\}$, то существует $t_j : p_{i_1}^c|t_j$ и $p_{i_1}^{c+1} \not| t_j$ ЧТД
6. Следует из 2-ого. Так как $t_1, \ldots, t_n$ - взаимно-простые, то в их разложении нет одинаковых простых $p_i^{\alpha_i}$, а так как $НОК$ должен делиться на все t_j, то он должен

делиться и на все отличные друг от друга $p_i^{\alpha_i}$ из чего вытекает нужное утверждение леммы. ЧТД

Теорема. Пусть p - нечётное простое, тогда найдётся целое a, $НОД(a,p)=1$, являющееся первообразным корнем по модулю p, то есть $ord_p a=\varphi(p)=p-1$.

Доказательство.

7. Построение.
   $a:1,2,\ldots,p-1$
   $t_i=ord_p i,\ i=1,2,\ldots,p-1$
   Определим $\tau=НОК(t_1,\ldots,t_{p-1})=p_1^{\alpha_1}\cdot\ldots\cdot p_k^{\alpha_k}$
   По второму свойству НОК существует $i_1: p_1^{\alpha_1}|t_{i_1},\ p_1^{\alpha_1+1}\not|\ t_{i_1}$
   Так как мы определили $t_i=ord_p i$, то $ord_p i_1=t_{i_1}=p_1^{\alpha_1}s_1$
   По свойству показателя по простому модулю $ord_p i_1^{s_1}=p_1^{\alpha_1}$
   Пусть $b_1\equiv i_1^{s_1}\ (mod\, p)$, тогда $ord_p b_1=ord_p i_1^{s_1}=p_1^{\alpha_1}$
   Аналогично получаем $b_2,\ldots,b_k$.

$$\left.\begin{matrix} ord_p b_1=p_1^{\alpha_1} \\ ord_p b_2=p_2^{\alpha_2} \\ \vdots \\ ord_p b_k=p_k^{\alpha_k}\end{matrix}\right\}\xRightarrow{По\ св-ву\ ord_p a} ord_p b=p_1^{\alpha_1}\cdot\ldots\cdot p_k^{\alpha_k}=\tau, b\equiv b_1\cdot\ldots\cdot b_k(mod\, p)$$

8. Равенство $\tau=\varphi(p)=p-1$
   1. По малой теореме Ферма $b^{p-1}\equiv 1(mod\, p)$

$$\left.\begin{matrix} b^{p-1}\equiv 1(mod\, p) \\ ord_p b=\tau\end{matrix}\right\}\xRightarrow{По\ св-ву\ ord_m a}\tau|(p-1)=\varphi(p)$$

   $\tau|(p-1)\Rightarrow\tau\le(p-1)$
   2. Обозначим $f(x)=x^\tau-1$
   Все значения $e=1,\ldots,p-1$ являются корнями $f(x)$, так как
   $e^{t_e}\equiv 1(mod\, p)$ Возведём левую и правую часть в степень $\frac{\tau}{t_e}$, это можно сделать, так как $\frac{\tau}{t_e}$ - целое. Получим

$$e^\tau\equiv 1(mod\, p)\Rightarrow e^\tau-1\equiv 0(mod\, p)$$

   Следовательно e - корень $f(x)$
   Так как $1,\ldots,p-1$ - корни, то $f(x)=(x-1)(x-2)\cdot\ldots\cdot(x-(p-1))f_1(x)$
   Следовательно $p-1\le\tau$, но так как $p-1\le\tau$, $\tau=p-1$
   Таким образом существует число $b: ord_p b=p-1=\varphi(p)$. ЧТД

28. Схема Диффи-Хеллмана выработки общего ключа и ее связь с первообразными корнями.

Перед описанием алгоритма введём несколько важных требований.
p - простое число, a - первообразный корень по модулю p $(ord_p a=p-1)$
$Z_p^*=\{a^k,k=1,\ldots,p-1\}$ - циклическая группа. Группа степеней a по модулю p.

Схема Диффи-Хеллмана.

Есть два абонента, которые хотят выработать общий ключ шифрования k.
Первый абонент выбирает случайный $k_1 \in \{1, \ldots, p-1\}$ и отправляет второму абоненту вычет $a^{k_1}(mod\, p)$. Второй абонент таким же образом выбирает k_2 и отправляет первому абоненту $a^{k_2}(mod\, p)$.

