1 Показатели. Первообразные корни.

1.1 Понятие показателя. Простейшие свойства.

Определение. Будем говорить, что *число* a, $(a,n)=1$ *принадлежит показателю* $\delta \in \mathbb{N}$ *по модулю* n, если δ - минимальное число, такое что $a^\delta \equiv 1(mod\, n)$.

Замечание. Из теоремы Эйлера следует, что $1 \leq \delta \leq \varphi(n)$.

Пример. Число 4 принадлежит показателю 3 по модулю 9, так как $4^3 \equiv 64 \equiv 1(mod\, 9)$, в то время как 4^2 и 4 не сравнимы с 1 по модулю 9.

Число 3 принадлежит показателю 4 по модулю 16, так как $3 \equiv 3(mod\, 16)$, $3^2 \equiv 9(mod\, 16)$, $3^3 \equiv 11(mod\, 16)$, $3^4 \equiv 1(mod\, 16)$.

Свойства показателей. Пусть a принадлежит показателю δ по модулю n. Тогда:

1)Числа a, $a^2, \ldots, a^\delta$ попарно несравнимы по модулю n.

Доказательство.

Предположим $a^\alpha \equiv a^\beta(mod\, n)$. Пусть $\alpha > \beta$. Тогда $a^{\alpha-\beta} \equiv 1(mod\, m)$. В тоже время $\alpha - \beta < \delta$, что противоречит тому, что a принадлежит показателю δ по модулю n.

2)Сравнение $a^\alpha \equiv a^\beta(mod\, n)$ выполнено тогда и только тогда, когда $\alpha \equiv \beta(mod\, \delta)$.

Доказательство

Предположим $a^\alpha \equiv a^\beta(mod\, n)$. Пусть $\alpha > \beta$. Тогда $a^{\alpha-\beta} \equiv 1(mod, m)$. По теореме о делении с остатком $\alpha - \beta = \delta p + q$, $0 \leq q < \delta$. Если $q \neq 0$, то получаем противоречие с минимальностью δ.

3)$\varphi(n)$ делится на δ.

Доказательство.

По теореме Эйлера $a^{\varphi(n)} \equiv 1(mod\, n)$. Исходя из этого и свойства 2 получаем необходимое.

Пример. Найдём показатель которому принадлежит 7 по модулю 36. Заметим, что $\varphi(36) = \varphi(9)\varphi(4) = 6 \cdot 2 = 12$. Исходя из свойства 3 показатель может быть равен $2, 3, 4, 6$ или 12. С помощью небольшого перебора получаем, что он равен 6.

Замечание. Максимальное δ, такое что a, $a^2, \ldots, a^\delta$ попарно несравнимы по модулю n, является показателем a по модулю δ(доказать самостоятельно). В тоже время, если δ делит $\varphi(n)$, не означает, что a принадлежит показателю δ по модулю n.

Задача 1. Пусть p, q - простые числа, $2^p \equiv 1(mod\, q)$. Докажите, что $q \equiv 1(mod\, p)$.

Решение.

Пусть δ - показатель 2 по модулю q. Тогда по свойству 2 $\delta | p$. Очевидно $\delta > 1$, тогда $\delta = p$. По свойству 3 $p | \varphi(q) = q - 1$, что и требовалось доказать.

Задача 2.Докажите, что не существует натурального числа n, большего 1, такого, что $n | 2^n - 1$.

Решение

Предположим, такое $n > 1$ существует. Нетрудно видеть, что n - нечётное. Пусть p - наименьший простой делитель числа n. Пусть 2 принадлежит показателю δ по модулю p. Так как $p|2^n - 1$ и $p|2^{p-1} - 1$ получаем, что $\delta|n$ и $\delta|p-1$. Тогда найдётся простое число q, такое что $q < p-1$ и $q|\delta$, тогда $q|n$, что противоречит минимальности p.

Задача 3. Докажите, что любой делитель d числа Ферма $f_n = 2^{2^n} + 1$ имеет вид $d = 2^{n+1}x + 1$, $x \in \mathbb{N}_0$. Доказать, что f_5 делится на 641.

