Тема 1. Основы элементарной теории чисел и приложения-1

Теоретический материал

§1. Множество вычетов по модулю, свойства сравнений. Пусть m – натуральное число, большее 1. Через Z_m обозначаем множество всех классов вычетов $\overline{a} = \{a + mt | t \in Z\}$. Грубо говоря, Z_m – это множество всех остатков $\overline{0}$, $\overline{1}$, …, $\overline{m-1}$ при делении на m. На множестве Z_m естественным образом вводятся операции сложения и умножения (по сути, по правилам сложения и умножения остатков).

Пусть *a, b* – целые числа, *m* – натуральное число. Говорят, что *a* сравнимо с *b* по модулю *m*, если $a - b$ делится на *m*. В этом случае будем писать $a \equiv b (\mathrm{mod}\, m)$. Приведем основные свойства сравнений:

1) $a \equiv a (\mathrm{mod}\, m)$;

2) если $a \equiv b (\mathrm{mod}\, m)$, то $b \equiv a (\mathrm{mod}\, m)$;

3) если $a \equiv b (\mathrm{mod}\, m)$, $b \equiv c (\mathrm{mod}\, m)$, то $a \equiv c (\mathrm{mod}\, m)$;

4) если $a \equiv b (\mathrm{mod}\, m)$, то $ca \equiv cb (\mathrm{mod}\, m)$;

5) если $ca \equiv cb (\mathrm{mod}\, m)$, $(c, m) = 1$, то $a \equiv b (\mathrm{mod}\, m)$;

6) если $a \equiv b (\mathrm{mod}\, m)$, то $ca \equiv cb (\mathrm{mod}\, cm)$;

7) если $a \equiv b (\mathrm{mod}\, m)$, $c \equiv d (\mathrm{mod}\, m)$, то $a \pm c \equiv b \pm d (\mathrm{mod}\, m)$, $ac \equiv bd (\mathrm{mod}\, m)$;

8) если $a \equiv b (\mathrm{mod}\, m)$, то $a^n \equiv b^n (\mathrm{mod}\, m)$ для любого натурального *n*;

9) если $a \equiv b (\mathrm{mod}\, m)$, $f(x)$ – многочлен с целыми коэффициентами, то $f(a) \equiv f(b) (\mathrm{mod}\, m)$;

10) $a \equiv b (\mathrm{mod}\, m_1), \ldots, a \equiv b (\mathrm{mod}\, m_k)$ тогда и только тогда, когда $a \equiv b (\mathrm{mod}\, [m_1, \ldots, m_k])$;

11) если $a \equiv b (\mathrm{mod}\, m)$, *m* делится на *d*, то $a \equiv b (\mathrm{mod}\, d)$;

12) если $a^k \equiv b^k (\mathrm{mod}\, m)$, *n* делится на *k*, то $a^n \equiv b^n (\mathrm{mod}\, m)$.

§2. Алгоритм Евклида. Линейные сравнения и системы. Китайская теорема об остатках. Пусть *a, b* – целые не нулевые числа, тогда существует единственная пара целых чисел *q, r* такая, что $a = bq + r$, причем $0 \le r < |b|$ (*теорема о делении с остатком*).

Наибольший общий делитель двух чисел можно найти с помощью *алгоритма Евклида*, не прибегая к каноническому разложению самих чисел. Для этого число *a* разделим на *b* с остатком: $a = bq_1 + r_1$, где $0 \le r_1 < |b|$. Если $r_1 = 0$, то $(a, b) = |b|$. Если $r_1 > 0$, то разделим *b* на r_1 с остатком: $b = r_1 q_2 + r_2$, где $0 \le r_2 < r_1$. Если $r_2 = 0$, то $(a, b) = r_1$. Если $r_2 > 0$, то разделим r_1 на r_2 с остатком: $r_1 = r_2 q_3 + r_3$, где $0 \le r_3 < r_2$. И так далее продолжаем эту

процедуру. Конечный не нулевой остаток и будет наибольшим общим делителем чисел a и b. Если на каждом шаге осуществляется деление $a = bq + r$, причем $-\frac{|b|}{2} \le r < \frac{|b|}{2}$, то говорят, что применяется алгоритм Евклида с выбором наименьшего по модулю остатка.

