Занятие 3

Задача 1.

a) *Найти все первообразные корни по модулю 27.*

Заметим, что $\varphi(27) = 27 - 9 = 18 = 2 \cdot 3^2$.

Воспользуемся критерием и проверим, является ли 2 первообразным корнем по модулю 27: $2^6 \equiv 64 \equiv 10 \not\equiv 1(mod\,27)$ и $2^9 \equiv 10 \cdot 8 \equiv 80 \equiv 26 \not\equiv 1(mod\,27)$, то есть 2 - первообразный корень по модулю 27.

Всего существует ровно $\varphi(\varphi(27)) = 6$ первообразных корней по модулю 27 не превосходящих 27. Найдём все такие γ, что $(\gamma, \varphi(27)) = (\gamma, 16) = 1$ и $1 < \gamma \leq 18$. Перебором убеждаемся что $\gamma \in \{5, 7, 11, 13, 17\}$, то есть 2^5, 2^7, 2^{11}, 2^{13} и 2^{17} также первообразные корни. Найдём их состаки по модулю 27 - это 5, 20, 23, 11 и 14 соответственно.

Таким образом $\{2, 5, 11, 14, 20, 23\}$ - множество всех первообразных корней по модулю 27 не превосходящих 27. Тогда множество всех первообразных корней имеет вид $\bigcup\limits_{i=1}^{5} \{g_i + 27k | k \in \mathbb{N}_0\}$, где g_i - первообразные корни найденные ранее.

b) *Найдите показатели, которым принадлежат 5 и 7 по модулю 24.*

Отметим, что $\varphi(24) = 8$.

Пусть δ_1 - показатель которому принадлежит 5 по модулю 24. Тогда δ_1 - делитель 8, то есть $\delta_1 = 2^k$, $k \in \{0, 1, 2, 3\}$. Заметим также, что $k \neq 3$ иначе по модулю 24 существует первообразный корень. Далее несложным перебором убеждаемся, что $k = 1$ и $\delta_1 = 2$.

Пусть δ_2 - показатель которому принадлежит 7 по модулю 24. Аналогичными рассуждениями получаем, что $\delta_2 = 2^k$, $k \in \{0, 1, 2\}$. Далее несложным перебором убеждаемся, что $k = 1$ и $\delta_2 = 2$.

Задача 2.

a) *Найдите все нечётные натуральные n, такие что $n|3^n + 1$.*

Отметим, что $n = 1$ подходит. Рассмотрим $n > 1$. Предположим, что такое существует. Пусть p - минимальный простой делитель n, тогда $p > 3$.

Из того, что $n|3^n + 1$ получаем, что $3^n \equiv -1(mod\,p)$ и $3^{2n} \equiv 1(mod\,p)$. Пусть δ - показатель которому принадлежит 3 по модулю p. Тогда $\delta|2n$. Рассмотрим два случая:

1)δ - нечётное. Тогда $\delta|n$. С другой стороны по малой теореме Ферма $\delta|p - 1$. Тогда найдётся простое q, такое что $1 < q < p - 1$ и такое что $q|\delta$, а значит $q|n$. Получаем противоречие с минимальностью p, так как $q < p$.

2)δ - чётное. Пусть $\delta = 2\widetilde{\delta}$. Аналогично предыдущему случаю получаем, что $\widetilde{\delta}|n$ и $\widetilde{\delta}|p - 1$. Тогда найдётся простое q, такое что $1 < q < p - 1$ и такое что $q|\widetilde{\delta}$ или же $\widetilde{\delta} = 1$. В первом случае получаем противоречие с минимальностью p. Во втором получаем, что $\delta = 2$, то есть $p = 2$, что невозможно.

Задача 2.

a) *Пусть p - простое число. Может ли квадратичный вычет по модулю p быть первообразным корнем по модулю p.*

Пусть a - квадратичный вычет по модулю p.

По критерию Эйлера получаем, что

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

Таким образом, показатель, которому принадлежит a по модулю p не превосходит $\frac{p-1}{2}$, то есть a не является первообразным корнем.

b)*Доказать, что 3 - первообразный корень по модулю простого числа* $2^n + 1$, $n > 1$.

Покажем, что 3 - квадратичный невычет по модулю $2^n + 1$, $n > 1$. Воспользуемся квадратичным законом взаимности:

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

Тогда по критерию Эйлера получаем, что $3^{2^{n-1}} \equiv \left(\frac{2^n+1}{3}\right) \equiv -1(mod\, 2^n + 1)$.

Пусть δ - показатель, которому принадлежит 3 по модулю 2^n+1. Исходя из того, что $2^n + 1$ простое, получаем, что $\varphi(2^n + 1) = 2^n$. Так как $\delta | 2^n$ получаем, что $\delta = 2^k$, $k \in \{1, 2, \ldots, n\}$. Пусть $k < n$, тогда

$$3^{2^{n-1}} \equiv \left(3^{\delta}\right)^{\frac{2^{n-1}}{\delta}} \equiv 1(mod\, 2^n + 1).$$

Получаем противоречие. Значит $k = n$ и 3 - первообразный корень по модулю простого $2^n + 1, n > 1$.