После того, как оба абонента получили вычеты друг от друга, они выбирают ключ по формуле

$$k \equiv (a^{k_1})^{k_2} \equiv (a^{k_2})^{k_1} \equiv a^{k_1 k_2}(mod\, p)$$

Злоумышленник, у которого есть возможность прослеживать канал связи, знает только вычеты $b_1 \equiv a^{k_1}(mod\, p)$ и $b_2 \equiv a^{k_2}(mod\, p)$, самих значений k_1, k_2 он не знает.

Что известно злоумышленнику: a, b_i, p
Нужно найти: k_i
Можно заметить, что $k_i \equiv \log_a b_i(mod\, p)$. То есть чтобы узнать k_i, нам будет необходимо решить задачу дискретного логарифмирования. Пример решения этой задачи - метод согласования - рассмотрен в следующем билете.

29. Метод согласования для решения задачи дискретного логарифмирования.

Для начала введём несколько определений, чтобы понять, для чего нам нужен метод согласования. Введём понятие дискретного логарифмирования

Пусть p - простое, a - первообразный корень по модулю p, те $ord_p a = p - 1 = m$.

Пусть задан вычет b, удовлетворяющий условию $a^x \equiv b(mod\, p)$

Задача **дискретного логарифмирования** заключается в том, чтобы найти этот $x(mod\, m)$.

Найденный x будет называться **дискретным логарифмом** b по основанию a и обозначается $x \equiv \log_a b(mod\, m)$

Из этого определения и свойств первообразных корней следует, что сравнение разрешимо только в том случае, когда $b \in A = \{a^0, a^1, a^2, \ldots, a^m\} \subset \mathbb{F}_p^*$, те b является элементом циклической группы, порождённой вычетом a. В таком случае вычет b принадлежит множеству всех возможных степеней вычета a по модулю p.

Также введём и докажем вспомогательную лемму.

Лемма. Пусть p - простое, a - первообразный корень по модулю p, $ord_p a = p - 1 = m$.
Пусть задан вычет b из множества A. Тогда выполнены следующие утверждения

1. $\log_a a \equiv 1(mod\, m)$

2. Если для b выполняется сравнение $b \equiv b_1^{\alpha_1} \cdot \ldots \cdot b_n^{\alpha_n} (mod\, p)$, где $\alpha_i \in \mathbb{N}, b_i \in A$. Тогда выполняется $\log_a b \equiv \alpha_1 log_a b_1 + \ldots + \alpha_n log_a b_n (m)$
3. $\log_a b^n \equiv n \log_a b (mod\, p)$
4. Пусть для $b, c, d \in A$ выполнено $d \equiv \frac{b}{c} (mod\, p)$. Тогда $\log_a d \equiv \log_a b - \log_a c (mod\, m)$
   Доказательство
5. $a^1 \equiv a (mod\, p) \Rightarrow \log_a a \equiv 1 (mod\, p)$
6. Рассмотрим случай $b \equiv b_1 b_2 (mod\, p)$. Поскольку $b_i \in A$ то найдутся такие x, y, что

$$a^x \equiv b_1 (mod\, p) \text{ и } a^y \equiv b_2 (mod\, p)$$
$$\text{или}$$
$$x \equiv \log_a b_1 (mod\, m) \text{ и } y \equiv \log_a b_2 (mod\, m)$$

Тогда получаем $b \equiv b_1 b_2 \equiv a^x a^y \equiv a^{x+y} (mod\, p)$ и выполняется

$$\log_a b \equiv \log_a b_1 b_2 \equiv x + y \equiv \log_a b_1 + \log_a b_2 (mod\, p)$$

Обобщая это сравнение на случай $b = b_1^{\alpha_1} \cdot \ldots \cdot b_n^{\alpha_1} (mod\, p)$ получаем второе утверждение леммы.
Стоит учитывать, что a обязан быть первообразным корнем, а $b \in A$. Если требование не удовлетворяется, то возникает противоречие лемме.
Пример.
Рассмотрим уравнение

$$27^x \equiv 520 (mod\, 547)$$

Заметим, что $ord_{547} 27 = 14$, то есть, вычет 27 не является первообразным корнем по модулю 547 и порождает группу $A =< 27 >$.
С другой стороны, выполнено равенство $520 = 2^3 \cdot 5 \cdot 13$. Применяя для нахождения неизвестного x утверждение леммы, мы должны записать сравнение

$$\log_{27} 520 \equiv 3 \log_{27} 2 + \log_{27} 5 + \log_{27} 13 \ \ (mod\, 14)$$