С помощью алгоритма Евклида наибольший общий делитель чисел $a_1,...,a_n$ можно представить в виде линейной комбинации этих чисел, а именно, существуют целые числа $y_1,...,y_n$ такие, что $y_1a_1 + ... + y_na_n = (a_1,...,a_n)$. Такое представление называется линейным разложением наибольшего общего делителя чисел $a_1,...,a_n$.

Сравнение $ax \equiv b(\mathrm{mod}\, m)$ разрешимо тогда и только тогда, когда b делится на (a, m). Причем, если x_0 - это одно из решений сравнения $ax \equiv b(\mathrm{mod}\, m)$, то множество всех решений этого сравнения имеет вид $\left\{ x_0 + \frac{m}{(a,m)}t : t \in Z \right\}$, т.е. $ax \equiv b(\mathrm{mod}\, m) \Leftrightarrow x \equiv x_0 \left(\mathrm{mod}\, \frac{m}{(a,m)} \right)$.

Вышеуказанное решение линейного сравнения $ax \equiv b(\mathrm{mod}\, m)$ позволяет найти все решения *линейного диофантова уравнения* $ax + by = c$, где a, b, c – целые числа, $a, b \neq 0$. Диофантово уравнение $ax + by = c$ имеет решение в целых числах x, y тогда и только тогда, когда c делится на (a,b). Причем, если (x_0, y_0) – это одно из решений этого уравнения, то множество всех решений задается в виде $x = x_0 + \frac{b}{(a,b)}t, y = y_0 - \frac{a}{(a,b)}t$, где t пробегает множество всех целых чисел. Частное решение (x_0, y_0) можно найти с помощью алгоритма Евклида. Индукцией по числу переменных аналогичным образом можно решить линейное диофантово уравнение от n переменных.

Пусть $m_1,...,m_k$ – попарно взаимно простые натуральные числа, $c_1,...,c_k$ – целые числа, $m = m_1 \cdot ... \cdot m_k$, тогда множество решений системы сравнений $\begin{cases} x \equiv c_1(\mathrm{mod}\, m_1) \\ ..... \\ x \equiv c_k(\mathrm{mod}\, m_k) \end{cases}$ имеет вид $x \equiv c_1x_1\frac{m}{m_1} + ... + c_kx_k\frac{m}{m_k}(\mathrm{mod}\, m)$, где x_i – произвольное целое число, удовлетворяющее сравнению $x_i\frac{m}{m_i} \equiv 1(\mathrm{mod}\, m_i)$ (*китайская теорема об остатках*).

§3. Функция Эйлера, теоремы Эйлера и Ферма. RSA-криптосистема. Пусть m – натуральное число, большее 1. Количество натуральных чисел, меньших m, которые взаимно просты с m, обозначим $\varphi(m)$. Функция φ называется *функцией Эйлера*. По определению полагают $\varphi(1) = 1$. Функция Эйлера мультипликативна, т.е. $\varphi(mn) = \varphi(m)\varphi(n)$ для любых взаимно простых натуральных чисел m, n. Пусть

$p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ – это каноническое разложение числа m, тогда

$$\varphi(m) = m\left(1-\frac{1}{p_1}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right) = p_1^{a_1-1}\cdot\ldots\cdot p_k^{a_k-1}\cdot(p_1-1)\cdot\ldots\cdot(p_k-1).$$

Пусть m – натуральное число, a – целое число, $(a,m)=1$, тогда $a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$ (*теорема Эйлера*).

Следствием теоремы Эйлера является *теорема Ферма*: пусть p – простое число, a – целое число, $(a,p)=1$, тогда $a^{p-1} \equiv 1(\mathrm{mod}\, p)$. Впрочем теорему Ферма можно сформулировать иначе:

пусть p – простое число, a – целое число, тогда $a^p \equiv a(\mathrm{mod}\, p)$.