Занятие 4

Задача 1.

а)*Найдите две различные системы индексов 7 по модулю 120.*

Разложим 120 на простые множители: $120 = 2^3 \cdot 3 \cdot 5$.

Заметим, что 2 - первообразный корень по модулю 3 и $\mathrm{ind}_2 7 = 0$, так как $7 \equiv 1(mod\, 3)$.

Найдём два(то есть все) первообразных корня по модулю 5. Нетрудно видеть, что подходят 2 и 3, причём $\mathrm{ind}_2 7 = 1$ и $\mathrm{ind}_3 7 = 2$.

Отметим, что $7 \equiv (-1) \equiv (-1)^1 \cdot 5^0 (mod\, 8)$, то есть получаем систему индексов $(1, 0)$ по модулю 8.

Таким образом получаем следующие две системы индексов 7 по модулю 120: $(0, 1, 1, 0)$ и $(0, 2, 1, 0)$.

б)*Решите сравнение* $3^x \equiv 92(mod\, 143)$.

Разложим 143 на простые множители: $143 = 11 \cdot 13$.

Перейдём от данного сравнения к равносильной системе сравнений:

$$\begin{cases} 3^x \equiv 4(mod\, 11) \\ 3^x \equiv 1(mod\, 13) \end{cases}$$

Решим каждое из сравнений и потом воспользуемся Китайской теоремой об остатках.

Пусть δ_1 - показатель, которому принадлежит 3 по модулю 11. Тогда $\delta_1|10$, то есть $\delta_1 \in \{1,2,5,10\}$. $3^1 \equiv 3(mod\,11)$, $3^2 \equiv 9(mod\,11)$, $3^5 \equiv 27 \cdot 9 \equiv 5 \cdot 9 \equiv 1(mod\,11)$. Таким образом $\delta_1 = 5$. Далее нетрудно видеть, что $4 \equiv 3^4(mod\,11)$, то есть первое сравнение равносильно сравнению $x \equiv 4(mod\,5)$.

Пусть δ_2 - показатель, которому принадлежит 3 по модулю 13. Тогда $\delta_2|12$, то есть $\delta_2 \in \{1,2,3,4,6,12\}$. $3^1 \equiv 3(mod\,13)$, $3^2 \equiv 9(mod\,13)$, $3^3 \equiv 1(mod\,13)$. Таким образом $\delta_2 = 3$, а значит второе сравнение равносильно сравнению $x \equiv 0(mod\,3)$.

Таким образом исходная система равносильна системе

$$\begin{cases} x \equiv 4(mod\,5) \\ x \equiv 0(mod\,3) \end{cases}$$

Тогда в обозначениях Китайской теоремы об остатках получаем $c_1 = 4$, $c_2 = 0$, $m_1 = 5$, $m_2 = 3$, $m = m_1 m_2 = 15$. Тогда

$$x \equiv x_1 c_1 \frac{m}{m_1} + x_2 c_2 \frac{m}{m_2} \equiv 12x_1(mod\,15),$$

где $3x_1 \equiv 1(mod\,5)$, то есть $x_1 \equiv 2(mod\,5)$. Отсюда получаем, что $x \equiv 9(mod\,15)$ и решениями исходного сравнения являются числа вида $9+15k$, $k \in \mathbb{N}_0$.

Задача 2.

а)*Докажите, что 2 - первообразный корень по модулю* 5^n.

Найдём значение функции Эйлера от 5^n: $\varphi(5^n) = 5^n - 5^{n-1} = 4 \cdot 5^n$.

Пусть δ - показатель, которому принадлежит 2 по модулю 5^n. Исходя из того, что $\delta|\varphi(5^n)$ получаем, что $\delta = 4 \cdot 5^k$ либо $\delta = 2 \cdot 5^k$ либо $\delta = 5^k$, где $k \in \{0,1,\ldots,n-1\}$. Предположим, что 2 - не первообразный корень, то есть что $\delta \neq 4 \cdot 5^{n-1}$.

Рассмотрим случай, когда $\delta = 4 \cdot 5^k$, $k \in \{0,1,2,\ldots,n-2\}$. Заметим, что $2^4 = 1 + 3 \cdot 5$, далее будем последовательно возводить обе части этого равенства в 5-тую степень, тем самым получая цепочку верных равенств:

$$2^4 = 1 + 3 \cdot 5,$$

$$2^{4 \cdot 5} = 1 + 3 \cdot 5^2 + 5^3 t_1,$$

$$2^{4 \cdot 5^2} = 1 + 3 \cdot 5^3 + 5^4 t_2,$$

$$\ldots$$

$$2^{4 \cdot 5^i} = 1 + 3 \cdot 5^{i+1} + 5^{i+2} t_i,$$

$$\ldots$$

$$2^{4 \cdot 5^{n-2}} = 1 + 3 \cdot 5^{n-1} + 5^n t_{n-2},$$

$$2^{4 \cdot 5^{n-1}} = 1 + 3 \cdot 5^n + 5^{n+1} t_{n-1} \equiv 1(mod\,5^n).$$

Заметим, что $2^{4 \cdot 5^i} \not\equiv 1(mod\,5^n)$, $i < n-1$, иначе $5^n | 3 \cdot 5^{i+1} + 5^{i+2} t_i$, что очевидно неверно при $i < n-1$. Таким образом данный случай невозможен.

