31 октября 2013. Квадратичные вычеты.

Определение. Число r называется *квадратичным вычетом* по модулю p (p – простое нечётное число), если существует такое целое a, что $a^2 \equiv r (mod\ p)$. В противном случае r называется *квадратичным невычетом*.

1. Докажите следующие свойства квадратичных вычетов:

а) среди чисел $1, 2, \dots (p-1)$ поровну вычетов и невычетов;
б) если r_1 и r_2 — вычеты, то $r_1 r_2$ тоже вычет;
в) если r_1 — вычет, а r_2 — невычет, то $r_1 r_2$ — невычет;
г) если r_1 и r_2 — невычеты, то $r_1 r_2$ — вычет.

Определение. *Символом Лежандра* вычета a по модулю p называется число $\left(\frac{a}{p}\right)$, равное 0, если a делится на p; равное 1, если a – квадратичный вычет; и –1, если a – квадратичный невычет.

2. Докажите, что $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ (mod\ p)$.

3. Решите для простых чисел p сравнение $x^2 + 1 \equiv 0\ (mod\ p)$, если **а)** $p = 4k + 3$; **б)** $p = 4k + 1$ для $k \in \mathbb{Z}$.

4. Докажите, что если $a^2 + b^2 \vdots p$, где $p = 4k + 3$ – простое, то a и b делятся на p.

5. Докажите, что простых чисел вида $4k + 1$ бесконечно много.

6. а) Лемма Туэ. Пусть $n > 1$ – натуральное число. Тогда для каждого натурального a, взаимно простого с n, существуют такие натуральные $x \leqslant \sqrt{n}, y \leqslant \sqrt{n}$, что $ay \equiv \pm\ x\ (mod\ n)$.
б) При помощи леммы Туэ докажите, что любое простое число вида $4k+1$ представимо в виде суммы двух точных квадратов.

7. а) Докажите, что произведение чисел, представляющихся в виде суммы двух квадратов, также представляется в таком виде.
б) Какие натуральные числа представляются в виде суммы двух квадратов, а какие – нет?

8. Решите в натуральных числах уравнение $4xy - x - y = z^2$.

9. Последовательности x_i и y_i заданы $x_1 = 1$, $y_1 = 100$, $x_{n+1} = x_n^{237} + y_n$, $y_{n+1} = y_n^{237} + x_n$. Докажите, что ни при каком n число $x_n y_n$ не делится на 239.

31 октября 2013. Квадратичные вычеты.

Определение. Число r называется *квадратичным вычетом* по модулю p (p – простое нечётное число), если существует такое целое a, что $a^2 \equiv r (mod\ p)$. В противном случае r называется *квадратичным невычетом*.

1. Докажите следующие свойства квадратичных вычетов:

а) среди чисел $1, 2, \dots (p-1)$ поровну вычетов и невычетов;
б) если r_1 и r_2 — вычеты, то $r_1 r_2$ тоже вычет;
в) если r_1 — вычет, а r_2 — невычет, то $r_1 r_2$ — невычет;
г) если r_1 и r_2 — невычеты, то $r_1 r_2$ — вычет.

Определение. *Символом Лежандра* вычета a по модулю p называется число $\left(\frac{a}{p}\right)$, равное 0, если a делится на p; равное 1, если a – квадратичный вычет; и –1, если a – квадратичный невычет.

2. Докажите, что $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ (mod\ p)$.

3. Решите для простых чисел p сравнение $x^2 + 1 \equiv 0\ (mod\ p)$, если **а)** $p = 4k + 3$; **б)** $p = 4k + 1$ для $k \in \mathbb{Z}$.

4. Докажите, что если $a^2 + b^2 \vdots p$, где $p = 4k + 3$ – простое, то a и b делятся на p.

5. Докажите, что простых чисел вида $4k + 1$ бесконечно много.

6. а) Лемма Туэ. Пусть $n > 1$ – натуральное число. Тогда для каждого натурального a, взаимно простого с n, существуют такие натуральные $x \leqslant \sqrt{n}, y \leqslant \sqrt{n}$, что $ay \equiv \pm\ x\ (mod\ n)$.
б) При помощи леммы Туэ докажите, что любое простое число вида $4k+1$ представимо в виде суммы двух точных квадратов.

7. а) Докажите, что произведение чисел, представляющихся в виде суммы двух квадратов, также представляется в таком виде.
б) Какие натуральные числа представляются в виде суммы двух квадратов, а какие – нет?

8. Решите в натуральных числах уравнение $4xy - x - y = z^2$.

9. Последовательности x_i и y_i заданы $x_1 = 1$, $y_1 = 100$, $x_{n+1} = x_n^{237} + y_n$, $y_{n+1} = y_n^{237} + x_n$. Докажите, что ни при каком n число $x_n y_n$ не делится на 239.