Криптосистема с открытым ключом (RSA-криптосистема). Пусть абоненты А и В решили организовать для себя возможность секретной переписки. Для этого каждый из них независимо друг от друга выбирает два различных больших простых числа, а именно,

А: p_A, q_A;

В: p_B, q_B.

Пусть $m_A = p_A q_A, m_B = p_B q_B$.

Абонент А выбирает случайное число e_A такое, что $0 < e_A < \varphi(m_A)$, НОД$(e_A, \varphi(m_A)) = 1$. Абонент В выбирает случайное число e_B такое, что $0 < e_B < \varphi(m_B)$, НОД$(e_B, \varphi(m_B)) = 1$.

Абонент А вычисляет d_A такое, что $0 < d_A < \varphi(m_A)$, $d_A e_A \equiv 1(\mathrm{mod}\varphi(m_A))$. Абонент В вычисляет d_B такое, что $0 < d_B < \varphi(m_B)$, $d_B e_B \equiv 1(\mathrm{mod}\varphi(m_B))$.

Затем А и В делают общедоступными следующие книги паролей:

А: e_A, m_A;

В: e_B, m_B.

Теперь можно отправлять конфиденциальные сообщения абонентам А или В.

Например, если пользователь книги паролей хочет отправить сообщение x для А, то он поступает следующим образом:

используует *открытый ключ* e_A из книги паролей,

вычисляет $x_1 \equiv x^{e_A}(\mathrm{mod}\, m_A)$,

отправляет сообщение x_1 абоненту А.

Абонент А для дешифровки сообщения x_1 использует *секретный ключ* d_A и вычисляет $x_1^{d_A}$. Используя теорему Эйлера, несложно проверить, что это и будет переданное сообщение *x*.

Корректность работы такой криптосистемы основана на том, что фактически требуется, чтобы $\text{НОД}(x, m_A) = 1$. Но вероятность того, что случайно взятое число *x* не является таковым, ничтожна мала при больших значениях m_A.

Криптосистема без передачи ключей. Пусть абоненты А и В условились организовать между собой секретную переписку. Для этого они выбирают достаточно большое простое число p.

Абоненты А и В выбирают себе секретные ключи e_A и e_B соответственно такие, что $0 < e_A < p-1,\ \text{НОД}(e_A, p-1) = 1,\ 0 < e_B < p-1,\ \text{НОД}(e_B, p-1) = 1.$

Затем абоненты А и В находят вторые секретные ключи d_A и d_B соответственно такие, что $0 < d_A < p-1,\ e_A d_A \equiv 1 (\text{mod}\, p-1),\ 0 < d_B < p-1,\ e_B d_B \equiv 1 (\text{mod}\, p-1).$

Пересылаемые сообщения разбиваются на части, меньшие $p-1$.

Предположим, абонент А решил отправить сообщение *x* абоненту В.

Для этого абонент А вычисляет $x_1 \equiv x^{e_A} (\text{mod}\, p)$ и отправляет абоненту В сообщение x_1.

Абонент В вычисляет $x_2 \equiv x_1^{e_B} (\text{mod}\, p)$ и отправляет абоненту А сообщение x_2.

Абонент А вычисляет $x_3 \equiv x_2^{d_A} (\text{mod}\, p)$ и отправляет абоненту В сообщение x_3.

Абонент В вычисляет $x_4 \equiv x_3^{d_B} (\text{mod}\, p)$, а это и есть переданное сообщение *x*.

Доказательство этого факта основано на теореме Ферма. Корректность работы такой криптосистемы аналогична работе криптосистемы с открытым ключом.

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

Приведем основные свойства показателей:

1) числа $1, a^1, ..., a^{n-1}$ попарно не сравнимы по модулю *m*;
2) $a^{k_1} \equiv a^{k_2} (\text{mod}\, m)$ тогда и только тогда, когда $k_1 \equiv k_2 (\text{mod}\, n)$;
3) $\varphi(m)$ делится на *n*;
4) если *bc* – показатель, которому принадлежит число *x* по модулю *m*, то *b* – показатель, которому принадлежит число x^c по модулю *m*;

5) пусть a – показатель, которому принадлежит число x по модулю m; b – показатель, которому принадлежит число y по модулю m, причем числа a и b взаимно простые, тогда ab – показатель, которому принадлежит число xy по модулю m.