Рассмотрим случай, когда $\delta = 2 \cdot 5^k$, $k \in \{0, 1, 2, \ldots, n-1\}$. Тогда

$$2^{2 \cdot 5^k} \equiv 4^{5^k} \equiv (-1)^{5^k} \equiv -1 (mod\, 5).$$

Очевидно, данный случай невозможен. Отсюда также следует невозможность третьего случая, так как если $2^{5^k} \equiv 1 (mod\, 5^n)$, то $2^{5^k} \equiv 1 (mod\, 5)$, а тогда $2^{2 \cdot 5^k} \equiv 1 (mod\, 5)$, что, как было доказано ранее, неверно.

Таким образом, получаем противоречие и $\delta = 4 \cdot 5^{n-1}$, то есть 2 - первообразный корень по модулю 5^n.

b) *Найдите первообразный корень по модулю* 7^n.

Покажем, что 5 является первообразным корнем по модулю 7^n. Действительно, пусть δ - показатель 5 по модулю 7. Значит $\delta | \varphi(7^n) = 6 \cdot 7^k$. Тогда $\delta = 6 \cdot 7^k$ либо $\delta = 3 \cdot 7^k$ либо $\delta = 2 \cdot 7^k$ либо $\delta = 7^k$, где $k \in \{0, 1, \ldots, n-1\}$. Предположим, что 5 - не первообразный корень, то есть что $\delta \neq 6 \cdot 7^{n-1}$.

Рассмотрим случай, когда $\delta = 6 \cdot 7^k$, $k \in \{0, 1, \ldots, n-2\}$. Заметим, что $5^6 = 1 + 2232 \cdot 7$, причём $2232 \not\equiv 0 (mod\, 7)$. Далее будем последовательно возводить обе части этого равенства в 7-тую степень, тем самым получая цепочку верных равенств:

$$5^6 = 1 + 2232 \cdot 7,$$

$$5^{6 \cdot 7} = 1 + 2232 \cdot 7^2 + 7^3 t_1,$$

$$5^{6 \cdot 7^2} = 1 + 2232 \cdot 7^3 + 7^4 t_2,$$

$$\ldots$$

$$5^{6 \cdot 7^i} = 1 + 2232 \cdot 7^{i+1} + 7^{i+2} t_i,$$

$$\ldots$$

$$5^{6 \cdot 7^{n-2}} = 1 + 2232 \cdot 7^{n-1} + 7^n t_{n-2},$$

$$5^{6 \cdot 7^{n-1}} = 1 + 2232 \cdot 7^n + 7^{n+1} t_{n-1} \equiv 1 (mod\, 7^n).$$

Заметим, что $5^{6 \cdot 7^i} \not\equiv 1 (mod\, 7^n)$, $i < n-1$, иначе $7^n | 2232 \cdot 7^{i+1} + 7^{i+2} t_i$, что очевидно неверно при $i < n-1$. Таким образом данный случай невозможен.

Рассмотрим случай, когда $\delta = 3 \cdot 7^k$, $k \in \{0, 1, \ldots, n-1\}$. Тогда

$$5^{3 \cdot 7^{n-1}} \equiv 125^{7^{n-1}} \equiv (-1)^{7^{n-1}} \equiv -1 (mod\, 7).$$

Таким образом данный случай невозможен. Отсюда также следует невозможность четвёртого случая, так как если $5^{7^k} \equiv 1 (mod\, 7^n)$, то $5^{7^k} \equiv 1 (mod\, 7)$, а тогда $5^{3 \cdot 7^k} \equiv 1 (mod\, 7)$, что, как было доказано ранее, неверно.

Рассмотрим случай, когда $\delta = 2 \cdot 7^k$, $k \in \{0, 1, \ldots, n-1\}$. Предположим $5^{2 \cdot 7^k} \equiv 1 (mod\, 7)$, тогда

$$5^{2 \cdot 7^k} \equiv 4^{7^k} \equiv 1 (mod\, 7).$$

Пусть $\widetilde{\delta}$ - показатель 4 по модулю 7. Тогда $\widetilde{\delta} \in \{1, 2, 3, 6\}$. Нетрудно проверить, что $\widetilde{\delta} = 3$. Но 7^k не кратно 3, а значит сравнение $4^{7^k} \equiv 1(mod\,7)$ не выполняется и данный случай невозможен.