Решение.

Пусть q - произвольный простой делитель f_n. Тогда $2^{2^{n+1}} \equiv 1(mod\, q)$. Пусть δ - показатель 2 по модулю q. Тогда $\delta|2^{n+1}$. Предположим $\delta = 2^k$, $k \leq n$, но тогда $2^{2^n} \equiv \left(2^\delta\right)^{\frac{2^n}{\delta}} \equiv 1(mod\, q)$. Следовательно $\delta = 2^{n+1}$. По малой теореме Ферма $2^{q-1} \equiv 1(mod\, q)$, а значит $2^{n+1}|q-1$. То есть $q = 2^{n+1}x + 1$. Далее нетрудно показать, что произведение чисел такого вида так же будет иметь вид $2^{n+1}y + 1$, $y \in \mathbb{N}_0$.

Покажем, что f_5 делится на $641 = 2^6 \cdot 10 + 1$. Используем тождество $641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$.

$$2^{32} \equiv 2^4 \left(2^7\right)^4 \equiv -5^4 \left(2^7\right)^4 \equiv -\left(5 \cdot 2^7\right) \equiv -(-1)^4 \equiv -1(mod\, 641).$$

Задача 4. Найдите все решения уравнения $2^x - 3^y = 5$ в натуральных числах.

Доказательство.

Перепишем уравнение в виде $2^x = 5 + 3^y$. Отсюда следует, что $x \geq 3$. Допустим $x \geq 6$, тогда $3^y \equiv 59(mod\, 64)$. Пусть δ - показатель 3 по модулю 64. Тогда $\delta|\varphi(64)$, то есть $\delta = 2^k$, где $k \in \{0, 1, 2, 3, 4, 5\}$. Небольшим перебором убеждаемся, что $\delta = 16$. Найдём минимальное решение сравнения $3^y \equiv 59(mod\, 64)$: $3^1 \equiv 3(mod\, 64)$, $3^2 \equiv 9(mod\, 64)$, $3^3 \equiv 27(mod\, 64)$, $3^4 \equiv 14(mod\, 64)$, $3^5 \equiv 51(mod\, 64)$, $3^6 \equiv 25(mod\, 64)$, $3^7 \equiv 11(mod\, 64)$, $3^8 \equiv 33(mod\, 64)$, $3^9 \equiv 35(mod\, 64)$, $3^{10} \equiv 41(mod\, 64)$, $3^{11} \equiv 59(mod\, 64)$.

Таким образом $y \equiv 11(mod\, 16)$, то есть $y = 16k + 11$. Подставим в исходное уравнение:

$$2^x = 3^{11+16k} + 5 \equiv 3^{11} + 5(mod\, 17).$$

Пусть $3^{11} \equiv a(mod\, 17)$. Тогда $3^5 a \equiv 243a \equiv 1(mod\, 17)$. То есть $5a \equiv 1(mod\, 17) \Rightarrow a \equiv 7(mod\, 17)$.

Таким образом $2^x \equiv 12(mod\, 17)$. Обозначим через Δ - показатель, которому принадлежит 2 по модулю 17. Тогда $\Delta|16$: $2^1 \equiv 2(mod\, 17)$, $2^2 \equiv 4(mod\, 17)$, $2^4 \equiv 16(mod\, 17)$, $2^8 \equiv 1(mod\, 17)$. Таким образом $\Delta = 8$. С другой стороны $2^3 \equiv 8(mod\, 17)$, $2^5 \equiv 15(mod\, 17)$, $2^6 \equiv 13(mod\, 17)$, $2^7 \equiv 9(mod\, 17)$. Таким образом сравнение $2^x \equiv 12(mod\, 17)$ не имеет решений.

Следовательно $x \in \{3, 4, 5\}$. Перебором находим, что $x = 3$, $y = 1$ или $x = 5, y = 3$.

1.2 Нахождение показателей.

