Тема 2. Основы элементарной теории чисел и приложения-2

Теоретический материал

§1. Первообразные корни, индексы.

Пусть a, m – натуральные взаимно простые числа, причем $m>1$, тогда, согласно теореме Эйлера, $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$. Наименьшее натуральное число n такое, что $a^n \equiv 1 (\mathrm{mod}\, m)$ называется *показателем*, которому принадлежит число a по модулю m.

Если $\varphi(m)$ – показатель, которому принадлежит число a по модулю m, то число а называется *первообразным корнем* по модулю m. Известно, что первообразный корень по модулю m существует тогда и только тогда, когда $m = 2, 4, p^k, 2p^k$, где p – нечетное простое число.

Для нахождения первообразных корней удобно использовать следующий факт. Пусть $q_1^{r_1} ... q_k^{r_k}$ – каноническое разложение числа $\varphi(m)$, g – натуральное число, взаимно простое с числом m. Число g является первообразным корнем по модулю m тогда и только тогда, когда $g^{\frac{\varphi(m)}{q_i}}$ не сравнимо с 1 по модулю m для любого i.

Пусть $m = p^k$ или $2p^k$, $c = \varphi(m)$, g – первообразный корень по модулю m, тогда числа $1, g, ..., g^{c-1}$ образуют приведенную систему вычетов по модулю m. Пусть число a взаимно просто с числом m. Целое неотрицательное число d называется *индексом* числа a по модулю m при основании g, если $g^d \equiv a (\mathrm{mod}\, m)$. Индекс d обозначают $ind_g a$ или $ind\ a$. Вообще говоря, индекс определен не однозначно, но если известен один из индексов d, то любой другой индекс d' можно найти по формуле $d' \equiv d (\mathrm{mod}\, c)$.

Свойства индексов:

1) $ind_g\ a_1 \cdot ... \cdot a_n \equiv ind_g a_1 + ... + ind_g a_n\ (\mathrm{mod}\ c)$;

2) $ind_g\ a^n \equiv n \cdot ind_g\ a (\mathrm{mod}\ c)$ для любого натурального значения n.

Если $(a, m) = 1$, $x^n \equiv a (\mathrm{mod}\, m)$ для некоторого целого значения x, то число a называется *вычетом* степени n по модулю m. В противном случае, число a называется *невычетом* степени n по модулю m. В приведенной системе вычетов по модулю m число вычетов степени n по модулю m равно $\dfrac{\varphi(m)}{(\varphi(m), n)}$. Число a является вычетом степени n по модулю m тогда и только тогда, когда $a^q \equiv 1 (\mathrm{mod}\, m)$, где $q = \dfrac{\varphi(m)}{(\varphi(m), n)}$.

Пусть $c = \varphi(m)$. Показатель, которому принадлежит число a по модулю m, равен $\dfrac{c}{(c, ind\ a)}$. В частности, число a является первообразным корнем по модулю m тогда и только тогда, когда $(c, ind\ a) = 1$. В приведенной системе вычетов по модулю m количество чисел, принадлежащих показателю t, равно $\varphi(t)$. В частности, количество первообразных корней в приведенной системе вычетов по модулю m равно $\varphi(\varphi(m))$.

Системой индексов нечетного числа a по модулю 2^k $(k \in N)$ называется пара чисел (γ, γ_0) такая, что $(-1)^\gamma 5^{\gamma_0} \equiv a(\mathrm{mod}\, 2^k)$. Зная одну пару индексов (γ, γ_0), можно найти все такие пары индексов (δ, δ_0) по формулам $\delta \equiv \gamma(\mathrm{mod}\, c), \delta_0 \equiv \gamma_0(\mathrm{mod}\, c_0)$, где $\begin{cases} c = 1, c_0 = 1 \text{ при } \mathrm{k} = 1, \\ c = 2, c_0 = 2^{k-2} \text{ при } \mathrm{k} > 1 \end{cases}$.

Пусть $2^{\alpha_0} p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ – каноническое разложение числа m, $m > 1, (a, m) = 1$, g_i – первообразный корень по модулю $p_i^{\alpha_i}$. Упорядоченный набор $(\gamma, \gamma_0, \gamma_1, \ldots, \gamma_k)$ называется *системой индексов числа a по модулю m*, если $(-1)^\gamma 5^{\gamma_0} \equiv a(\mathrm{mod}\, 2^{\alpha_0})$, $g_i^{\gamma_i} \equiv a(\mathrm{mod}\, p_i^{\alpha_i})$ для любого $i = 1, \ldots, k$. Любая другая система индексов $(\delta, \delta_0, \delta_1, \ldots, \delta_k)$ связана с исходной следующим образом: $\delta \equiv \gamma(\mathrm{mod}\, c), \delta_i \equiv \gamma_i(\mathrm{mod}\, c_i)$, где $\begin{cases} c = 1, c_0 = 1 \text{ при } \mathrm{k} = 1, \\ c = 2, c_0 = 2^{k-2} \text{ при } \mathrm{k} > 1, \\ c_i = \varphi(p_i^{\alpha_i}) \text{ при } \mathrm{i} = 1, \ldots, k. \end{cases}$

§2. Показательные и полиномиальные сравнения.