Таким образом, получаем противоречие и $\delta = 6 \cdot 7^{n-1}$, то есть 5 - первообразный корень по модулю 7^n.

Занятие 5

Задача 1.

а) *Решите сравнение* $x^3 + 16x + 27 \equiv 0(mod\,900)$.

Разложим 900 на простые множители: $900 = 2^5 \cdot 5^2 \cdot 3^2$. И теперь от данного сравнения перейдём к равносильной системе сравнений:

$$\begin{cases} x^3 + 16x + 27 \equiv 0(mod\,4) \\ x^3 + 16x + 27 \equiv 0(mod\,25) \\ x^3 + 16x + 27 \equiv 0(mod\,9) \end{cases}$$

Решим каждое из сравнений системы и воспользуемся Китайской теоремой об остатках.

Рассмотрим первое сравнение. Преобразуем его и получим, что $x^3 \equiv 1(mod\,4)$. Теперь нетрудно убедиться что существует только одно решение по модулю 4: $x \equiv 1(mod\,4)$.

Рассмотрим второе сравнение. Обозначим $f(x) = x^3 + 16x + 27$. Воспользуемся методом подъёма приведённым в Лекции 6. Для начала решим сравнение $f(x) \equiv 0(mod\,5)$. Нетрудно видеть, что оно эквивалентно сравнению $x^2 + x + 2 \equiv 0(mod\,5)$. Перебором убеждаемся, что существует ровно одно решение по модулю 5: $x \equiv 4(mod\,5)$, то есть $x = 4 + 5t$, $t \in \mathbb{Z}$. Далее рассмотрим сравнение $\frac{f(4)}{5} + tf'(4) \equiv 0(mod\,5)$. Вычисляя значении многочлена и его производной при $x = 4$ и подставляя в сравнение получаем $31 + 64t \equiv 0(mod\,5)$. Отсюда получаем, что $t \equiv 1(mod\,5)$, то есть $t = 1 + 5z$, $z \in \mathbb{Z}$. Отсюда следует, что решениями этого сравнения являются следующие числа: $x \equiv 9(mod\,25)$.

Рассмотрим третье сравнение.Снова воспользуемся методом подъёма. Сравение $f(x) \equiv 0(mod\,3)$ имеет ровно одно решение по модулю 3: $x \equiv 0(mod\,3)$, то есть $x = 3t$, $t \in \mathbb{Z}$. Далее рассмотрим сравнение $\frac{f(0)}{3} + tf'(0) \equiv 0(mod\,3)$. Подставляя в него значения многочлена и его производной и преобразуя получаем, что $t = 3z$, $z \in \mathbb{Z}$. Таким образом решениеями второго сравнения являются следующие числа: $x \equiv 0(mod\,9)$.

Таким образом данная система равносильная следующей:

$$\begin{cases} x \equiv 1(mod\,4) \\ x \equiv 9(mod\,25) \\ x \equiv 0(mod\,9) \end{cases}$$

В обозначениях Китайской теоремы об остатках: $c_1 = 1$, $c_2 = 9$, $c_3 = 0$, $m_1 = 4$, $m_2 = 25$, $m_3 = 9$, $m = m_1 m_2 m_3 = 900$. Тогда

$$x \equiv c_1 x_1 \frac{m}{m_1} + c_2 x_2 \frac{m}{m_2} + c_3 x_3 \frac{m}{m_3} \equiv 225x_1 + 324x_2 (mod\, 900),$$

где $225x_1 \equiv 1(mod\, 4)$, то есть $x_1 \equiv 1(mod\, 4)$, и $36x_2 \equiv 1(mod\, 25)$, то есть $11x_2 \equiv 1(mod\, 25)$. Заметим, что подходит $x_2 \equiv 16(mod\, 25)$(это также может быть получено с помощью алгоритма Евклида). Используя найденные значения получаем, что $x \equiv 9(mod\, 900)$.

b)*Решите сравнение* $x^{12} \equiv 25(mod\, 41)$.

Указание. 6 - первообразный корень по модулю 41.

В исходном сравнении произведём замену: $y \equiv \mathrm{ind}_6 x(mod\, 40)$(такая замена корректна, так как 6 - первообразный корень по модулю 41). Тогда исходное сравнение равносильно сравнению $12y \equiv \mathrm{ind}_6 25(mod\, 40)$, $\mathrm{ind}_6 25 = 4$, действительно $6^4 \equiv 36 \cdot 36 \equiv (-5) \cdot (-5) \equiv 25(mod\, 41)$. Преобразуем данное сравнение и получим, что $3y \equiv 1(mod\, 10)$. Отсюда получаем, что $y \equiv 7(mod\, 10)$. Тогда $x \equiv 6^7 \equiv 11 \cdot 11 \cdot 6 \equiv 25 \cdot 11 \equiv 261 \equiv 15(mod\, 41)$. Таким образом решениями являются $x \equiv 15(mod\, 41)$.

c)*Найдите максимальную степень 7 делящую* $3^{7007} + 4^{7007}$.