Поскольку 2, 5, 13 не принадлежат A, то логарифмы из правой части не существуют следовательно правая часть сравнения не существует, таким образом получено противоречие с леммой.
Метод согласования
Пусть p - простое, a - первообразный корень по модулю p, те $ord_p a = p - 1 = m$, $b \in A$
Рассмотрим сравнение $a^x \equiv b (mod\, p)$
Если $b \equiv 1 (mod\, p)$, то, очевидно выполнено $x \equiv b (mod\, m)$. Задана решена
В остальных случаях ищем $h = \lceil \sqrt{m} \rceil$. Поскольку мы ищем $0 < x < m$, мы также можем воспользоваться операцией деления с остатком и найти такие u, v, что

$$x = hu + v, \ 0 \leq u < h, \ 0 \leq v < h$$

Тогда подставляем и получаем сравнение

$$b \equiv a^x \equiv a^{hu+v} \equiv (a^h)^u a^v$$
$$(a^h)^u \equiv ba^{-v} (mod\, p)$$

Поиск x осуществляется следующим образом:

7. Перебираем u от 0 до $h-1$, узнаём значения $(a^h)^u$, так как h нам известно, и записываем их в памяти
8. Перебираем v от 0 до $h-1$, узнаем значения ba^{-v}, так как b нам известно. Если мы находим значение, сравнимое по модулю p с одним из тех, что были найдены в пункте 1, берем соответствующие значения u, v и вычисляем $x = hu + v$. Заканчиваем просчёт. Задача выполнена.

30. Понятие систематической дроби. Периодичность систематической дроби.

Определение. $b \in \mathbb{N}, b > 1$. **Систематической дробью** α называется ряд

$\alpha = \sum\limits_{k=0}^{\infty} a_k b^{-k} = a_0 + \frac{a_1}{b} + \frac{a_2}{b^2} + \ldots$

где $a_0 \in \mathbb{Z}, a_1, a_2, \ldots \in \mathbb{Z}$ и $0 \le a_n < b$ для $n = 1, 2, \ldots$

$a_0, a_1 a_2 a_3 a_4 a_5 \ldots_b$ - форма записи систематической дроби, число b системой счисления систематической дроби.

$S_n = \sum\limits_{k=0}^{n} a_k b^{-k}$ - **частичная сумма** систематической дроби.

Систематическая дробь **конечна**, если найдётся индекс $n_0 \in \mathbb{N} : \forall n \ge n_0\ a_n = 0$. Это условие равносильно тому, что $S_n = S_{n_0}, n \ge n_0$

Систематическая дробь **периодична**, если найдётся индекс $\lambda \in \mathbb{N}$ и натуральное $\tau \ge 1$ такие, что для всех индексов $n \ge \lambda$ выполнено равенство

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

τ - период, λ - длинна подхода к периоду

Лемма. $\sum\limits_{n=0}^{\infty} b^{-n} = \frac{b}{b-1}$

1. $S_k = \sum\limits_{n=0}^{k} a_n b^{-n}$, пусть все $a_n = 1$, $q = \frac{1}{b}$ тогда

$$S_k = \sum_{n=0}^{k} b^{-n} = (1 + q + q^2 + \ldots + q^k) = \frac{(1 + q + q^2 + \ldots + q^k)(1-q)}{1-q} =$$

$$= \frac{1 + q + q^2 + \ldots + q^k - q - q^2 - \ldots - q^{k+1}}{1-q} = \frac{1 - q^{k+1}}{1-q}$$

2. $0 < q < 1 \Rightarrow 1 - q > 0$

$$\frac{b}{b-1} = \frac{1}{1-q}$$

$$|S_k - \frac{1}{1-q}| = |\frac{1-q^{k+1}-1}{1-q}| = \frac{q^{k+1}}{1-q} < \varepsilon = \frac{u}{v}$$

$$\frac{q^{k+1}}{1-q} = \frac{b^{-(k+1)}}{1-\frac{1}{b}} = \frac{b^{-(k+1)}}{\frac{b-1}{b}} = \frac{b}{b^{k+1}(b-1)} < \frac{u}{v} bv < u(b-1)b^{k+1}v < u(b-1)b^k$$