Рассмотрим показательное сравнение $a^x \equiv b(\mathrm{mod}\, m)$ (1). Предположим, что $(a, m) = 1$, тогда условие $(b, m) = 1$ является необходимым для разрешимости сравнения (1). Пусть $2^{\alpha_0} p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ - каноническое разложение модуля m, где α_0 может быть нулем. Сравнение (1) равносильно системе сравнений: $a^x \equiv b(\mathrm{mod}\, 2^{\alpha_0})$, $a^x \equiv b(\mathrm{mod}\, p_i^{\alpha_i})$, $i = \overline{1, k}$ (2). Пусть $(\gamma, \gamma_0, \gamma_1, \ldots, \gamma_k)$, $(\delta, \delta_0, \delta_1, \ldots, \delta_k)$ - системы индексов соответственно чисел a и b по модулю m, то есть $(-1)^\gamma 5^{\gamma_0} \equiv a(\mathrm{mod}\, 2^{\alpha_0})$, $g_i^{\gamma_i} \equiv a(\mathrm{mod}\, p_i^{\alpha_i})$, $(-1)^\delta 5^{\delta_0} \equiv b(\mathrm{mod}\, 2^{\alpha_0})$, $g_i^{\delta_i} \equiv b(\mathrm{mod}\, p_i^{\alpha_i})$, где g_i - первообразный корень по модулю $p_i^{\alpha_i}$ ($i = \overline{1, k}$). Тогда система (2) эквивалентна системе сравнений первого порядка: $x\gamma \equiv \delta(\mathrm{mod}\, c)$, $x\gamma_0 \equiv \delta_0(\mathrm{mod}\, c_0)$, $x\gamma_i \equiv \delta_i(\mathrm{mod}\, c_i)$, $i = \overline{1, k}$, (5.3) где $c = \begin{cases} 2, \alpha_0 \geq 2, \\ 1, \alpha_0 < 2, \end{cases}$ $c_0 = \begin{cases} 2^{\alpha_0 - 2}, \alpha_0 \geq 2, \\ 1, \alpha_0 < 2, \end{cases}$ $c_i = \varphi(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}(p_i - 1)$, $i = \overline{1, k}$. Решение системы (3), если оно существует, может быть найдено с помощью китайской теоремы об остатках.

Другой подход к решению показательного сравнения (1) заключается в использовании свойств показателей и дальнейшем применении китайской теоремы об остатках.

Укажем способ решения степенного сравнения $ax^n \equiv b(\bmod m)$ (4). Рассмотрим случай, когда $(b,m)=1$. Пусть $2^{\alpha_0} p_1^{\alpha_1} \dots p_k^{\alpha_k}$ - каноническое разложение модуля m, где $\alpha_0 \geq 0$, тогда сравнение (4) эквивалентно системе сравнений: $ax^n \equiv b(\bmod 2^{\alpha_0})$, $ax^n \equiv b(\bmod p_i^{\alpha_i})$, $i=\overline{1,k}$. Пусть $(\gamma, \gamma_0, \gamma_1, \dots, \gamma_k)$, $(\delta, \delta_0, \delta_1, \dots, \delta_k)$ - системы индексов соответственно чисел a и b по модулю m , то есть $(-1)^{\gamma} 5^{\gamma_0} \equiv a(\bmod 2^{\alpha_0})$, $g_i^{\gamma_i} \equiv a(\bmod p_i^{\alpha_i})$, $(-1)^{\delta} 5^{\delta_0} \equiv b(\bmod 2^{\alpha_0})$, $g_i^{\delta_i} \equiv b(\bmod p_i^{\alpha_i})$, где g_i - первообразный корень по модулю $p_i^{\alpha_i}$. Тогда система индексов $(\lambda, \lambda_0, \lambda_1, \dots, \lambda_k)$ числа x по модулю m может быть найдена из следующих сравнений: $\gamma + n\lambda \equiv \delta(\bmod c)$, $\gamma_0 + n\lambda_0 \equiv \delta_0(\bmod c_0)$, $\gamma_i + n\lambda_i \equiv \delta_i(\bmod c_i)$, $i=\overline{1,k}$. Решение сравнения (4) можно найти из системы: $x \equiv (-1)^{\lambda} 5^{\lambda_0}(\bmod 2^{\alpha_0})$, $x \equiv g_i^{\lambda_i}(\bmod p_i^{\alpha_i})$, $i=\overline{1,k}$.