Отметим, что 7 - простое, 7007 - нечётное и $7|(3+4)$. Таким образом выполнены все условия одного из следствий из леммы Гензеля для нечётного p:

$$v_7(3^{7007} + 4^{7007}) = v_7(3 + 4) + v_7(7007) = 3.$$

Задача 2.

Обозначим через $\omega(m, n) = |\{x^m \equiv 1(mod\, n) | 0 \leq x < n\}|$, *то есть число решений сравнения* $x^m \equiv 1(mod\, n)$ *не превосходящих* n.

a)*Докажите, что* $\omega(m, kl) = \omega(m, k)\omega(m, l)$, $(k, l) = 1$.

Рассмотрим следующую систему сравнений:

$$\begin{cases} x^m \equiv 1(mod\, k) \\ x^m \equiv 1(mod\, l) \end{cases}$$

Первое уравнение имеет ровно $\omega(m, k)$ решений по модулю k, второе - ровно $\omega(m, l)$ решений по модулю l. Исходя из китайской теоремы об остатках и комбинаторного правила произведения получаем, что система имеет ровно $\omega(m, k)\omega(m, l)$ решений по модулю kl. С другой стороны данная система равносильна сравнению $x^m \equiv 1(mod\, kl)$, которое имеет ровно $\omega(m, kl)$ решений по модулю kl. То есть $\omega(m, kl) = \omega(m, k)\omega(m, l)$.

b)*Вычислите* $\omega(m, p^\alpha)$, *где* p - *простое нечётное,* $\alpha \in \mathbb{N}$.

Отметим, что по модулю p^α существует некоторый первообразный корень g. Введём замену $y \equiv \mathrm{ind}_g x(mod\, \varphi(p^\alpha))$. Тогда исходное сравнение равносильно сравнению $my \equiv 0(mod\, \varphi(p^\alpha))$, которое в свою очередь равносильно сравнению $y \equiv 0 \left(mod\, \frac{\varphi(p^\alpha)}{(m, \varphi(p^\alpha))}\right)$, а значит таких y от 0 до $\varphi(p^\alpha) - 1$ существует ровно $(\varphi(p^\alpha), m)$. То есть $\omega(m, p^\alpha) = (\varphi(p^\alpha), m)$.

c)*Вычислите* $\omega(m, 2^\alpha)$, $\alpha \in \mathbb{N}$.

Случай $\alpha = 1$ тривиален и $\omega(m, 2) = 1$.

Пусть $\alpha > 1$, и пусть (c_0, c_1) - система индексов x по модулю 2^α. Тогда исходное сравнение равносильно системе

$$\begin{cases} mc_0 \equiv 0 (mod\, 2) \\ mc_1 \equiv 0 (mod\, 2^{\alpha-2}) \end{cases}$$

Исходя из китайской теоремы об остатках и комбинаторного правила произведения получаем, что система имеет ровно $(m, 2)(m, 2^{\alpha-2})$ решений по модулю $2^{\alpha-1}$, то есть $\omega(m, 2^\alpha) = (m, 2)(m, 2^{\alpha-2})$ при $\alpha > 1$.

d)*Вычислите $\omega(m, n)$ если известно каноническое разложение n.*

Пусть $n = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, где $\alpha \in \mathbb{N}_0$, $\alpha_i \in \mathbb{N}$, p_i - простые нечётные.

Рассмотрим случай, когда $\alpha = 0, 1$. Воспользуемся предыдущими пунктами данной задачи:

$$\omega(m, n) = \omega\left(m, 2^\alpha \prod_{i=1}^{r} p_i^{\alpha_i}\right) = \omega(m, 2^\alpha) \prod_{i=1}^{r} \omega(m, p_i^{\alpha_i}) = \prod_{i=1}^{r} \omega(m, p_i^{\alpha_i}) = \prod_{i=1}^{r} (m, \varphi(p_i^{\alpha_i})).$$

Рассмотрим случай $\alpha > 1$. Аналогично:

$$\omega(m, n) = \omega\left(m, 2^\alpha \prod_{i=1}^{r} p_i^{\alpha_i}\right) = \omega(m, 2^\alpha) \prod_{i=1}^{r} \omega(m, p_i^{\alpha_i}) = (m, 2)(m, 2^{\alpha-2}) \prod_{i=1}^{r} (m, \varphi(p_i^{\alpha_i})).$$

Таким образом верна следующая общая формула:

$$\omega(m, n) = \begin{cases} \prod\limits_{i=1}^{r} (m, \varphi(p_i^{\alpha_i})), & \alpha = 0, 1 \\ (m, 2)(m, 2^{\alpha-2}) \prod\limits_{i=1}^{r} (m, \varphi(p_i^{\alpha_i})), & \alpha > 1 \end{cases}$$

e)*Покажите, что $\omega(m, n) | \varphi(n)$.*

Воспользуемся формулой полученной в предыдущем пункте. В случае $\alpha = 0, 1$:

$$\omega(m, n) = \prod_{i=1}^{r} (m, \varphi(p_i^{\alpha_i})) \qquad \varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}).$$

Очевидно $(m, \varphi(p_i^{\alpha_i})) | \varphi(p_i^{\alpha_i})$ для любого $i = \overline{1, r}$. То есть $\omega(m, n) | \varphi(n)$.