Представим v в системе счисления по основанию b и запишем.
$v = v_0 + v_1 b + v_2 b^2 + \ldots + v_{s-1} b^{s-1}$ для некоторых $v_0, \ldots, v_{s-1} \in \mathbb{N}_0$. Тогда $v < b^s$
Получим $v < b^s < u(b-1)b^s$

$$\frac{1}{b^s(b-1)} < \frac{u}{v} = \varepsilon$$

Таким образом $\forall \varepsilon \ \exists k : \frac{1}{b^s(b-1)} < \varepsilon$, означает, что $\lim\limits_{k\to\infty} S_k = \lim\limits_{k\to\infty} \sum\limits_{n=0}^{k} b^{-n} = \frac{b}{b-1}$. Из чего вытекает утверждение данной леммы.
Теорема. Последовательность S_k сходится к некоторому пределу и этот предел равен $\alpha \lim\limits_{n\to\infty} S_n = \alpha$

Доказательство теоремы.

Надо доказать, что $\forall \varepsilon \ \exists k : |S_k - \alpha| < \varepsilon$

$$|S_k - \alpha| = |\alpha - S_k| = |\sum_{n=0}^{\infty} a_n b^{-n} - \sum_{n=0}^{k} a_n b^{-n}| =$$
$$= |-a_0 b^0 - a_1 b^{-1} - \ldots - a_{k-1} b^{-(k-1)} - a_k b^{-k} + a_0 b^0 + a_1 b^{-1} + \ldots + a_k b^{-k} + a_{k+1} b^{-(k+1)} + \ldots| =$$
$$= |a_{k+1} b^{-(k+1)} + a_{k+2} b^{-(k+2)} + \ldots| =$$
$$= b^{-(k+1)} |a_{k+1} b^0 + a_{k+2} b^{-1} + \ldots| = b^{-(k+1)} |\sum_{n=0}^{\infty} a_{n+k+1} b^{-n}| < b^{-(k+1)} |\sum_{n=0}^{\infty} b^{-n}| =$$
$$= \frac{b}{b^{k+1}(b-1)} = \frac{1}{b^k(b-1)} < \varepsilon$$

В доказательстве леммы выше мы уже доказали, что $\forall \varepsilon$ найдётся такое k, что $\frac{1}{b^k(b-1)} < \varepsilon$.
Следовательно $\lim\limits_{n\to\infty} S_n = \alpha$ ЧТД
Теорема. Пусть α - вещественное число, его систематическая дробь конечна или периодична тогда и только тогда, когда α - рациональное.

Доказательство.
Любая конечная систематическая дробь - периодическая, так как в конечной дроби после какого-то a_n все $a_i = 0, i \geq n$, таким образом для любого $i > n$ будет выполнено, что $a_i = a_{i+1} = 0$.
$\Rightarrow$

Нам надо доказать, что если дробь периодична, то α - рациональное.
$\alpha = \sum\limits_{k=0}^{\infty} a_n b^{-n}$ - периодическая систематическая дробь.

$\exists \lambda, \tau :\ a_{n+\tau} = a_n, \forall n > \lambda$

Тогда $\alpha = a_0 + a_1 b^{-1} + a_2 b^{-2} + \ldots + a_\lambda b^{-\lambda} + \sum\limits_{n=\lambda+1}^{\infty} a_n b^{-n}$

$a_0 + a_1 b^{-1} + a_2 b^{-2} + \ldots + a_\lambda b^{-\lambda} = a_0 + \frac{a_1}{b} + \frac{a_2}{b^2} + \ldots + \frac{a_\lambda}{b^{-\lambda}} = \alpha_1 \in \mathbb{Q}$

$\sum\limits_{n=\lambda+1}^{\infty} a_n b^{-n} = b^{-\lambda} \sum\limits_{n=1}^{\infty} a_{n+\lambda} b^{-n} = b^{-\lambda} \alpha_2$

$\alpha_2 = \sum\limits_{n=1}^{\infty} a_{n+\lambda} b^{-n} = \sum\limits_{n=1}^{\infty} c_n b^{-n}$

$c_1, \ldots, c_\tau$ - они периодичны.