Перейдем к рассмотрению полиномиальных сравнений $f(x) \equiv 0(\bmod m)$ (5), где $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$, $a_i \in Z$ для любого $i=\overline{0,n}$. Сравнение (5) равносильно системе сравнений $f(x) \equiv 0(\bmod p_i^{\alpha_i})$, $i=\overline{1,l}$, где $p_1^{\alpha_1} \dots p_l^{\alpha_l}$ - каноническое разложение модуля m. Таким образом, для решения сравнения (5) следует решить каждое из сравнений $f(x) \equiv 0(\bmod p_i^{\alpha_i})$, а затем применить китайскую теорему об остатках.

Приведем способ нахождения решения полиномиального сравнения $f(x) \equiv 0(\bmod p^{\alpha})$ по примарному модулю.

1) Применяя теорему Ферму, сравнение $f(x) \equiv 0(\bmod p)$ сводим к полиномиальному сравнению $g(x) \equiv 0(\bmod p)$, где g - многочлен с целыми коэффициентами степени не выше, чем $p-1$. Находим решения сравнения $g(x) \equiv 0(\bmod p)$: $x \equiv x_1(\bmod p), \dots, x \equiv x_r(\bmod p)$.

2) Для каждого фиксированного $i=\overline{1,r}$ полагаем $x = x_i + t_i p$, где $t_i \in Z$. Левую часть сравнения $f(x_i + t_i p) \equiv 0(\bmod p^2)$ раскладываем по формуле Тейлора (принимая во внимание, что число $f^{(j)}(x_i)/j!$ является целым, и отбрасывая члены, кратные p^2): $f(x_i) + t_i p f'(x_i) \equiv 0(\bmod p^2)$. Сокращая обе части сравнения и модуль на p, получаем: $\dfrac{f(x_i)}{p} + t_i f'(x_i) \equiv 0(\bmod p)$. Находим решения этого сравнения: $t_i \equiv t_{i,1}(\bmod p)$,…, $t_i \equiv t_{i,s}(\bmod p)$. Таким образом, $x \equiv x_i + t_{i,j} p = x_{i,j}(\bmod p^2)$, $i=\overline{1,r}$, $j=\overline{1,s}$.

3) Для каждых фиксированных $i=\overline{1,r}$, $j=\overline{1,s}$ полагаем $x=x_i+t_{i,j}p+z_{i,j}p^2=x_{i,j}+z_{i,j}p^2$, где $z_{i,j}\in Z$. Аналогично левую часть сравнения $f(x_{i,j}+z_{i,j}p^2)\equiv 0(\operatorname{mod} p^3)$ раскладываем по степеням p и отбрасываем члены, кратные p^3: $f(x_{i,j})+p^2 z_{i,j}f'(x_{i,j})\equiv 0(\operatorname{mod} p^3)$. Сокращая сравнение на p^2, получим: $\dfrac{f(x_{i,j})}{p}+z_{i,j}f'(x_{i,j})\equiv 0(\operatorname{mod} p)$. Решая сравнение, находим, что $z_{i,j}\equiv z_{i,j,k}(\operatorname{mod} p)$, $k=\overline{1,q}$. Подставляя в x, получим: $x\equiv x_{i,j}+z_{i,j,k}p=x_{i,j,k}(\operatorname{mod} p^3)$.

4) Проделывая последовательно для модулей $p^4,\dots,p^\alpha$ описанную процедуру, найдем решения $x\equiv x_\lambda(\operatorname{mod} p^\alpha)$ сравнения $f(x)\equiv 0(\operatorname{mod} p^\alpha)$.

Отметим, что в случае $f'(x_i)\not\equiv 0(\operatorname{mod} p)$ решение $x\equiv x_i(\operatorname{mod} p)$ сравнения $g(x)\equiv 0(\operatorname{mod} p)$ даст одно решение $x\equiv \beta_i(\operatorname{mod} p^\alpha)$ сравнения $f(x)\equiv 0(\operatorname{mod} p^\alpha)$.

§3. Квадратичные вычеты.

Рассмотрим двучленное сравнение второй степени $x^2\equiv a(\operatorname{mod} m)$ (6), где $(a,m)=1$. Если сравнение (6) имеет решение, то число a называется *квадратичным вычетом* по модулю m, в противном случае a называется *квадратичным невычетом* по модулю m.

