Семинар 6 Вычеты

Малая теорема Ферма. Для любого простого p и любого целого a, не делящегося на p, справедливо сравнение

$$a^{p-1} \equiv 1 \pmod{p}.$$

Теорема Эйлера. Для любых взаимно простых $a, n \in \mathbb{Z}$ справедливо сравнение

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

где $\varphi(n)$ — это количество целых чисел от 1 до n, взаимно простых с n (функция Эйлера).

Китайская теорема об остатках. Пусть заданы произвольные попарно взаимно простые целые числа $m_1, \ldots, m_n$ и произвольные целые числа $a_1, \ldots, a_n$. Тогда

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv a_n \pmod{m_n} \end{cases} \iff x \equiv \sum_{i=1}^{n} x_i M_i \pmod{M},$$

где $M = \prod_{j=1}^{n} m_j$, $M_i = M/m_i$, x_i — решение сравнения $x_i M_i \equiv a_i \pmod{m_i}$, $i = 1, \ldots, n$.

6.1. Решите сравнения:

а) $8x \equiv 3 \pmod{13}$;
б) $17x \equiv 1 \pmod{37}$;
в) $7x \equiv 2 \pmod{11}$;
г) $80x \equiv 17 \pmod{169}$.

6.2. Решите сравнение $79x + 32y \equiv 1 \pmod{17}$.

6.3. Докажите, что существует бесконечно много натуральных чисел, не представимых в виде суммы а) двух б) трех квадратов целых чисел.

6.4. Докажите, что если длины сторон прямоугольного треугольника суть целые числа, то хотя бы одна из них кратна пяти, а длина хотя бы одного из катетов кратна трём.

6.5. Найдите

а) последнюю цифру числа $7^{7^{7}}$;
б) остаток от деления числа 2^{2011} на 17;
в) остаток от деления $12^{12^{12}}$ на 2010.

6.6. Докажите, что $2222^{5555} + 5555^{2222}$ делится на 7.

6.7. Докажите, что если p — простое число, то

а) для любых целых a и b справедливо сравнение $(a+b)^p \equiv a^p + b^p \pmod{p}$;
б) для любого многочлена $f(x) \in \mathbb{Z}[x]$ и любого целого a справедливо сравнение

$$(f(a))^p \equiv f(a^p) \pmod{p}.$$

6.8. Докажите, что если при простом p и натуральном n справедливо сравнение $a \equiv b \pmod{p^n}$, то справедливо и сравнение $a^p \equiv b^p \pmod{p^{n+1}}$.

6.9. Теорема Вильсона. Докажите, что для любого простого p справедливо сравнение

$$(p-1)! \equiv -1 \pmod{p}.$$

6.10. Обращение теоремы Вильсона. Докажите, что если $n > 1$ и

$$(n-1)! \equiv -1 \pmod{n},$$

то n — простое число.

6.11. Теорема Лейбница. Докажите, что число p является простым тогда и только тогда, когда

$$(p-2)! \equiv 1 \pmod{p}.$$

6.12. Теорема Клемента. Докажите, что числа p и $p+2$ являются простыми (то есть *простыми числами-близнецами*) тогда и только тогда, когда

$$4((p-1)!+1)+p \equiv 0 \pmod{p^2+2p}.$$

6.13. Критерий Кармайкла (в одну сторону). Пусть натуральное число n является произведением s различных простых чисел: $n = p_1 \dots p_s$. Пусть также для каждого i выполняется сравнение $n-1 \equiv 0 \pmod{p_i-1}$. Докажите, что для любого целого a, взаимно простого с n, справедливо сравнение $a^{n-1} \equiv 1 \pmod{n}$ (составное n, обладающее таким свойством, называется *числом Кармайкла*).

6.14. Докажите, что если p — нечётный простой делитель числа n^2+1, то $p \equiv 1 \pmod{4}$. Выведите отсюда бесконечность множества простых чисел вида $4k+1$.

6.15. Докажите, что если p — простой делитель числа $n^4+n^3+n^2+n+1$ и $p > 5$, то справедливо сравнение $p \equiv 1 \pmod{5}$. Выведите отсюда бесконечность множества простых чисел вида $5k+1$.

6.16. Докажите, что если p — простой делитель числа n^2+n+1 и $p > 3$, то $p \equiv 1 \pmod{6}$. Выведите отсюда бесконечность множества простых чисел вида $6k+1$.

6.17. Пусть p — простое число. Докажите, что если $p = 4k+1$, то p делит $((2k)!)^2+1$, а если $p = 4k-1$, то p делит $((2k-1)!)^2-1$.

6.18. Решите в целых числах уравнения

а) $n^2-n-4 \equiv 0 \pmod{17}$; б) $n^2-n-4 \equiv 0 \pmod{289}$; в) $n^2+3n+1 \equiv 0 \pmod{55}$.

6.19. Пусть заданы произвольные попарно взаимно простые целые числа $m_1, \dots, m_n$. Докажите, что число $(m_2 m_3 \dots m_n)^{\varphi(m_1)}$ удовлетворяет системе сравнений

$$\begin{cases} x \equiv 1 \pmod{m_1} \\ x \equiv 0 \pmod{m_2} \\ \dots\dots\dots\dots\dots \\ x \equiv 0 \pmod{m_n} \end{cases}$$

Выведите отсюда китайскую теорему об остатках.

6.20. Решите системы сравнений:

а) $\begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 8 \pmod{17} \end{cases}$; б) $\begin{cases} 3x \equiv 5 \pmod{10} \\ 5x \equiv 3 \pmod{19} \end{cases}$; в) $\begin{cases} x \equiv 1 \pmod{15} \\ x \equiv 2 \pmod{16} \\ x \equiv 3 \pmod{17} \end{cases}$

6.21. Найдите остаток от деления

а) 17^{30} на 77; б) 19^{79} на 144.

6.22*. Больное войско. Генерал хочет построить для парада своих солдат в одинаковые каре (так называется боевой порядок пехоты, построенной в виде квадрата), но не знает, сколько солдат находится в лазарете, знает лишь, что их там не более 37 человек. Докажите, что у генерала войско может быть такого размера, что он, независимо от количества больных солдат, сумеет выполнить своё намерение.

6.23* Докажите для произвольных натуральных $a_1, \dots, a_m$ сравнение $a_1^{a_2^{\cdot^{\cdot^{\cdot^{a_m^{a_{m-1}}}}}}} \equiv a_1^{a_2^{\cdot^{\cdot^{\cdot^{a_{m-1}}}}}} \pmod{m}$.

6.24 Аналог Малой теоремы Ферма для $\mathbb{Z}[i]$.** Множество $\mathbb{Z}[i]$ всех комплексных чисел $a+bi$ с целыми a и b называется *кольцом целых гауссовых чисел*. Пусть $z = a+bi$ — простое целое гауссово число (т.е. не имеющее в $\mathbb{Z}[i]$ никаких делителей, кроме ± 1, $\pm i$, $\pm z$, $\pm iz$). Докажите, что для любого $w \in \mathbb{Z}[i]$ справедливо сравнение

$$w^{a^2+b^2} \equiv w \pmod{z}.$$