$$\frac{c_1}{b} + \frac{c_2}{b^2} + \ldots + \frac{c_\tau}{b^\tau} = \frac{1}{b^\tau}(c_1 b^{\tau-1} + c_2 b^{\tau-2} + \ldots + c_\tau) = \frac{A}{b^\tau}$$

$$\frac{c_{\tau+1}}{b^{\tau+1}} + \frac{c_{\tau+2}}{b^{\tau+2}} + \ldots + \frac{c_{2\tau}}{b^{2\tau}} = \frac{1}{b^\tau}(\frac{c_1}{b} + \frac{c_2}{b^2} + \ldots + \frac{c_\tau}{b^\tau}) = \frac{A}{b^{2\tau}}$$

Таким образом

$$\alpha_2 = \tfrac{A}{b^\tau} + \tfrac{A}{b^{2\tau}} + \tfrac{A}{b^{3\tau}} + \ldots = A \sum\limits_{n=1}^{\infty} b^{-n\tau} = A \sum\limits_{n=0}^{\infty} b^{-(n-1)\tau} =$$
$$= A \sum\limits_{n=0}^{\infty} b^{-n\tau} b^\tau = A b^\tau \sum\limits_{n=0}^{\infty} b^{-n\tau} = A b^\tau \sum\limits_{n=0}^{\infty} (b^\tau)^{-n}$$

По лемме доказанной выше

$$\alpha_2 = A b^\tau \sum_{n=0}^{\infty} (b^\tau)^{-n} = A b^\tau \frac{b^\tau}{b^\tau - 1} \in \mathbb{Q}$$

Так как α_1 - рациональное, α_2 - рациональное, так как поле $\mathbb{Q}$ замкнуто, то и
$\alpha = \alpha_1 + \alpha_2 \in \mathbb{Q}$

$\Leftarrow$
Нам надо доказать, что, если α - рациональное, то её систематическая дробь периодична.
$\alpha = \frac{r}{q},\ \text{НОД}(r, q) = 1$
Для доказательства нам достаточно в явном виде предъявить систематическую дробь для $\frac{r}{q}$.
$r = a_0 q + p,\ 0 \le p < q$

$\alpha = \frac{a_0 q + p}{q} = a_0 + \frac{p}{q}\ \ (1)$
Определим $\text{НОД}(q, b) = d$. Если $d > 1$ определим m_q - натуральное число, как

максимальную степень в которой число d входит в q, те $d^{m_q}|q$, но $d^{m_q+1}\not| \ q$, иначе если $d=1$, то $m_q=0$. Аналогично определяем m_b.

Тогда $q=d^{m_q}q_1,\ b=d^{m_b}b_1,\ НОД(q,q_1)=НОД(b,b_1)=НОД(b_1,q_1)=1$.

Поделим m_q с остатком на m_b. $m_q=sm_b+g,\ 0\le g<m_b$

$$q=d^{m_q}q_1=d^{sm_b+g}q_1=d^g\cdot(d^{m_b})^sq_1=d^g(\frac{b}{b_1})^sq_1$$

$$\frac{p}{q}=\frac{pb_1^s}{d^gb^sq_1}=\frac{1}{b^s}\cdot\frac{pb_1^s}{d^gq_1}=\frac{1}{b^s}(c_0+\frac{p_1'}{q_1'})$$

где $pb_1^s=c_0(d^gq_1)+p_1',\ 0\le p_1'<d^gq_1,\ d^gq_1=q_1'$

Таким образом любое α можно представить в виде

$$\alpha=a_0+\frac{1}{b^s}(c_0+\frac{p_1'}{q_1'})$$

Поскольку $p<q$, то $c_0<b^s$, следовательно представив c_0 в системе счисления b имеем

$$c_0=a_s+a_{s-1}b+\ldots+a_1b^{s-1}\ \ (2)$$

Тогда

$$\frac{p}{q}=\frac{1}{b^s}(c_0+\frac{p_1'}{q_1'})=a_1b^{-1}+a_2b^{-2}+\ldots+a_sb^{-s}+\frac{1}{b^s}\frac{p_1'}{q_1'}$$

Обозначим $t=ord_{q_1'}b\Rightarrow b^t\equiv1(mod\ q_1')\Rightarrow b^t=1+zq_1'\Rightarrow b^t-1=zq_1'$

$$\frac{p_1'}{q_1'}=\frac{zp_1'}{zq_1'}=\frac{zp_1'}{b^t-1}=zp_1'\sum_{n=1}^{\infty}b^{-nt}$$

$$zp_1'=c_1+c_2b^1+\ldots+c_\tau b^{\tau-1}\ \ (3),\ \ zp_1'<zq_1'=b^t-1<b^t\Rightarrow\tau=t$$