Утверждение 1. Если a принадлежит показателю $\delta_1\delta_2$ по модулю n, то a^{δ_1} принадлежит показателю δ_2 по модулю n.

Доказательство

От противного. Пусть a^{δ_1} принадлежит показателю $\Delta \neq \delta_2$ по модулю n. Очевидно $\Delta < \delta_2$. Тогда

$$\left(a^{\delta_1}\right)^{\Delta} \equiv a^{\Delta\delta_1} \equiv 1(mod\, n).$$

Но тогда $\delta_1\delta_2 > \Delta\delta_1$. Получаем противоречие.

Утверждение 2. Если a принадлежит показателю δ_1, а b показателю δ_2 по модулю n, и $(\delta_1, \delta_2) = 1$, то ab принадлежит показателю $\delta_1\delta_2$ по модулю n.

Доказательство

Случай, когда одно из чисел a и b сравнимо с 1 по модулю n очевиден. Далее будем считать, что $a \not\equiv 1(mod\, n)$, $b \not\equiv 1(mod\, n)$. Тогда и $\delta_1, \delta_2 \neq 1$.

Пусть ab принадлежит показателю Δ по модулю n. Отметим также, что $\Delta \neq 1$, в противном случае $b \equiv a^{-1}(mod\, n)$ и $\delta_1 = \delta_2$.

Нетрудно видеть, что $(ab)^{\delta_1\delta_2} \equiv 1(mod\, n)$. Тогда $\Delta|\delta_1\delta_2$, тогда $\Delta = q_1q_2$, где $q_1|\delta_1$ и $q_2|\delta_2$. Отсюда следует что

$$(ab)^{\Delta} \equiv (ab)^{q_1q_2}(mod\, n) \Rightarrow ((ab)^{q_1q_2})^{\frac{\delta_1}{q_1}} \equiv a^{\delta_1q_2}b^{\delta_1q_2} \equiv b^{\delta_1q_2}(mod\, n).$$

Таким образом $\delta_2|\delta_1q_2$, исходя из того, что $(\delta_1, \delta_2) = 1$ получаем, что $\delta_2|q_2$. Но как ранее было сказано $q_2|\delta_2$, а значит $q_2 = \delta_2$. Аналогично показываем, что $q_1 = \delta_1$. Таким образом $\Delta = \delta_1\delta_2$, что и требовалось доказать.

Утверждение 3. Пусть a принадлежит показателю δ по модулю n. Тогда a^{γ}, $\gamma \in \mathbb{N}$ принадлежит показателю $\frac{\delta}{(\delta,\gamma)}$ по модулю n.

Доказательство

Пусть a^{γ} принадлежит показателю Δ по модулю n. Тогда $a^{\Delta\gamma} \equiv 1(mod\, n)$. Это равносильно тому, что $\delta|\Delta\gamma$. Найдём минимальное натуральное Δ удовлетворяющее этому условию. Нетрудно видеть, что это условие равносильно тому, что Δ кратно $\frac{\delta}{(\delta,\gamma)}$. Отсюда получаем, что $\Delta = \frac{\delta}{(\delta,\gamma)}$.

Пример. В предыдущем примере было показано, что 7 принадлежит показателю 6 по модулю 36. Исходя из Утверждения 1 7^2 принадлежит показателю 3 по модулю 36. Исходя из утверждения 3 получаем, что 7^8 принадлежит показателю 3 по модулю 36, а 7^3 принадлежит показателю 2 по модулю 36. Используя это и утверждение 2 получаем, что 7^{11} принадлежит показателю 6 по модулю 36.

Задача 5. Пусть натуральное число a принадлежит показателю δ по модулю n. Для любого натурального γ найдите такое число принадлежащее показателю (δ, γ) по модулю n.

Решение.