В случае $\alpha > 1$:

$$\omega(m, n) = (m, 2)(m, 2^{\alpha-2}) \prod_{i=1}^{r} (m, \varphi(p_i^{\alpha_i})) \qquad \varphi(n) = 2^{\alpha-1} \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}).$$

Очевидно $(m, \varphi(p_i^{\alpha_i})) | \varphi(p_i^{\alpha_i})$ для любого $i = \overline{1, r}$ и $(m, 2)(m, 2^{\alpha-2}) | 2^{\alpha-1}$. То есть $\omega(m, n) | \varphi(n)$.

f**)*Пусть $x^m \equiv 1 (mod\, n)$. Покажите, что $x^{\omega(m,n)} \equiv 1 (mod\, n)$.*

Обозначим $\mathcal{G}_{m,n} = \{x | x^m \equiv 1 (mod\, n), 0 \leq x < n\}$. Нетрудно видеть, что выполнено включение $\mathcal{G}_{m,n} \subseteq \mathbb{Z}_n^*$. Покажем, что $\mathcal{G}_{m,n}$ - подгруппа по умножению группы $\mathbb{Z}_n^*$. Действительно: $1 \in \mathcal{G}_{m,n}$; пусть x, $y \in \mathcal{G}_{m,n}$, тогда $(xy)^m \equiv x^m y^m \equiv 1 (mod\, n)$, то есть $xy \in \mathcal{G}_{m,n}$; пусть $x \in \mathcal{G}_{m,n}$, тогда $(x^{-1})^m \equiv (x^m)^{-1} \equiv 1 (mod\, n)$, то есть $x^{-1} \in \mathcal{G}_{m,n}$. Таким образом $\mathcal{G}_{m,n}$ - подгруппа $\mathbb{Z}_n^*$.

Воспользуемся теоремой Лагранжа: порядок любого элемента конечной группы делит порядок этой группы. Нетрудно видеть, что $\mathrm{ord}\mathcal{G}_{m,n} = \omega(m,n)$. Исходя из теоремы Лагранжа получаем, что $x^{\omega(m,n)} \equiv 1 (mod\, n)$.

Задача 3.

a)*Пусть k - натуральное число. Найдите все такие l, что $3^k | 2^l - 1$.*

Нетрудно видеть, что l - чётное, в противном случае $2^l - 1 \equiv 1 (mod\, 3)$. Пусть $l = 2m$, $m \in \mathbb{N}$.

$3^k | 2^{2m} - 1$ равносильно тому, что $v_3(2^{2m} - 1) \geq k$. Воспользуемся леммой Гензеля для нечётного p:

$$v_3(2^{2m} - 1) = v_3(4 - 1) + v_3(m) = 1 + v_3(m) \geq k.$$

Это равносильно следующему неравенству: $v_3(m) \geq k - 1$. Это в свою очередь равносильно тому, что $l = 2 \cdot 3^q \cdot p$, где $q \geq k - 1$.

Занятие 6

Задача 1

a)*Решить сравнение $x^2 \equiv 34 (mod\, 37)$.*

Воспользуемся алгоритмом приведённый в Лекции 7. В обозначениях алгоритма $a = 34$. Для начала найдём квадратичный невычет по модулю 37. Покажем, что это 5. Действительно:

$$\left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Тогда в обозначениях алгоритма $n = 5$.

Вычислим a^{-1}. С помощью алгоритма Евклида нетрудно получить, что $a^{-1} \equiv 12 (mod\, 37)$.

Найдём s и α: $37 - 1 = 2^2 \cdot 9$, то есть $\alpha = 2$, $s = 9$.

Вычислим b: $b \equiv 5^9 \equiv 125^3 \equiv 14^3 \equiv 2^3 \cdot 7^3 \equiv 8 \cdot 49 \cdot 72 \equiv 56 \cdot 49 \equiv 12 \cdot 19 \equiv 228 \equiv 6 (mod\, 37)$.

Найдём r: $r \equiv 34^5 \equiv (-3)^5 \equiv -3 \cdot 81 \equiv -3 \cdot 7 \equiv 16 (mod\, 37)$.