Пусть $m=p$, где p - нечетное простое число. Приведенная система вычетов по модулю p состоит из $\dfrac{p-1}{2}$ квадратичных вычетов и $\dfrac{p-1}{2}$ квадратичных невычетов. *Символ Лежандра* $\left(\dfrac{a}{p}\right)$ определяется равенством $\left(\dfrac{a}{p}\right)=1$, если a является квадратичным вычетом по модулю p, и равенством $\left(\dfrac{a}{p}\right)=-1$, если a является квадратичным невычетом по модулю p. Для любых $a,b\in Z$, $(a,p)=(b,p)=1$ и любого нечётного простого числа q, $(p,q)=1$, имеют место следующие свойства:

1) $a\equiv b(\operatorname{mod} p)\Rightarrow\left(\dfrac{a}{p}\right)=\left(\dfrac{b}{p}\right)$;

2) $\left(\dfrac{a}{p}\right)\equiv a^{\frac{p-1}{2}}(\operatorname{mod} p)$ (критерий Эйлера);

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

4) $\left(\frac{a}{p}\right)=(-1)^{\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{2ai}{p}\right]}$;

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

Пусть теперь P - нечётное натуральное число, большее 1, и $p_1 \dots p_n$ - разложение числа P на простые множители. Для всякого целого числа a, взаимно простого с P, *символ Якоби* $\left(\frac{a}{P}\right)$ определяется через символы Лежандра по формуле: $\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)\cdot\left(\frac{a}{p_2}\right)\cdot\ldots\cdot\left(\frac{a}{p_n}\right)$. Для любых целых a,b, взаимно простых с P, и любого нечётного натурального Q, большего 1 и взаимно простого с P, имеют место следующие свойства символа Якоби:

6) $a \equiv b \pmod P \Rightarrow \left(\frac{a}{P}\right)=\left(\frac{b}{P}\right)$;

7) $\left(\frac{ab}{P}\right)=\left(\frac{a}{P}\right)\cdot\left(\frac{b}{P}\right)$;

8) $\left(\frac{1}{P}\right)=1$;

9) $\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}$;

10) $\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}$;

11) $\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right)$.

Отметим, что равенство символа Якоби $\left(\frac{a}{P}\right)$ единице является необходимым условием для того, чтобы число a было квадратичным вычетом по модулю P, но не достаточным.

Задачи

1. Решите показательное сравнение $5^x \equiv 229 (\bmod 1001)$.

► Так как $1001 = 7 \cdot 11 \cdot 13$, то сравнение $5^x \equiv 229 (\bmod 1001)$ равносильно системе сравнений:

$$\begin{cases} 5^x \equiv 229 (\bmod 7), \\ 5^x \equiv 229 (\bmod 11), \\ 5^x \equiv 229 (\bmod 13). \end{cases}$$

Показатель δ_m, которому принадлежит число 5 по модулю m делит $\varphi(m)$. Отсюда находим, что $\delta_7 = 6$, $\delta_{11} = 5$, $\delta_{13} = 4$. Так как $5^1 \equiv 5 \equiv 229 (\bmod 7)$, $5^4 \equiv 9 \equiv 229 (\bmod 11)$, $5^3 \equiv 8 \equiv 229 (\bmod 13)$, то имеем:

$$\begin{cases} 5^x \equiv 229 (\bmod 7), \\ 5^x \equiv 229 (\bmod 11), \\ 5^x \equiv 229 (\bmod 13), \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 (\bmod 6), \\ x \equiv 4 (\bmod 5), \\ x \equiv 3 (\bmod 4), \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 (\bmod 3), \\ x \equiv 4 (\bmod 5), \\ x \equiv 3 (\bmod 4). \end{cases}$$

Применяя к последней системе китайскую теорему об остатках, получаем $x \equiv 19 (\bmod 60)$.◄

2. Решите степенное сравнение $7x^{17} \equiv 157 (\bmod 1144)$.