Обозначим $c_1=a_{s+\tau},\ldots,c_\tau=a_{s+1}\ \ (3.1)$

$$\tfrac{p_1'}{q_1'}=(a_{s+\tau}+a_{s+\tau-1}b^1+\ldots+a_{s+1}b^{\tau-1})\sum_{n=1}^{\infty}b^{-n\tau}=$$

$$=a_{s+1}b^{-1}+\ldots+a_{s+\tau}b^{-\tau}+a_{s+1}b^{-\tau-1}+\ldots+a_{s+\tau}b^{-2\tau}+\ldots=b^s\sum_{n=s+1}^{\infty a_nb^{-n}}$$

те дробь $\frac{p_1'}{q_1'}$ можно представить в виде периодической систематической дроби с периодом τ $a_{s+1},\ldots,a_{s+\tau}$.
Теперь запишем окончательное равенство.

$$\frac{r}{q}=a_0+\frac{p}{q}=a_0+a_1b^{-1}+a_2b^{-2}+\ldots+a_sb^{-s}+\frac{1}{b^s}\frac{p_1'}{q_1'}=a_0+\sum_{n=1}^{s}a_nb^{-n}+\sum_{n=s+1}^{\infty}a_nb^{-n}=\sum_{n=0}^{\infty}a_nb^{-n}$$

Таким образом рациональное α представляется в виде периодической систематической дроби $\alpha=a_0,a_1\ldots a_s(a_{s+1}\ldots a_{s+\tau})_b$, где коэффициент a_0 определён равенством (1), коэффициенты $a_1, \ldots, a_s$ определены равенством (2), а коэффициенты $a_{s+1}, \ldots, a_{s+\tau}$ определены равенством (3) и определением (3.1).

Теорема доказана в обе стороны, следовательно систематическая дробь числа α периодична или конечна тогда и только тогда, когда α - рациональное. ЧТД

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

Введём несколько определений.
$\alpha_0 \in \mathbb{R}, \alpha_0 > 0$
$a_n = \lfloor \alpha_n \rfloor$ - целая часть от $\alpha_n \Rightarrow a_n \leq \alpha_n$, a_n - неполное частное, α_n - полное частное.
Определим последовательность действительных чисел $\alpha_1, \alpha_2, \ldots$ следующим рекуррентным соотношением.

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n} \ \ (1)$$

Причём, если $\alpha_n = a_n$, то последовательность обрывается.
Перепишем соотношение (1) в виде

$$\alpha_n = a_n + \frac{1}{\alpha_n}$$

Тогда можно выразить изначальное значение α_0 в виде

$$\alpha_0 = a_0 + \frac{1}{\alpha_1} = a_0 + \frac{1}{a_1 + \frac{1}{\alpha_2}} = \ldots = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\cdots + \frac{1}{\alpha_n}}}}$$

Для произвольного индекса n.

Для упрощённой записи данного выражения используется обозначение $[a_0, a_1, \ldots, a_{n-1}, \alpha_n]$. Такое представление числа α_0 называется **непрерывной или цепной дробью** числа α_0.

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

$$\frac{P_n}{Q_n} = a_0 + \frac{1}{a_1 + \frac{1}{\cdots + \frac{1}{a_n}}} = [a_0, a_1, \ldots, a_n]$$

(ВАЖНО a_n, а не α_n)
Такая дробь называется **подходящей дробью** к числу α_0

Лемма 1.

Пусть $\alpha_0 \neq 0$ - действительное число. Тогда для P_n и Q_n - числителя и знаменателя подходящих дробей числа α_0 выполнены следующие рекуррентные соотношения:

$$P_{-1} = 1,\ Q_{-1} = 0,\ P_0 = a_0,\ Q_0 = 1 P_{n+1} = a_{n+1}P_n + P_{n-1} Q_{n+1} = a_{n+1}Q_n + Q_{n-1}$$

Доказательство. По математической индукции.
База индукции.

$$\frac{P_1}{Q_1} = a_0 + \frac{1}{a_1} = \frac{a_1 a_0 + 1}{a_1} = \frac{a_1 P_0 + P_{-1}}{a_1 Q_0 + Q_{-1}}$$