Будем искать такое число в виде a^m. Исходя из Утверждения 3 оно будет иметь показатель $\frac{\delta}{(\delta,m)}$. Получается, что число a^m подходит тогда и только тогда, когда выполняется равенство

$$(\gamma, \delta) = \frac{\delta}{(\delta, m)}.$$

Пусь $d = (\gamma, \delta)$ и $\delta = d\delta_1$, $\gamma = d\gamma_1$, $(\gamma_1, \delta_1) = 1$. Тогда данное равенство можно переписать в виде

$$\delta_1 = (m, d\delta_1).$$

Отсюда очевидно следует, что число $m = \delta_1 = \frac{\delta}{(\delta,n)}$ подходит. То есть число $a^{\frac{\delta}{(\delta,n)}}$ принадлежит показателю (δ, γ) по модулю n.

1.3 Первообразные корни.

Определение. Будем говорить, что g является *первообразным корнем по модулю* n, если g принадлежит показателю $\varphi(n)$ по модулю n.

Замечание. Из свойств показателя следует эквивалентное определение первообразного корня: g является первообразным корнем, если g, $g^2, \ldots, g^{\varphi(n)}$ попарно несравнимы по модулю n, то есть множество остатков элементов указанного множества по модулю n есть множество всех остатков по модулю n взаимнопростых с n(то есть *образует приведённую систему вычетов*).

Пример. Рассмотрим показатель, которому принадлежит 2 по модулю 9: $2^1 \equiv 2(mod\,9)$, $2^2 \equiv 4(mod\,9)$, $2^3 \equiv 8(mod\,9)$, $2^6 \equiv 1(mod\,9)$. Получаем, что 2 принадлежит $\varphi(9)$ по модулю 9, а значит 2 - первообразный корень по модулю 9. Нетрудно видеть, что 8 не является первообразным корнем по модулю 9, так как $8^2 \equiv 1(mod\,9)$.

Теорема. Первообразный корень по модулю n существует тогда и только тогда, когда $n = 2$, 4, $p^\alpha, 2p^\alpha$, где p - простое нечётное.

Доказательство приведено в книге Виноградова И.М. Основы теории чисел.

Пример. По модулю 4, 9, 50, 243 существуют первообразные корни, а по модулю $8, 64, 75$ - нет.

Теорема. g является первообразным корнем по модулю $\varphi(n) = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, p_i - простые, тогда и только тогда, когда $g^{\frac{\varphi(n)}{p_i}} \not\equiv 1(mod\,n)$ для любого $i \in \overline{1,r}$.

Доказательство.

Заметим, что если g - первообразный корень, то это утверждение очевидно выполнено исходя из определения.

Далее покажем, что если g не является первообразным корнем, то существует такое i, что $g^{\frac{\varphi(n)}{p_i}} \equiv 1(mod\,n)$. Пусть g - принадлежит показателю δ по модулю n. Тогда $\delta|\varphi(n)$, а значит имеет вид $p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$, где $0 \le \beta_i \le \alpha_i$. Также все β_i не могут быть одновременно равными α_i соответственно, исходя из того, что g - не первообразный корень. Тогда очевидно, что хотя бы одно из чисел $\frac{\varphi(n)}{p_i}$ будет кратно δ, то есть $g^{\frac{\varphi(n)}{p_i}} \equiv 1(mod\,n)$.

Пример. Определим являются числа 4 и 5 первообразными корнями по модулю 9. $\varphi(9) = 6 = 2 \cdot 3$ и $4^3 \equiv 1(mod\,9)$, $5^3 \equiv 8(mod\,9)$, $5^2 \equiv 7(mod\,9)$. Таким образом 4 - не является первообразным корнем по модулю 9, а 5 - первообразный корень.

Теорема. Если по модулю n существует первообразный корень, то по этому модулю существует ровно $\varphi(\varphi(n))$ первообразных корней(не превосходящих n).

Доказательство

Как было сказано ранее множество остаток во модулю n множества $\{g, g^2, \ldots, g^{\varphi(n)}\}$ образует приведённую систему вычетов. А это значит, что любой другой первообразный корень G по модулю n представим в виде g^γ. G принадлежит показателю $\varphi(n)$ по модулю n, с другой стороны по Утверждению 3 он принадлежит показателю $\frac{\varphi(n)}{(\varphi(n),\gamma)}$. Исходя из этого получаем, что подходят только γ взаимнопростые с $\varphi(n)$. А их существует ровно $\varphi(\varphi(n))$, что и требовалось доказать.