► Найдем системы индексов чисел $a = 7$, $b = 157$ по модулю $m = 1144 = 2^3 \cdot 11 \cdot 13$. Имеем $7 \equiv (-1)^1 5^2 (\bmod 8)$, $157 \equiv 5 = (-1)^2 5^1 (\bmod 8)$; $\operatorname{ind}_2 7 (\bmod 11) = 7$, $\operatorname{ind}_2 157 (\bmod 11) = \operatorname{ind}_2 3 (\bmod 11) = 8$; $\operatorname{ind}_2 7 (\bmod 13) = 11$, $\operatorname{ind}_2 157 (\bmod 13) = \operatorname{ind}_2 1 (\bmod 13) = 12$. Следовательно, $(1,2,7,11)$ и $(2,1,8,12)$ - системы индексов чисел 7 и 157 по модулю 1144. Для нахождения системы индексов неизвестного числа x получаем систему сравнений:

$$\begin{cases} 1+17\lambda \equiv 2 (\bmod 2), \\ 2+17\lambda_0 \equiv 1 (\bmod 2), \\ 7+17\lambda_1 \equiv 8 (\bmod 10), \\ 11+17\lambda_2 \equiv 12 (\bmod 12). \end{cases}$$

Решая систему, находим, что $(1,1,3,5)$ - система индексов числа x. Получаем систему сравнений для нахождения x:

$$\begin{cases} x \equiv -5 (\bmod 8), \\ x \equiv 8 (\bmod 11), \\ x \equiv 32 (\bmod 13). \end{cases}$$

Используя китайскую теорему об остатках, получаем, что $x \equiv 19 (\bmod 1144)$. ◄

3. Решите полиномиальное сравнение $16x^8 - 8x^7 + 9x^4 - 1 \equiv 0 (\bmod 196)$.

► Исходное сравнение эквивалентно системе сравнений:

$$\begin{cases} 16x^8 - 8x^7 + 9x^4 - 1 \equiv 0 (\bmod 2^2), \\ 16x^8 - 8x^7 + 9x^4 - 1 \equiv 0 (\bmod 7^2). \end{cases}$$

Из первого сравнения системы получаем: $x \equiv \pm 1 (\bmod 4)$. Обозначим $f(x) = 16x^8 - 8x^7 + 9x^4 - 1$. Найдем решение сравнения $f(x) \equiv 0 (\bmod 7)$. Имеем: $f(x) \equiv 2x^2 - x + 2x^4 - 1 \equiv 2x^2 - x + 16x^4 - 1 = (2x-1)(x + 8x^3 + 4x^2 + 2x + 1) \equiv$

$\equiv (2x-1)(x^3 - 3x^2 + 3x + 1) = (2x-1)((x-1)^3 + 2) \equiv 0 (\bmod 7)$. Отсюда получаем, что $x \equiv 4 (\bmod 7)$. Пусть $x = 4 + 7t$, $t \in Z$.

Далее $f(x) = f(4+7t) \equiv f(4) + 7t \cdot f'(4) \equiv 28 + 14t \equiv 0 (\bmod 7^2)$. Следовательно, $t \equiv 5 (\bmod 7)$. Таким образом, $x \equiv 39 (\bmod 49)$ - решение второго сравнения системы.

Применяя китайскую теорему об остатках к системам

$$\begin{cases} x \equiv 1 (\bmod 4), \\ x \equiv 39 (\bmod 49), \end{cases} \quad \begin{cases} x \equiv -1 (\bmod 4), \\ x \equiv 39 (\bmod 49), \end{cases}$$

заключаем, что $x \equiv 137 (\bmod 196)$, $x \equiv 39 (\bmod 196)$.◄

4. Докажите, что сравнение $x^8 \equiv 23 (\bmod 41)$ не имеет решений.

► Воспользуемся тем, что число 6 – первообразный корень по модулю 41. Тогда $x^8 \equiv 23 (\bmod 41) \Leftrightarrow 8\,\mathrm{ind}_6 x \equiv \mathrm{ind}_6 23 (\bmod 40)$. Так как $\mathrm{ind}_6 23 \equiv 36 (\bmod 40)$ и $(8,40) \nmid 36$, то исходное сравнение решений не имеет.◄

5. Решите уравнение $2^x - 3^y = 5$ в натуральных числах.

► $2^x = 3^y + 5 \geq 8 \;\Rightarrow\; x \geq 3$. Допустим, что $x \geq 6$, тогда $3^y \equiv 59 (\bmod 64)$. Пусть n - показатель, которому принадлежит число 3 по модулю 59, тогда $n \mid \varphi(2^6)$, то есть $n = 2^k,\; k \in \{0,1,2,3,4,5\}$. Так как $3^1 \equiv 3 (\bmod 64)$, $3^2 \equiv 9 (\bmod 64)$, $3^4 \equiv 17 (\bmod 64)$, $3^8 \equiv 33 (\bmod 64),\; 3^{16} \equiv 1 (\bmod 64)$, то $n = 16$. Найдем наименьшее натуральное решение сравнения $3^y \equiv 59 (\bmod 64)$.

y	1	2	3	4	5	6	7	8	9	10	11
$3^y (\bmod 64)$	3	9	27	17	51	25	11	33	35	41	59

Таким образом, $y \equiv 11 (\bmod 16)$.