Предположим, что лемма справедлива для всех индексов, меньших или равных n.
Тогда выполняется равенство

$$\frac{P_n}{Q_n} = [a_0, a_1, a_2, \ldots, a_{n-1}, a_n] = \frac{a_n P_{n-1} + P_{n-2}}{a_n Q_{n-1} + Q_{n-2}}$$

Рассмотрим $\frac{P_{n+1}}{Q_{n+1}}$

$$\begin{gathered}\tfrac{P_{n+1}}{Q_{n+1}} = [a_0, a_1, \ldots, a_{n-1}, a_n, a_{n+1}] = [a_0, a_1, \ldots, a_{n-1}, a_n + \tfrac{1}{a_{n+1}}] = \\ = \tfrac{(a_n + \frac{1}{a_{n+1}})P_{n-1} + P_{n-2}}{(a_n + \frac{1}{a_{n+1}})Q_{n-1} + Q_{n-2}} = \tfrac{a_n a_{n+1} P_{n-1} + P_{n-1} + a_{n+1} P_{n-2}}{a_n a_{n+1} Q_{n-1} + Q_{n-1} + a_{n+1} Q_{n-2}} = \\ = \tfrac{a_{n+1}(a_n P_{n-1} + P_{n-2}) + P_{n-1}}{a_{n+1}(a_n Q_{n-1} + Q_{n-2}) + Q_{n-1}} = \tfrac{a_{n-1} P_n + P_{n-1}}{a_{n-1} Q_n + Q_{n-1}}\end{gathered}$$

Для $n+1$ выполнено, следовательно выполнено и для всех индексов больших n.
Таким образом лемма доказана.

Лемма 2. Для всех индексов $n = 0, 1, \ldots$ выполнено $P_{n+1}Q_n - Q_{n+1}P_n = (-1)^n$
Доказательство.

$$\begin{gathered}P_{n+1}Q_n - Q_{n+1}P_n = (a_{n+1}P_n + P_{n-1})Q_n - (a_{n+1}Q_n + Q_{n-1})P_n = \\ = a_{n+1}P_n Q_n + P_{n-1}Q_n - a_{n+1}Q_n P_n - Q_{n-1}P_n = \\ = P_{n-1}Q_n - Q_{n-1}P_n = (-1)(P_n Q_{n-1} - Q_n P_{n-1}) = \ldots = \\ = (-1)^2(P_{n-1}Q_{n-2} - Q_{n-1}P_{n-2}) = \ldots = (-1)^n(P_1 Q_0 - Q_1 P_0) = \ldots = \\ = (-1)^n(P_1 - Q_1 a_0) = (-1)^n(a_1 a_0 + 1 - a_1 a_0) = (-1)^n\end{gathered}$$

ЧТД
Следствие. $\text{НОД}(P_n, Q_n) = 1 \Rightarrow \frac{P_n}{Q_n}$ - несократима.

Лемма 3. Если $\alpha \in \mathbb{Q}$, то цепная дробь конечна и $\exists n : \frac{P_n}{Q_n} = \alpha$
Доказательство. Так как $\alpha \in \mathbb{Q}$, то $\alpha = \frac{u}{v}$ - несократимая дробь, следовательно $\text{НОД}(u, v) = 1$
Применим алгоритм Евклида, чтобы найти остатки от деления для поиска НОД:

$$u = q_1 v + r_1,\ 0 < r_1 < v v = q_2 r_1 + r_2,\ 0 \leq r_2 < r_1 r_1 = q_3 r_2 + r_3,\ 0 \leq r_2 < r_2 \ldots r_{n-1} = q_{n+1} r_n + 0$$

Тогда $\text{НОД}(u, v) = r_n = 1$
Раскрываем α, используя разложения из алгоритма Евклида.

$$\frac{u}{v} = q_1 + \frac{r_1}{v} = q_1 + \frac{1}{\frac{v}{r_1}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_1}{r_2}}} = \ldots = q_1 + \frac{1}{q_2 + \frac{1}{\cdots + q_{n+1}}} = \frac{P_{n+1}}{Q_{n+1}}$$

Таким образом мы получили $\frac{P_{n+1}}{Q_{n+1}} = [q_1, q_2, \dots, q_{n+1}] = \frac{u}{v} = \alpha$ - конечную цепную дробь, и нашли индекс $n+1$ при котором подходящая дробь равна α. ЧТД

32. Теорема о сходимости подходящих дробей.

