8В, спецкурс, занятие 18

26 января 2024

Малая теорема Ферма

Теорема (Малая теорема Ферма)**.** Пусть p — простое число и a не делится на p. Тогда $a^{p-1} \equiv 1 \pmod p$.

Эквивалентная формулировка: $a^p \equiv a \pmod p$ для простого p и произвольного a.

Доказательство 1. Рассмотрим всевозможные ненулевые остатки от деления на p:

$$1,\ 2,\ 3,\ \ldots,\ p-1.$$

Домножим их на a:

$$a,\ 2a,\ 3a,\ \ldots,\ (p-1)a.$$

Поскольку $\text{НОД}(a, p) = 1$, то, как было доказано на прошлой лекции, все эти числа дают разные (и ненулевые) остатки по модулю p. Поскольку их ровно $p-1$, то они дают все остатки $1,\ 2,\ \ldots,\ p-1$ по одному разу. Перемножим и получим:

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod p$$

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod p$$

Поскольку $(p-1)!$ взаимно просто с p, то можно сократить сравнение на $(p-1)!$ и получить требуемое:

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

Доказательство 2. Решим следующую комбинаторную задачу:

На карусели p одинаковых сидений. У маляра есть a красок. Сколькими способами он может раскрасить сидения карусели, если раскраски, переходящие друг в друга при повороте, считаются одинаковыми?

Сначала закрепим карусель на месте. Есть a^p способов покрасить ее сидения (по a вариантов для каждого из p сидений). Теперь пусть карусель вращается. Большую часть раскрасок мы посчитали по p раз (например, при $p = 5$ раскраски КЖКЗС, ЖКЗСК, КЗСКЖ, ЗСКЖК, СКЖКЗ считаются одинаковыми).

Исключение составляют только одноцветные раскраски (их a штук), которые мы посчитали по одному разу. Вычтем их, поделим на p и добавим обратно. Получится

$$\frac{a^p - a}{p} + a \text{ раскрасок.}$$

Поскольку количество раскрасок обязательно должно быть целым, то $a^p - a \vdots p$ и следовательно $a^p \equiv a \pmod p$.

Замечание. Очень важно, что p — простое число. Если, например, $p = 6$, то у нас есть раскраски, которые мы считали 6 раз (например, КОЖЗСФ), есть раскраски, которые мы считали по 3 раза (КЖЗКЖЗ), раскраски, которые мы считали по 2 раза (КЗКЗКЗ) и одноцветные раскраски, которые мы считали по 1 разу. Вычислить общее число раскрасок в этом случае заметно сложнее.

1 Найдите остатки от деления:
a$^{\vee}$ 2^{100} на 101; b$^{\vee}$ 7^{102} на 101; c$^{\vee}$ 8^{900} на 29; d$^{\vee}$ 3^{2023} на 43;
e 220^{1543} на 43; f 4^{1111} на 112.
Подсказка: в пункте f найдите отдельно остатки от деления на 16 и на 7.

2$^{\vee}$ Какой остаток при делении на простое p дает сумма $1^{p-1}+2^{p-1}+3^{p-1}+\cdots+(p-1)^{p-1}$?

3 Найдите все такие простые p, что $5^{p^2}+1$ делится на p.

4 Числа p и q — различные простые, а число n не делится ни на p, ни на q. Докажите, что $n^{(p-1)(q-1)}-1$ делится на pq.

5 Числа p и q — различные простые. Докажите, что $p^q+q^p\equiv p+q \pmod{pq}$.

6 Число $p>2$ простое. Докажите, что 7^p-5^p-2 делится на $6p$.

7 Пусть $p>5$ — простое число. Докажите, что $\underbrace{111\ldots11}_{p-1 \text{ единиц}}$ делится на p.

8 Простое число p дает остаток 3 от деления на 4. Докажите, что если a^2+b^2 делится на p, то числа a и b сами делятся на p.

9* Число $p>2$ простое и a не делится на p.
a Докажите, что $a^{\frac{p-1}{2}}\equiv 1 \pmod{p}$ или $a^{\frac{p-1}{2}}\equiv -1 \pmod{p}$.
b Докажите, что если $a^{\frac{p-1}{2}}\equiv -1 \pmod{p}$, то сравнение $x^2\equiv a \pmod{p}$ не имеет решений.

Такие числа a, для которых сравнение $x^2\equiv a \pmod{p}$ имеет два решения, называются *квадратичными вычетами*. А те числа, для которых сравнение $x^2\equiv a \pmod{p}$ не имеет решений называются *квадратичными невычетами*.

c Докажите, что из $p-1$ ненулевых остатков по модулю p ровно половина является квадратичными вычетами, а другая половина — квадратичными невычетами.
d Выведите из этого, что если $a^{\frac{p-1}{2}}\equiv 1 \pmod{p}$, то сравнение $x^2\equiv a \pmod{p}$ имеет два решения.