§5. Простые числа. Числа вида $f_n = 2^{2^n} + 1$, $M_n = 2^n - 1$ называются соответственно числами Ферма и Мерсенна. При любом $n \geq 1$ на отрезке $[n, 2n]$ можно найти хотя бы одно простое число (*постулат Бертрана*). Если натуральные числа a и m взаимно просты, то бесконечная арифметическая прогрессия $a + mt,\ t \in Z$, содержит бесконечно много простых чисел (*теорема Дирихле*). Обозначим через p_n – n-е простое число в ряду натуральных чисел, $\pi(n)$ – количество простых чисел, не превосходящих числа n. Б. Риман доказал, что $\pi(n) \sim \frac{n}{\ln n}$, т.е. $\lim_{n\to\infty} \frac{\pi(n) \ln n}{n} = 1$. Известно, что существуют две положительные постоянные c и d такие, что для любого натурального n выполняются неравенства $cn \ln n < p_n < dn \ln n$. В. Серпинский доказал следующую формулу для n-го простого числа: $p_n = \left[10^{2^n}\alpha\right] - 10^{2^{n-1}}\left[10^{2^{n-1}}\alpha\right]$, где $\alpha = \sum_{i=1}^{\infty} p_i 10^{-2^i}$.

Пусть n – натуральное число, большее 1. Число n является простым тогда и только тогда, когда $(n-1)! + 1$ делится на n (*теорема Вильсона*). Число Мерсенна M_n, $n \geq 3$, является простым тогда и только тогда, когда n - простое число и $L_{n-2} \equiv 0 (mod\ M_n)$, где $L_0 = 4$, $L_{k+1} \equiv L_k^2 - 2 (mod\ M_n)$, $k \geq 0$ (*критерий Люка-Лемера*).

Задачи

1. Найдите наибольшее возможное число шагов алгоритма Евклида для двух трёхзначных чисел.

2. Докажите, что для любого натурального $n > 1$ существует простое $p \in [n, n!]$.

3. Докажите, что для любых натуральных m, n ($m \neq n$) числа Ферма $f_m = 2^{2^m} + 1$, $f_n = 2^{2^n} + 1$ взаимно просты.

4. Существует ли многочлен с целыми коэффициентами от целой переменной, значениями которого могут быть только простые числа или им противоположные?

5. Решить систему сравнений $5x \equiv 8 (mod\ 12)$, $7x \equiv 16 (mod\ 18)$, $11x \equiv 8 (mod\ 42)$.

6. Используя теорему Эйлера и китайскую теорему об остатках, найти остаток от деления числа 5^{509}на 1323.

7. Доказать, что для любого нечетного натурального n число $2^{n!} - 1$ делится на n.

8. Натуральные числа a, b взаимно просты, p – простое число вида $4k + 3$. Доказать, что число $a^2 + b^2$ не делится на p.

9. Доказать, что существует бесконечно много простых чисел вида $4k + 1$ и вида $4k + 3$.

10. Пусть p, q – простые числа, $2^p \equiv 1 (\mathrm{mod}\, q)$. Докажите, что $q \equiv 1 (\mathrm{mod}\, p)$.

11. Докажите, что любой натуральный делитель d числа Ферма $f_n = 2^{2^n} + 1$ имеет вид $d = 2^{n+1}x + 1,\ x \in N \cup \{0\}$. Доказать, что f_5 делится на 641.

12. Докажите, что не существует натурального числа n, большего 1, такого, что $n \mid 2^n - 1$.

13. Пусть натуральное число a принадлежит показателю δ по модулю m. Для любого натурального числа γ найдите показатель, которому принадлежит число a^γ по модулю m.