Найдём j_0. Для этого возведём $r^2 a^{-1}$ в степень $2^{\alpha - 2}$. Получим:

$$r^2 a^{-1} \equiv 16^2 \cdot 12 \equiv 256 \cdot 12 \equiv 34 \cdot 12 \equiv 1 (mod\, 37).$$

Значит $j_0 = 0$. Тогда и $j = 0$. Получаем, что $x_1 \equiv 16 (mod\, 37)$. Тогда $x_2 \equiv 21 (mod\, 37)$.

b)*Решить сравнение $x^2 + 2x + 7 \equiv 0 (mod\, 121)$.*

Воспользуемся методом спуска приведённым в Лекции 6. Для начала решим сравнение $x^2 + 2x + 7 \equiv 0 (mod\, 11)$. Преобразуем данное сравнение

следующим образом $(x+1)^2 \equiv 5(mod\,11)$ и введём замену $y \equiv x+1(mod\,11)$. Рассмотрим сравнение $y^2 \equiv 5(mod\,11)$. Отметим, что 11 - простое число вида $4k+3$, а значит можно применить Теорему 1 Лекции 7: $y \equiv \pm 5^3 \equiv \pm(3 \cdot 5) \equiv \pm 4 \equiv 4, 7(mod\,11)$. Тогда получаем два решения относительно x: $x_1 \equiv 3(mod\,11)$ и $x_2 \equiv 6(mod\,11)$.

Рассмотрим случай $x_1 = 3+11t$, $t \in \mathbb{Z}$. Тогда $f(3) = 22$, $f'(3) = 8$. Решим сравнение $2 + 8t \equiv 0(mod\,11)$. Оно равносильно сравнению $8t \equiv 9(mod\,11)$. Отсюда нетрудно найти, что $t \equiv 8(mod\,11)$. То есть $x_1 = 91 + 121z$, $z \in \mathbb{Z}$.

Рассмотрим случай $x_1 = 6 + 11t$, $t \in \mathbb{Z}$. Тогда $f(6) = 55$, $f'(6) = 14$. Решим сравнение $5 + 14t \equiv 0(mod\,11)$. Оно равносильно сравнению $3t \equiv 6(mod\,11)$. Отсюда нетрудно найти, что $t \equiv 2(mod\,11)$. То есть $x_1 = 28 + 121z$, $z \in \mathbb{Z}$.

Таким образом $x_1 = 91 + 121z$, $z \in \mathbb{Z}$ либо $x_1 = 28 + 121z$, $z \in \mathbb{Z}$.

c)*Решить сравнение* $x^2 \equiv 1(mod\,32)$.

Так как 32 - степень двойки, то можно использовать явные формулы полученные в Теореме 4 Лекции 3. Получаем ровно 4 решения: $x \equiv 1, 15, 17, 31(mod\,32)$.

Занятие 7

Задача 1

a)*Разложить в цепную дробь число* $131/583$*, найти все подходящие дроби.*

Запишем алгоритм Евклида для пары $(131, 583)$:

$$131 = 0 \cdot 583 + 131,$$
$$583 = 4 \cdot 131 + 59,$$
$$131 = 2 \cdot 59 + 13,$$
$$59 = 4 \cdot 13 + 7,$$
$$13 = 1 \cdot 7 + 6,$$
$$7 = 1 \cdot 6 + 1,$$
$$6 = 6 \cdot 1.$$

Исходя из Теоремы 1 Лекции 8 получаем, что $131/583 = [0, 4, 2, 4, 1, 1, 6]$.

Подходящие дроби вычислим используя Теорему 2 Лекции 8.

$$P_0 = 0, \qquad Q_0 = 1,$$
$$P_1 = 1, \qquad Q_1 = 4,$$
$$P_2 = 2, \qquad Q_2 = 9,$$
$$P_3 = 9, \qquad Q_3 = 40,$$
$$P_4 = 11, \qquad Q_4 = 49,$$

$$P_5 = 20, \qquad Q_5 = 89,$$
$$P_6 = 131, \qquad Q_5 = 583.$$

b)*Найти значение бесконечной чисто периодической цепной дроби* $[1, 2, 2, 2, 1, 2, 2, 2, \dots]$.

Исходя из Теоремы 7 Лекции 8 существует действительное α, такое что $\alpha = [1, 2, 2, 2, 1, 2, 2, 2, \dots]$. Тогда верно равенство:

$$\alpha = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\alpha}}}}.$$

Преобразуя данное равенство получаем квадратичное уравнение $15\alpha^2 - 2\alpha - 7 = 0$. Оно имеет два корня $\alpha_{1,2} = \frac{1 \pm \sqrt{106}}{15}$. Очевидно отрицательное значение не подходит, а значит $\alpha = [1, 2, 2, 2, 1, 2, 2, 2, \dots] = \frac{1+\sqrt{106}}{15}$.

c)*Представить в виде бесконечной цепной дроби* $\sqrt{2}$.