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

Пусть $3^{11} \equiv a (\bmod 17)$, тогда $243a \equiv 1 (\bmod 17) \;\Rightarrow\; 5a \equiv 1 (\bmod 17) \;\Rightarrow\; a \equiv 7 (\bmod 17)$.

Таким образом, $2^x \equiv 12 (\bmod 17)$.

Обозначим через m показатель, которому принадлежит число 2 по модулю 17, тогда $m \mid 16$. Так как $2^1 \equiv 2 (\bmod 17),\; 2^2 \equiv 4 (\bmod 17)$, $2^4 \equiv -1 (\bmod 17)$, $2^8 \equiv 1 (\bmod 17)$, то $m = 8$. Кроме того, $2^3 \equiv 8 (\bmod 17)$, $2^5 \equiv 15 (\bmod 17)$, $2^6 \equiv 13 (\bmod 17)$, $2^7 \equiv 9 (\bmod 17)$. Поэтому сравнение $2^x \equiv 12 (\bmod 17)$ не имеет решений.

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

6. Для каждого натурального $m > 1$ найдите число вычетов в полной системе вычетов по модулю m, удовлетворяющих сравнению $x^2 \equiv 4 (\bmod m)$.

► Пусть $m = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ - каноническое разложение числа m.

$$x^2 \equiv 4 (\bmod m) \Leftrightarrow \begin{cases} x^2 \equiv 4 (\bmod p_1^{\alpha_1}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x^2 \equiv 4 (\bmod p_k^{\alpha_k}) \end{cases}$$

Если $p_i > 2$, то $x^2 \equiv 4 (\mathrm{mod}\, p_i^{\alpha_i}) \Leftrightarrow (x-2)(x+2) \equiv 0 (\mathrm{mod}\, p_i^{\alpha_i}) \Rightarrow x \equiv \pm 2 (\mathrm{mod}\, p_i^{\alpha_i})$.

Рассмотрим сравнение $x^2 \equiv 4 (\mathrm{mod}\, 2^\alpha)$, $\alpha \in N$.

Если $\alpha \geq 5$, то $x \equiv \pm 2, \pm 2 + 2^{\alpha-2}, \pm 2 + 2^{\alpha-1}, \pm 2 + 3 \cdot 2^{\alpha-2} (\mathrm{mod}\, 2^\alpha)$,

Если $\alpha = 4$, то $x \equiv \pm 2, \pm 6 (\mathrm{mod}\, 16)$,

если $\alpha = 3$, то $x \equiv \pm 2 (\mathrm{mod}\, 8)$,

если $\alpha = 2$, то $x \equiv 0, 2 (\mathrm{mod}\, 4)$,

если $\alpha = 1$, то $x \equiv 0 (\mathrm{mod}\, 2)$.

В силу китайской теоремы об остатках каждая система $\begin{cases} x \equiv c_1 (\mathrm{mod}\, p_1^{\alpha_1}) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv c_k (\mathrm{mod}\, p_k^{\alpha_k}) \end{cases}$ имеет единственное решение по модулю m. Обозначим через $N(m)$ число решений сравнения $x^2 \equiv 4 (\mathrm{mod}\, m)$, тогда $N(m) = \begin{cases} 2^{k-1}, \mathrm{ord}_2 m = 1, \\ 2^k, \mathrm{ord}_2 m \in \{0, 2, 3\}, \\ 2^{k+1}, \mathrm{ord}_2 m = 4, \\ 2^{k+2}, \mathrm{ord}_2 m \geq 5. \end{cases}$ ◄

7. Исследовать на разрешимость сравнение $x^2 \equiv 557 (\mathrm{mod}\, 854)$.

► В силу китайской теоремы об остатках исходное сравнение разрешимо тогда и только тогда, когда разрешимо каждое сравнение системы. Первое сравнение, очевидно, разрешимо. Вычислим символы Лежандра $\left(\frac{557}{7}\right)$ и $\left(\frac{557}{61}\right)$: $\left(\frac{552}{7}\right) = \left(\frac{4}{7}\right) = 1$, $\left(\frac{557}{61}\right) = \left(\frac{8}{61}\right) = \left(\frac{2}{61}\right) = -1$. Решений нет.◄

8. В приведенной системе вычетов по модулю 23 найдите все квадратичные вычеты.