14. Докажите, что для любого простого числа p и любого целого числа a сравнение $x^x \equiv a(\mathrm{mod}\, p)$ разрешимо.

15. Доказать теорему Вильсона.

Задачи для самостоятельного решения

1. Решить систему сравнений $x \equiv 19(mod\ 30)$, $x \equiv 10(mod\ 21)$, $x \equiv 3(mod\ 28)$.

2. Найдите все нечетные натуральные n, такие, что $n \mid 3^n + 1$.

3. Пусть натуральное число a принадлежит показателю δ по модулю m. Для любого натурального числа γ найдите натуральное число, которое принадлежит показателю (δ, γ) по модулю m.

4. Найдите наибольшее возможное число шагов алгоритма Евклида с выбором наименьшего по модулю остатка (см. теорию) для двух четырехзначных чисел.

5. Найдите все простые числа $p \geq 3$ и целые числа x, y, удовлетворяющие уравнению $x^{p-1} + x^{p-2} + \ldots + x + 2 = y^2$.

6. Пусть *n* – натуральное число, большее 4. Докажите, что число *n* является простым тогда и только тогда, когда $(n-1)!$ не делится на *n*.

Решения задач

1. Найдите наибольшее возможное число шагов алгоритма Евклида для двух трёхзначных чисел.

►Пусть $a,\ b$ - натуральные числа, $100 \leq b < a \leq 999$. Пусть $d = (a,b)$ и на предпоследнем шаге алгоритма Евклида мы получили $a_{n-1} = q_{n-1} \cdot b_{n-1} + d$, при этом $d \mid b_{n-1}$ и $d < b_{n-1}$. Поэтому $b_{n-1} \geq 2d,\ a_{n-1} \geq 3d$. Далее $a_{n-2} = q_{n-2} \cdot b_{n-2} + b_{n-1}$. Здесь $b_{n-2} = a_{n-1} \geq 3d$, $a_{n-2} \geq 5d$. Таким образом, $b = b_1 \geq F_{n+1} \cdot d,\ a = a_1 \geq F_{n+2} \cdot d$, где F_k -

число Фибоначчи с номером k. Так как $a \le 999$, то $F_{n+2} \le 999$, отсюда находим, что $n+2 \le 15$. Число шагов алгоритма Евклида не превосходит 13. Оценка достигается в случае $a = F_{15} = 987,\ b = F_{14} = 610$:

$987 = 1 \cdot 610 + 377,\quad 610 = 1 \cdot 377 + 233$, $377 = 1 \cdot 233 + 144$, $144 = 1 \cdot 89 + 55$, $89 = 1 \cdot 55 + 34$, $55 = 1 \cdot 34 + 21$, $34 = 1 \cdot 21 + 13$, $21 = 1 \cdot 13 + 8$, $13 = 1 \cdot 8 + 5,$ $8 = 1 \cdot 5 + 3,\ 5 = 1 \cdot 3 + 2,\ 3 = 1 \cdot 2 + 1,\ 2 = 2 \cdot 1 + 0.$ ◄

2. Докажите, что для любого натурального $n > 1$ существует простое $p \in [n, n!]$.

►При $n = 2$ утверждение верно. Пусть $n \ge 3$. Допустим, все числа от n до $n!$ составные. Число $n!-1$ не делится ни на одно из чисел от 2 до n. Поэтому число $n!-1$ имеет простой делитель, больший n, следовательно, этот простой делитель принадлежит отрезку $[n, n!-1]$. Противоречие. ◄

3. Докажите, что для любых натуральных $m,\ n$ ($m \ne n$) числа Ферма $f_m = 2^{2^m} + 1,$ $f_n = 2^{2^n} + 1$ взаимно просты.

