Семінар 25. Мала теорема Ферма.
20.04.2019

Мала теорема Ферма.

a) Доведіть, що якщо модуль - простий, то в кожній строчці і в кожному стовпчику таблиці множення залишків всі числа різні. (Тобто кожна строчка таблиці містить всі ненульові залишки, переставлені в якомусь порядку.)

b) Доведіть, що якщо p – просте число, і $p > a > 0$, то:

$$a \times 2a \times 3a \times \ldots \times (p-1)a \equiv (p-1)!\ (mod\ p)$$

c) Ферма. Якщо p – просте число і a не ділиться на p, то $a^{p-1} \equiv 1\ (mod\ p)$.

1. Знайдіть залишок від ділення А) 3^{102} на 101; Б) 8^{900} на 29.

2. Доведіть, що А) $7^{120} - 1$ ділиться на 143. Б) $3^{3000} - 1$ ділиться на 1001.

3. Доведіть, що число $30^{239} + 239^{30}$ — складене.

4. Доведіть, що для складеного числа 561 справедливий аналог малої теореми Ферма: якщо $(a, 561) = 1$, то виконується порівняння $a^{560} \equiv 1 (mod\ 561)$. Числа, які мають таку властивість, називаються числами Кармайкла.

5. Доведіть, що сума $1^{100} + 2^{100} + \ldots + 100^{100} + 1$ ділиться на 101.

6. Відомо, що $a^{12} + b^{12} + c^{12} + d^{12} + e^{12} + f^{12}$ ділиться на 13. Доведіть, що $abcdef$ ділиться на 13^6.

7. Сума трьох чисел a, b і c ділиться на 30. Доведіть, що $a^5 + b^5 + c^5$ також ділиться на 30.

8. Нехай n – натуральне число, не кратне 17. Доведіть, що або $n^8 + 1$, або $n^8 - 1$ ділиться на 17.

9. Доведіть, що $\underbrace{111\ldots1}_{12}$ ділиться на 13.

10. Нехай $p > 2$ — просте число. Доведіть, що $7^p - 5^p - 2$ ділиться на $6p$.

11. Нехай p - просте число. Доведіть, що $(a + b)^p \equiv a^p + b^p\ (mod\ p)$ для будь-яких цілих a і b.

12. Нехай p і q – різні прості числа. Доведіть, що $p^q + q^p \equiv p + q\ (mod\ pq)$.

13. Доведіть, що якщо $x^2 + 1$ ділиться на непарне просте p, то $p = 4k + 1$. За допомогою цього факту, доведіть, що існує нескінченно багато простих чисел вигляду $p = 4k + 1$.

Для задоволення

14. Теорема Ойлера. Нехай $m \geq 1$ і $(a,\ m) = 1$. Тоді має місце порівняння $a^{\varphi(m)} \equiv\ 1\ (mod\ m)$.

15. Нехай p - просте число, і а не ділиться на р. Доведіть, що знайдеться натуральне число b, для якого $ab \equiv 1(mod\ p)$.

16. Доведіть, що якщо число $n! + 1$ ділиться на $n + 1$, то $n + 1$ — просте число.

17. Теорема Вільсона. Доведіть, що для простого p вірно:

$$(p - 1)!\ \equiv -1(mod\ p).$$

18. Дано просте p і ціле a, яке не ділиться на p. Нехай k — найменше натуральне число, таке що $a^k \equiv 1(mod\ p)$. Доведіть, що p - 1 ділиться на k.

19. Доведіть, що ні при якому цілому k число $k^2 + k + 1$ не ділиться на 101.