Замечание. Из доказательства следует способ нахождения всех первообразных корней, если известен один из них.

Пример. По модулю 9 существует ровно $\varphi(\varphi(9)) = 2$ первообразных корня не превосходящих 9. Они были найдены ранее - это 2 и 5. Тогда всё множество первообразных корней может быть описано следующим образом $\{2 + 9k | k \in \mathbb{N}_0\} \cup \{5 + 9k | k \in \mathbb{N}_0\}$.

По модулю 1250 существует ровно $\varphi(\varphi(1250)) = \varphi(500) = 200$ первообразных корней не превосходящих 1250.

Задача 6. Найти наименьший первообразный корень по модулю 18. Найти все первообразные корни по модулю 18.

Решение.

5 - наименьшее число отличное от 1 взаимнопростое с 18. Так как $\varphi(18) = 6$ и $5^3 \not\equiv 1 (mod\, 18)$, $5^2 \not\equiv 1 (mod\, 18)$ получаем, что 5 - наименьший первообразный корень по модулю 18.

Всего по модулю 18 существует $\varphi(\varphi(18)) = 2$ первообразных корня не превосходящих 18. Найдём все такие γ, что $(\gamma, \varphi(18))$ и $1 \leq \gamma \leq 6$. Таких γ ровно 2: 1 и 5. Отсюда получаем второй первообразный коренm $5^5 \equiv 11 (mod\, 18)$. Тогда всё множество первообразных корней может быть описано следующим образом $\{5 + 18k | k \in \mathbb{N}_0\} \cup \{11 + 18k | k \in \mathbb{N}_0\}$.

Замечание. Определение показателя и первообразного корня можно ввести используя язык алгебры. Далее будем обозначать через $\mathbb{Z}_n$ - аддитивную группу вычетов, а через $\mathbb{Z}_n^*$ - мультипликативную группу вычетов. Рассмотрим $a, 0 \leq a < n$. Тогда a можно рассматривать как элемент группы $\mathbb{Z}_n^*$. Тогда показатель δ, которому принадлежит a есть ни что иное, как порядок a в группе $\mathbb{Z}_n^*$, то есть $\delta = ord_{\mathbb{Z}_n^*} a$. Отметим, что тогда набор остатков элементов множества $\{a, a^2, \ldots, a^\delta\}$ с операцией умножения остатков представляет собой циклическую подгруппу группы $\mathbb{Z}_n^*$ порождённую элементом a.

Существование первообразного корня g по модулю n будет означать, что группа $\mathbb{Z}_n^*$ является циклической, а значит изоморфной некоторой аддитивной группе вычетов. Действительно, нетрудно видеть, что $\mathbb{Z}_n^* \simeq \mathbb{Z}_{\varphi(n)}$. Например $\mathbb{Z}_9^* \simeq \mathbb{Z}_6$. В качестве изоморфизма может выступать отображение $\psi(a) = \gamma$, где $a = g^\gamma$. Исходя из ранее приведённых результатов получаем, что группа $\mathbb{Z}_n^*$ является циклической тогда и только тогда, когда

$n = 2,\ 4,\ p^\alpha, 2p^\alpha$, где p - простое нечётное. Первообразный корень g является есть не что иное как порождающий элемент группы $\mathbb{Z}_n^*$. Таким образом, если $\mathbb{Z}_n^*$ - циклическая, то ровно $\varphi(\varphi(n))$ её элементов являются порождающими.

Отметим, что существование первообразного корня по модулю p может быть получено из того факта, что $\mathbb{Z}_p^*$ является мультипликативной группой поля $(\mathbb{Z}_p, +, \cdot)$.

1.4 Задачи для самостоятельного решения.

Задача 1

a)Найти все первообразные корни по модулю 27.

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

Задача 2

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

Задача 3

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

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