►Пусть $m > n$. Заметим, что

$$f_m - 2 = 2^{2^m} - 1 = (2^{2^{m-1}} + 1)(2^{2^{m-1}} - 1) = (2^{2^{m-1}} + 1)(2^{2^{m-2}} + 1)(2^{2^{m-2}} - 1) = \ldots = \prod_{i=1}^{m-1} f_i .$$

Если допустить, что $(f_m, f_n) = d \ge 2,$ то получим, что $d \mid f_m - 2,\ d \mid f_m \Rightarrow d \mid 2$, то есть $d = 2$, что невозможно, потому что числа Ферма нечётные. ◄

4. Существует ли многочлен с целыми коэффициентами от целой переменной, значениями которого могут быть только простые числа или им противоположные?

►Допустим, существует такой многочлен $f \in Z[x]$, $f(x) = \sum_{i=0}^{n} a_i x^i$, $a_n \ne 0$. Пусть $f(0) = \pm p$, p - простое число. Очевидно, что все числа $f(pt)$, $t \in Z$, делятся на p . И, следовательно, равны $\pm p$. Однако многочлен $f(x)$ принимает значения $\pm p$ не более, чем в $2n$ различных точках. Противоречие. Следовательно, такого многочлена не существует. ◄

5. Решить систему сравнений $5x \equiv 8 (mod\ 12)$, $7x \equiv 16 (mod\ 18)$, $11x \equiv 8 (mod\ 42)$.

► $\begin{cases} 5x \equiv 8 (\mathrm{mod}\, 12) \\ 7x \equiv 16 (\mathrm{mod}\, 18) \\ 11x \equiv 8 (\mathrm{mod}\, 42) \end{cases} \Leftrightarrow \begin{cases} x \equiv 4 (\mathrm{mod}\, 12) \\ x \equiv 10 (\mathrm{mod}\, 18) \\ x \equiv 16 (\mathrm{mod}\, 42) \end{cases} \Leftrightarrow$

$\begin{cases} x \equiv 4 (\mathrm{mod}\, 2^2), x \equiv 4 (\mathrm{mod}\, 3) \\ x \equiv 10 (\mathrm{mod}\, 2), x \equiv 10 (\mathrm{mod}\, 3^2) \\ x \equiv 16 (\mathrm{mod}\, 2), x \equiv 16 (\mathrm{mod}\, 3), x \equiv 16 (\mathrm{mod}\, 7) \end{cases} \Leftrightarrow \begin{cases} x \equiv 0 (\mathrm{mod}\, 2), x \equiv 0 (\mathrm{mod}\, 2^2) \\ x \equiv 1 (\mathrm{mod}\, 3), x \equiv 1 (\mathrm{mod}\, 3^2) \\ x \equiv 2 (\mathrm{mod}\, 7) \end{cases}$

$\Leftrightarrow \begin{cases} x \equiv 0 (\mathrm{mod}\, 2^2) \\ x \equiv 1 (\mathrm{mod}\, 3^2) \\ x \equiv 2 (\mathrm{mod}\, 7) \end{cases}$.

$7 \cdot 9 \cdot x_1 \equiv 1 (\mathrm{mod}\, 4), \quad 4 \cdot 7 \cdot x_2 \equiv 1 (\mathrm{mod}\, 9), \quad 4 \cdot 9 \cdot x_3 \equiv 1 (\mathrm{mod}\, 7) \Rightarrow x_1 = -1, \quad x_2 = 1$, $x_3 = 1$. Поэтому $x \equiv 0 \cdot (-1) \cdot 7 \cdot 9 + 1 \cdot 1 \cdot 4 \cdot 7 + 2 \cdot 1 \cdot 4 \cdot 9 (\mathrm{mod}\, 4 \cdot 9 \cdot 7)$, $x \equiv 100 (\mathrm{mod}\, 252)$. ◄

6. Используя теорему Эйлера и китайскую теорему об остатках, найти остаток от деления числа 5^{509} на 1323.