► Так как $\left(\frac{2}{23}\right) = 1$, то 2 - квадратичный вычет по модулю 23. Следовательно, все степени двойки $2, 4, 8, 16, 9, 18, 13, 3, 6, 12, 1$ по модулю 23 являются квадратичными вычетами. ◄

9. Покажите, что в RSA-криптосистеме с параметрами p,q,e,d имеется $r+s+rs$ неподвижных сообщений x, $0<x<N=pq$, где $r=(p-1,e-1)$, $s=(q-1,e-1)$.

► Если $e=1$, то все сообщения неподвижны и их количество равно $N-1=pq-1=(p-1)+(q-1)+(p-1)(q-1)=r+s+rs$. Пусть $e>1$. Найдём число решений сравнения $x^e \equiv x(\operatorname{mod} pq)$. Сравнение равносильно системе $\begin{cases} x^e \equiv x(\operatorname{mod} p), \\ x^e \equiv x(\operatorname{mod} q). \end{cases}$ Так как $(x, x^{e-1}-1)=1$, то последняя система эквивалентна совокупности систем:

$$\begin{cases} x \equiv 0(\operatorname{mod} p), \\ x \equiv 0(\operatorname{mod} q), \end{cases} \begin{cases} x \equiv 0(\operatorname{mod} p), \\ x^{e-1} \equiv 1(\operatorname{mod} q), \end{cases} \begin{cases} x^{e-1} \equiv 1(\operatorname{mod} p), \\ x \equiv 0(\operatorname{mod} q), \end{cases} \begin{cases} x^{e-1} \equiv 1(\operatorname{mod} p), \\ x^{e-1} \equiv 1(\operatorname{mod} q). \end{cases}$$

Первая система не имеет решений x, $0<x<N$. Отметим, что сравнение $x^{e-1} \equiv 1(\operatorname{mod} p)$ равносильно сравнению $(e-1)\operatorname{ind}_g x \equiv 0(\operatorname{mod} p-1)$, где g - некоторый первообразный корень по модулю p. Число решений этого сравнения из промежутка $(0,N)$ равно $(p-1,e-1)=r$. Аналогично сравнение $x^{e-1} \equiv 1(\operatorname{mod} p)$ имеет $(q-1,e-1)=s$ решений из промежутка $(0,N)$. Используя китайскую теорему об остатках, получаем, что всего решений $r+s+rs$. ◄

10. Пусть $N=pq$, где p,q - различные простые числа вида $4k+3$. Доказать эквивалентность условий:

1) существует эффективный алгоритм решения сравнения $x^2 \equiv a(\operatorname{mod} N)$;

2) существует эффективный алгоритм факторизации модуля N.

► 1) Пусть известно разложение $N=pq$, тогда сравнение $x^2 \equiv a(\operatorname{mod} N)$ распадается на четыре системы: $x \equiv \pm a^{(p+1)/4}(\operatorname{mod} p)$, $x \equiv \pm a^{(q+1)/4}(\operatorname{mod} q)$, решение каждой из которых находится с помощью китайской теоремы об остатках.

2) Пусть имеется эффективный алгоритм решения сравнения $x^2 \equiv a(\operatorname{mod} N)$. Выберем случайное натуральное число $a \in (0,N)$, взаимно простое с модулем N. Пусть $m \equiv a^2(\operatorname{mod} N)$. Рассмотрим сравнение $x^2 \equiv m(\operatorname{mod} N)$. Найдём его решения $\{a, N-a, b, N-b\}$ из промежутка $(0,N)$, где $a \neq b$, $a \neq N-b$. Так как $a^2 \equiv m(\operatorname{mod} N)$, $b^2 \equiv m(\operatorname{mod} N)$, то $(a-b)(a+b) \equiv 0(\operatorname{mod} N)$. Так как $a \pm b \not\equiv 0(\operatorname{mod} N)$, то $(N,a+b)$ равно p или q. Найдя $(N,a+b)$ с помощью алгоритма Евклида, узнаем один из простых делителей числа N. ◄

11. Покажите, что, зная $\varphi(N)$, легко факторизовать RSA-модуль $N = pq$.

► Пусть известно число $c = \varphi(N) = (p-1)(q-1) = pq - p - q + 1 = N + 1 - (p+q)$. Таким образом, $q = N + 1 - c - p$. Поэтому $N = p(N+1-c) - p^2$. Решив квадратное уравнение, найдем p, а, следовательно, и q. ◄

12. В полной системе вычетов найдите все числа, принадлежащие показателю 6 по модулю 43.