Воспользуемся алгоритмом Теоремы 4 Лекции 7:

$$\alpha_0 = \sqrt{2}, \qquad a_0 = 1,$$
$$\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1, \qquad a_1 = 2,$$
$$\alpha_2 = \frac{1}{\sqrt{2} + 1 - 2} = \frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1, \qquad a_2 = 2,$$
$$\alpha_3 = \frac{1}{\sqrt{2} + 1 - 2} = \frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1, \qquad a_3 = 2$$

и так далее. Нетрудно видеть, что в итоге мы получим $\sqrt{2} = [1, 2, 2, \dots]$.

d)*Решить уравнения* $131x + 583y = 1$ *и* $x^2 - 2y^2 = 1$*(в целых и натуральных числах соответственно).*

Вопользуемся полученными ранее разложениями в цепные дроби чисел $131/583$ и $\sqrt{2}$ и формулами приведёнными в Лекции 8. Решения линейного уравнения:

$$x = -89 \cdot 131 \cdot \frac{1}{131} + 583t = -89 + 583t, \qquad t \in \mathbb{Z},$$
$$y = 20 \cdot 583 \cdot \frac{1}{583} - 131t = 20 - 131t.$$

Решения уравнения Пелля:

$$x_n = \frac{1}{2}\left((3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n\right), \qquad n \in \mathbb{N},$$
$$y_n = \frac{1}{2\sqrt{2}}\left((3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n\right).$$

e)*Найти несколько разложений в обобщённую цепную дробь числа* $131/583$.

Воспользуемся замечанием из Лекции 8 и запишем несколько вариантов обобщённого алгоритма Евклида для пары $(131, 583)$:

$$131 = 0 \cdot 583 + 131,$$

$$583 = 4 \cdot 131 + 59,$$

$$131 = 2 \cdot 59 + 13,$$

$$59 = 5 \cdot 13 - 6,$$

$$13 = (-3) \cdot (-6) - 5,$$

$$-6 = 1 \cdot (-5) - 1,$$

$$-5 = 5 \cdot (-1).$$

То есть $131/583 = [0, 4, 2, 5, -3, 1, 5]$.

$$131 = 0 \cdot 583 + 131,$$

$$583 = 4 \cdot 131 + 59,$$

$$131 = 2 \cdot 59 + 13,$$

$$59 = 5 \cdot 13 - 6,$$

$$13 = (-2) \cdot (-6) + 1,$$

$$-6 = (-6) \cdot 1.$$

То есть $131/583 = [0, 4, 2, 5, -2, -6]$.

Задача 2

a)*Получить аналоги свойств 1,4 и 5,6 для подходящих дробей* P_n/Q_n *и* P_{n-3}/Q_{n-3}, *где* $3 \leq n \leq m$.

Рассмотрим следующее выражение:

$$P_nQ_{n-3} - P_{n-3}Q_n = (a_nP_{n-1} + P_{n-2})Q_{n-3} - P_{n-3}(a_nQ_{n-1} - Q_{n-2}) =$$

$$= a_n(P_{n-1}Q_{n-3} - P_{n-3}Q_{n-1}) + (P_{n-2}Q_{n-3} - P_{n-3}Q_{n-2}) =$$

$$= a_na_{n-1}(-1)^{n-1} + (-1)^{n-1} = (a_na_{n-1} + 1)(-1)^{n-1}.$$

Таким образом $P_nQ_{n-3} - P_{n-3}Q_n = (a_na_{n-1} + 1)(-1)^{n-1}$. Разделим обе части этого равенства на Q_nQ_{n-3} и получим:

$$\frac{P_n}{Q_n} - \frac{P_{n-3}}{Q_{n-3}} = \frac{(a_na_{n-1} + 1)(-1)^{n-1}}{Q_nQ_{n-3}},$$

$$\left|\frac{P_n}{Q_n} - \frac{P_{n-3}}{Q_{n-3}}\right| = \frac{a_na_{n-1} + 1}{Q_nQ_{n-3}},$$

b)*Пусть* $f_\alpha(n)$ *- количество точек с натуральными координатами в области координатной плоскости ограниченной прямой* $y = \alpha x$, *прямой*

$x = n$ и осью Ox. Будем считать, что $n \in \mathbb{N}$ и $\alpha > 0$. Пусть α иррационально. Покажите, что $f_\alpha(n) = f_{P_k/Q_k}(n)$, где P_k/Q_k - любая подходящая дробь для α с знаменателем большим n.

Предположим, что это не так. То есть найдутся некоторые α и n что $f_\alpha(n) \neq f_{P_k/Q_k}(n)$. Тогда найдётся точка (x_0, y_0), $x_0, y_0 \in \mathbb{N}$ с абсциссой не превосходящей n лежащая между этими прямыми. Нетрудно видеть, что эта точка не может лежать на самих прямых. Тогда выполнено неравенство:

$$|\alpha x_0 - y_0| < \left|\alpha x_0 - \frac{P_k}{Q_k} x_0\right|,$$

что равносильно

$$\left|\alpha - \frac{y_0}{x_0}\right| < \left|\alpha - \frac{P_k}{Q_k}\right|.$$

Получаем противоречие, так как $\frac{P_k}{Q_k}$ является лучшим приближением, то есть для любой дроби $\frac{a}{b}$, $a, b \in \mathbb{N}$, $b < Q_k$ выполнено $\left|\alpha - \frac{P_k}{Q_k}\right| < |\alpha - \frac{a}{b}|$.