► $x \equiv 5^{509} (\mathrm{mod}\, 1323) \Leftrightarrow \begin{cases} x \equiv 5^{509} (\mathrm{mod}\, 27) \\ x \equiv 5^{509} (\mathrm{mod}\, 49) \end{cases} \Leftrightarrow \begin{cases} x \equiv 5^5 (\mathrm{mod}\, 27) \\ x \equiv 5^5 (\mathrm{mod}\, 49) \end{cases} \Leftrightarrow$

$\begin{cases} x \equiv 20 (\mathrm{mod}\, 27) \\ x \equiv 38 (\mathrm{mod}\, 49) \end{cases}$

Так как $49x_1 \equiv 1 (\mathrm{mod}\, 27) \Leftrightarrow x_1 \equiv 16 (\mathrm{mod}\, 27)$, $27x_2 \equiv 1 (\mathrm{mod}\, 49) \Leftrightarrow x_2 \equiv 20 (\mathrm{mod}\, 49)$, то $x \equiv 20 \cdot 16 \cdot 49 + 38 \cdot 20 \cdot 27 = 20 \cdot 1810 \equiv 479 (\mathrm{mod}\, 1323)$. ◄

7. Доказать, что для любого нечетного натурального n число $2^{n!} - 1$ делится на n.

► Так как $\varphi(n) < n$, то $\varphi(n) \mid n!$. Применяя теорему Эйлера, получим, что $2^{n!} = (2^{\varphi(n)})^{n!/\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$. ◄

8. Натуральные числа a, b взаимно просты, p – простое число вида $4k + 3$. Доказать, что число $a^2 + b^2$ не делится на p.

► Допустим, что $a^2 + b^2 \equiv 0 (\mathrm{mod}\, p)$. Возведя обе части сравнения $a^2 \equiv -b^2 (\mathrm{mod}\, p)$ в степень $(p-1)/2$, получим, что $a^{p-1} \equiv -b^{p-1} (\mathrm{mod}\, p)$. Используя малую теорему Ферма и условие $p \geq 3$, заключаем, что $a \equiv b \equiv 0 (\mathrm{mod}\, p)$, что противоречит условию $(a,b) = 1$. ◄

9. Доказать, что существует бесконечно много простых чисел вида $4k + 1$ и вида $4k + 3$.

►1) Допустим, что существует лишь конечное число простых чисел $p_1,\ p_2,...,\ p_n$ вида $4k+1$. Рассмотрим число $N=4p_1^2...p_n^2+1$. Оно является составным, все простые делители числа N имеют вид $4k+3$. Пусть $p=4k+3$ – простой делитель числа N. Тогда $(2p_1...p_n)^2\equiv -1(\mathrm{mod}\,p)$. Возведя обе части сравнения в степень $(p-1)/2$, получим $(2p_1...p_n)^{p-1}\equiv -1(\mathrm{mod}\,p)$, что противоречит теореме Ферма.

2) Допустим, что существует лишь конечное число простых чисел $p_1,\ p_2,...,\ p_n$ вида $4k+3$. Число $N=4p_1...p_n+3$ не является простым числом и не делится ни на одно из чисел $p_1,\ p_2,...,\ p_n$. Поэтому все простые делители числа N имеют вид $4k+1$, но тогда число N при делении на 4 должно давать остаток 1. Противоречие.◄

10. Пусть *p, q* – простые числа, $2^p\equiv 1(\mathrm{mod}\,q)$. Докажите, что $q\equiv 1(\mathrm{mod}\,p)$.

► Пусть r - показатель, которому принадлежит число 2 по модулю q, тогда $r\mid p$. Очевидно, $r>1$, следовательно, $r=p$. Также $r\mid \varphi(q)=q-1$. Значит $q\equiv 1(\mathrm{mod}\,p)$.◄

11. Докажите, что любой натуральный делитель d числа Ферма $f_n=2^{2^n}+1$ имеет вид $d=2^{n+1}x+1,\ x\in N\cup\{0\}$. Доказать, что f_5 делится на 641.