Теорема. Пусть $\alpha_0 \neq 0$ - действительное число. Тогда последовательность подходящих дробей сходится к α_0, то есть выполняется $\alpha_0 = \lim\limits_{n\to\infty} \frac{P_n}{Q_n}$

Доказательство.

Сначала докажем существование предела, а затем его значение.

1. Существование.
   В начале докажем, что для любого $n = 0, 1, \dots$ следует, что $Q_n > 0$
   Пусть $\alpha_0 > 0$ (если она меньше, то вынесем -1), следовательно $a_0 > 0$
   $\alpha_{n+1} = \frac{1}{\alpha_n - a_n}$, $0 < \alpha_n - a_n < 1 \Rightarrow \frac{1}{\alpha_n - a_n} > 1$
   $a_{n+1} \geq 1 \forall n \geq 0$
   По лемме о рекуррентном соотношении P_n и Q_n получаем
   $Q_{n+1} = a_{n+1}Q_n + Q_{n-1}, Q_{-1} = 0, Q_0 = 1$
   Следовательно, $Q_n > 0 \forall n \geq 0$

   Теперь приступаем к доказательству существования предела.
   Воспользуемся критерием Коши: последовательность x_n сходится тогда и только тогда, когда $\forall \varepsilon > 0 \, \exists N$ такой, что $\forall n, m > N : |x_n - x_m| < \varepsilon$
   Возьмём индексы $n+1$ и n и докажем, что
   $\forall \varepsilon > 0 \, \exists N$ такой, что $\forall n > N : |\frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n}| < \varepsilon$

   $$|\frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n}| = |\frac{P_{n+1}Q_n - P_nQ_{n+1}}{Q_nQ_{n+1}}| = |\frac{(-1)^n}{Q_nQ_{n+1}}| = \frac{1}{Q_nQ_{n+1}} =$$
   $$= \frac{1}{Q_n(a_{n+1}Q_n + Q_{n-1})} < \frac{1}{a_{n+1}Q_n^2} < \frac{1}{Q_n^2} < \varepsilon$$

   Существование доказано.
2. Значение предела.
   По определению предела, если пределом последовательности подходящих дробей является α_0, то $\forall \varepsilon > 0 \exists N : \forall n > N :$

   $$|\frac{P_n}{Q_n} - \alpha_0| < \varepsilon$$
   $$|\alpha_0 - \frac{P_n}{Q_n}| < \varepsilon \ (1)$$

   Найдём представление α_0.
   Сначала определим
   $\frac{P_{n+1}}{Q_{n+1}} = [a_0, a_1, \dots, a_n, a_{n+1}] = [a_0, a_1, \dots, a_n + \frac{1}{a_{n+1}}] = \frac{(a_n + \frac{1}{a_{n+1}})P_{n-1} + P_{n-2}}{(a_n + \frac{1}{a_{n+1}})Q_{n-1} + Q_{n-2}}$
   Так как α_0 - цепная дробь, в её представлении $\frac{1}{a_{n+1}}$ поменяется на $\frac{1}{\alpha_{n+1}}$. Таким образом,

   $$\alpha_0 = \frac{(a_n + \frac{1}{\alpha_{n+1}})P_{n-1} + P_{n-2}}{(a_n + \frac{1}{\alpha_{n+1}})P_{n-1} + P_{n-2}}$$

Разберём левую часть неравенства (1)

$$|\alpha_0 - \frac{P_n}{Q_n}| = |\frac{(a_n+\frac{1}{\alpha_{n+1}})P_{n-1}+P_{n-2}}{(a_n+\frac{1}{\alpha_{n+1}})P_{n-1}+P_{n-2}} - \frac{P_n}{Q_n}| = |\frac{\alpha_{n+1}P_n+P_{n-1}}{\alpha_{n+1}Q_n+Q_{n-1}} - \frac{P_n}{Q_n}| =$$

$$= |\frac{Q_nP_{n-1}-P_nQ_{n-1}}{Q_n(\alpha_{n+1}Q_n+Q_{n-1})}| = |\frac{(-1)^{n-1}}{Q_n(\alpha_{n+1}Q_n+Q_{n-1})}| = \frac{1}{Q_n(\alpha_{n+1}Q_n+Q_{n-1})} < \varepsilon$$

33* Квадратичные иррациональности. Приведённые квадратичные иррациональности и теорема о периодичности квадратичных иррациональностей.

АААААААААА я не буду это делать.