► Так как $\varphi(43) = 42 = 2 \cdot 3 \cdot 7$ и $3^{21} \equiv -1(\bmod 43)$, $3^{14} \equiv 36(\bmod 43)$, $3^6 \equiv 41(\bmod 43)$, то число 3 является первообразным корнем по модулю 43. Поэтому числа $3^1, 3^2, ..., 3^{42}$ образуют приведенную систему вычетов по модулю 43. Число 3^γ принадлежит показателю $\dfrac{\varphi(43)}{(\gamma, \varphi(43))} = \dfrac{42}{(\gamma, 42)}$. Так как по условию $\dfrac{42}{(\gamma, 42)} = 6$, то $(\gamma, 42) = 7$, откуда находим, что $\gamma = 7$ или $\gamma = 35$. Так как $3^7 \equiv 37(\bmod 43)$, $3^{35} \equiv 7(\bmod 43)$, то существует два числа 7 и 37, принадлежащие показателю 6 по модулю 43. ◄

13. Доказать, что если по модулю m существует первообразный корень, то по этому модулю существует ровно $\varphi(\varphi(m))$ первообразных корней.

► Пусть $m = 2, 4, p^k, 2p^k$ и g - один из первообразных корней по модулю m. Тогда $(g, m) = 1$. Докажем, что множество $\{g^1, g^2, ..., g^{\varphi(m)}\}$ образует приведенную систему вычетов. Достаточно убедиться, что $g^i \not\equiv g^j (\bmod m)$ для любых $i, j \in \{1, ..., \varphi(m)\}$, $i \neq j$. Допустим найдутся такие i, j ($1 \le j < i \le \varphi(m)$), что $g^i \equiv g^j (\bmod m)$. Так как $(g^j, m) = 1$, то $g^{i-j} \equiv 1(\bmod m)$. То есть показатель, которому принадлежит g по модулю m, меньше $\varphi(m)$. Противоречие. Следовательно, все первообразные корни по модулю m являются элементами множества $\{g^1, g^2, ..., g^{\varphi(m)}\}$. Получаем, что число g^γ принадлежит показателю $\varphi(m)/(\gamma, \varphi(m))$ по модулю m. Таким образом, остаётся найти число решений уравнения $\dfrac{\varphi(m)}{(\gamma, \varphi(m))} = \varphi(m)$. Отсюда получаем, что $(\gamma, \varphi(m)) = 1$. Число первообразных корней равно $\varphi(\varphi(m))$.◄

14. Найти наименьший натуральный первообразный корень по модулю 18. Найти все первообразные корни по модулю 18.

► Наименьшее натуральное g, взаимно простое с модулем, это 5. Так как $\varphi(18) = 6$ и $5^2 \not\equiv 1(mod\ 18)$, $5^3 \not\equiv 1(mod\ 18)$, то 5 – первообразный корень. Всего первообразных корней $\varphi(\varphi(18)) = 2$. Находим такие γ, что $(\gamma, \varphi(18)) = 1$. Подходят лишь $\gamma = 1$ и $\gamma = 5$. Вторым первообразным корнем является $5^5 \equiv 11$.◄

15. Пусть p – простое число вида $4k + 3$. Докажите, что если сравнение $x^2 \equiv a(mod\, p)$ разрешимо, то его решения задаются соотношениями $x \equiv \pm a^{\frac{p+1}{4}}(mod\, p)$.

► Если $a \equiv 0(mod\, p)$, то существует единственное решение $x \equiv 0(mod\, p)$. Пусть $a \not\equiv 0(mod\, p)$, тогда существуют ровно 2 решения. Покажем, что $x \equiv \pm a^{\frac{p+1}{4}}(mod\, p)$ удовлетворяют сравнению. Имеем $x^2 \equiv a^{\frac{p+1}{2}} = a \cdot a^{\frac{p-1}{2}} \equiv a \cdot \left(\frac{a}{p}\right) \equiv a(mod\, p)$.◄

Задачи для самостоятельного решения

1. Докажите, что для простых $p > 5$ и натуральных m равенство $(p-1)! + 1 = p^m$ невозможно.

2. Пусть натуральные числа a и b таковы, что $a^n + n \mid b^n + n$ для любого натурального n. Докажите, что $a = b$.

3. Найдите все натуральные x, удовлетворяющие равенству $\varphi(2x) = \varphi(3x)$.

4. Решите сравнение $x^3 + 16x + 27 \equiv 0(\text{mod}\, 900)$.

5. Решите сравнение $3^x \equiv 92(\text{mod}\, 143)$.

6. Решите сравнение $x^{12} \equiv 37(\text{mod}\, 41)$.

7. Покажите, что сообщение $x = 67$ является неподвижным ($E(x) = x$) в RSA-криптосистеме с параметрами $N = 187,\ e = 141$. Найдите все неподвижные сообщения.