► Пусть q - произвольный простой делитель числа f_n, тогда $2^{2^n}\equiv -1(\mathrm{mod}\,q)$, следовательно, $2^{2^{n+1}}\equiv 1(\mathrm{mod}\,q)$. Пусть δ - показатель, которому принадлежит число 2 по модулю q, тогда $\delta\mid 2^{n+1}$. Если предположить, что $\delta=2^k$, где $k\le n$, то получим, что $2^{2^n}=(2^\delta)^{2^n/\delta}\equiv 1(\mathrm{mod}\,q)$. Поэтому $\delta=2^{n+1}$. Так как $2^{q-1}\equiv 1(\mathrm{mod}\,q)$, то $\delta=2^{n+1}\mid q-1$. Таким образом, любой простой делитель числа f_n имеет вид $2^{n+1}t+1$, $t\in N$. Очевидно, что конечное произведение чисел вида $2^{n+1}t+1$ есть число вида $2^{n+1}t+1$.

Покажем, что f_5 делится на простое число $641=2^6\cdot 10+1$. Воспользуемся тождеством $641=2^4+5^4=5\cdot 2^7+1$.

Действительно, $2^{32}=2^4\cdot(2^7)^4\equiv -5^4\cdot(2^7)^4=-(5\cdot 2^7)^4\equiv -(-1)^4=-1(\mathrm{mod}\,641)$.◄

12. Докажите, что не существует натурального числа n, большего 1, такого, что $n\mid 2^n-1$.

► Допустим, существует такое $n>1$. Очевидно, n нечётное. Пусть p - наименьший простой делитель числа n. Обозначим через δ показатель, которому принадлежит число 2 по модулю p. Так как $p\mid 2^n-1,\ p\mid 2^{p-1}-1$, то $\delta\mid n$ и $\delta\mid p-1$. Так как $\delta\mid p-1$, то

существует простое q, $q < p$, $q \mid \delta$. Тогда $q \mid n$, что противоречит минимальности p. ◄

13. Пусть натуральное число a принадлежит показателю δ по модулю m. Для любого натурального числа γ найдите показатель, которому принадлежит число a^{γ} по модулю m.

► Обозначим через β показатель, которому принадлежит число a^{γ} по модулю m. Тогда $a^{\gamma\beta} \equiv 1(\mathrm{mod}\, m)$. Следовательно, $\delta \mid \gamma\beta$. Пусть $d = (\gamma, \delta)$, $\gamma = d\gamma_1$, $\delta = d\delta_1$, тогда $\delta_1 \mid \beta\gamma_1$. Так как $(\gamma_1, \delta_1) = 1$, то $\delta_1 \mid \beta$. Поэтому $\beta \geq \delta_1 = \dfrac{\delta}{(\gamma, \delta)}$. С другой стороны, $(a^{\gamma})^{\delta_1} = a^{[\gamma,\delta]} = (a^{\delta})^t \equiv 1(\mathrm{mod}\, m)$. Следовательно, $\beta = \dfrac{\delta}{(\gamma, \delta)}$. ◄

14. Докажите, что для любого простого числа p и любого целого числа a сравнение $x^x \equiv a(\mathrm{mod}\, p)$ разрешимо.

► В силу китайской теоремы об остатках существует целое x, такое, что

$\begin{cases} x \equiv a(\mathrm{mod}\, p) \\ x \equiv 1(\mathrm{mod}\, p-1) \end{cases}$. Тогда $x^x \equiv a^x = a^{1+t(p-1)} = a \cdot (a^{p-1})^t \equiv a(\mathrm{mod}\, p)$. Легко видеть, что одним из решений исходного сравнения является $x = p + a - ap$. ◄

15. Доказать теорему Вильсона.

► **Необходимость.** Пусть p - простое число. Для любого $a \in \{1, \ldots, p-1\}$ существует единственное $x \in \{1, \ldots, p-1\}$ такое, что $ax \equiv 1(mod\, p)$. Все числа от 2 до $p-2$ разбиваются на пары (a, b), для которых $ab \equiv 1(mod\, p)$. Поэтому $(p-1)! \equiv p - 1(mod\, p)$ **Достаточность.** Допустим, что n – составное, тогда существуют натуральные числа a, b, большие 1, такие, что $n = a \cdot b$. Так как $a \mid n$, то $a \mid (n-1)! + 1$. Поскольку $a \leq n - 1$, то $a \mid 1$, что невозможно.◄