Квадратичные вычеты

группа 10-2

7.11.16

Определение. Пусть $m > 1$ — натуральное число и a — целое число, взаимно простое с m. Число a называется квадратичным вычетом по модулю m, если существует $x \in \mathbb{N}$ такое, что $a \equiv x^2 \ (mod\ m)$. В противном случае число a называется квадратичным невычетом по модулю m.

1. Докажите, что если p — нечетное простое число, то по модулю p существует ровно $\frac{p-1}{2}$ квадратичных вычетов и столько же невычетов.

Таким образом можно сделать вывод, что квадратичное сравнение вида $x^2 \equiv a \ (mod\ p)$ при простых p имеет либо ноль решений, либо два решения, либо одно решение в случае $a \equiv 0 \ (mod\ p)$.

2. Приведите пример чисел a и m таких, что сравнение $x^2 \equiv a \ (mod\ m)$ имеет больше двух решений.

Далее мы будем считать, что p — простое нечетное число.

3. Докажите, что для данного модуля p
(a) произведение двух квадратичных вычетов — вычет;
(b) произведение вычета на невычет — невычет;
(c) произведение двух невычетов — вычет.

4. **(a)** Докажите, что если a — квадратичный вычет по модулю p, то $a^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$.
(b) Докажите, что если a — квадратичный невычет по модулю p, то $a^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$.

5. Решите сравнение $ax^2 + bx + c \equiv 0 \ (mod\ p)$, где $a \not\equiv 0 \ (mod\ p)$.

6. Докажите, что сравнение $1 + x^2 + y^2 \equiv 0 \ (mod\ p)$ имеет хотя бы одно решение.

Определение. *Символом Лежандра* называется выражение, обозначаемое $(\frac{a}{p})$, равное 1, если a — квадратичный вычет по модулю p; -1, если a — невычет по модулю p и 0, если a кратно p.

Из задачи 4 следует, что $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \ (mod\ p)$.

7. **(a)** При каких p вычет -1 является квадратичным вычетом по модулю p?
(b) (Теорема Жирара.) Пусть $x^2 + y^2$ делится на простое число $p = 4k + 3$. Докажите тогда, что x и y делятся на p.

8. **(a)** Докажите, что многочлен $x^4 + 4$ — приводим над $\mathbb{Z}$.
(b) Докажите, что многочлен $x^2 + 1$ — приводим над $\mathbb{Z}_p$ при $p = 4k + 1$.
(c) Докажите, что многочлен $x^4 + 1$ — приводим над $\mathbb{Z}_p$ при любом p.

Квадратичные вычеты

группа 10-2

7.11.16

Определение. Пусть $m > 1$ — натуральное число и a — целое число, взаимно простое с m. Число a называется квадратичным вычетом по модулю m, если существует $x \in \mathbb{N}$ такое, что $a \equiv x^2 \ (mod\ m)$. В противном случае число a называется квадратичным невычетом по модулю m.

1. Докажите, что если p — нечетное простое число, то по модулю p существует ровно $\frac{p-1}{2}$ квадратичных вычетов и столько же невычетов.

Таким образом можно сделать вывод, что квадратичное сравнение вида $x^2 \equiv a \ (mod\ p)$ при простых p имеет либо ноль решений, либо два решения, либо одно решение в случае $a \equiv 0 \ (mod\ p)$.

2. Приведите пример чисел a и m таких, что сравнение $x^2 \equiv a \ (mod\ m)$ имеет больше двух решений.

Далее мы будем считать, что p — простое нечетное число.

3. Докажите, что для данного модуля p
(a) произведение двух квадратичных вычетов — вычет;
(b) произведение вычета на невычет — невычет;
(c) произведение двух невычетов — вычет.

4. **(a)** Докажите, что если a — квадратичный вычет по модулю p, то $a^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$.
(b) Докажите, что если a — квадратичный невычет по модулю p, то $a^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$.

5. Решите сравнение $ax^2 + bx + c \equiv 0 \ (mod\ p)$, где $a \not\equiv 0 \ (mod\ p)$.

6. Докажите, что сравнение $1 + x^2 + y^2 \equiv 0 \ (mod\ p)$ имеет хотя бы одно решение.

Определение. *Символом Лежандра* называется выражение, обозначаемое $(\frac{a}{p})$, равное 1, если a — квадратичный вычет по модулю p; -1, если a — невычет по модулю p и 0, если a кратно p.

Из задачи 4 следует, что $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \ (mod\ p)$.

7. **(a)** При каких p вычет -1 является квадратичным вычетом по модулю p?
(b) (Теорема Жирара.) Пусть $x^2 + y^2$ делится на простое число $p = 4k + 3$. Докажите тогда, что x и y делятся на p.

8. **(a)** Докажите, что многочлен $x^4 + 4$ — приводим над $\mathbb{Z}$.
(b) Докажите, что многочлен $x^2 + 1$ — приводим над $\mathbb{Z}_p$ при $p = 4k + 1$.
(c) Докажите, что многочлен $x^4 + 1$ — приводим над $\mathbb{Z}_p$ при любом p.