Арифметика остатков. Добавка

Определение. Вычет a называется *обратимым* по модулю m, если существует вычет b (быть может, совпадающий с вычетом a), такой что $a \cdot b \equiv 1 \pmod{m}$. В таком случае вычет b называется *обратным* к a.

1. Вычет a обратим по модулю m тогда и только тогда, когда НОД(a,m)=1.
2. Докажите, что если вычет обратим, то обратный к нему единственный.
3. При каких условиях вычет обратен сам себе?
4. **Теорема Вильсона.** Докажите, что для простого p выполнено сравнение
$$(p-1)! \equiv -1 \pmod{p}.$$
5. Пусть $p > 2$ простое число. Докажите, что сравнение $x^2 \equiv -1 \pmod{p}$ имеет решения тогда и только тогда, когда $p = 4k + 1$.