Первообразные корни и квадратичные вычеты

Определение: Если g и n – взаимно простые натуральные числа, и показатель g по модулю n равен $\varphi(n)$, то g называется *первообразным корнем* по модулю n. В таком случае $g^0, g^1, \ldots, g^{\varphi(n)-1}$ дают по разу всевозможные остатки по модулю n, взаимно простые с n.

Упр1: Покажите справедливость предыдущего утверждения.

Упр2: Существует ли первообразный корень по модулю 8? По модулю 9?

Вопрос: По каким модулям n существуют первообразные корни?

Ответ: (пока слишком сложный для нас) При $n = 2, 4, p^t, 2p^t$, где $p > 2$ — простое.

Однако мы докажем следующий факт.

Теорема 3: По простому модулю всегда существует первообразный корень.

Ключевая лемма 4: Для любого натурального k по простому модулю p существует не более k таких остатков, что их k-я степень сравнима с 1 по модулю p.

Доказательство теоремы 3 (воспроизведите основные шаги):

Во всех пунктах имеем в виду показатель по модулю p.

I. Если x имеет показатель ab, то x^a – показатель b.

II. Если x и y имеют взаимно простые показатели a и b соответственно, то xy имеет показатель ab.

III. Пусть s – наименьшее общее кратное всех возможных показателей остатков по модулю p. Далее, пусть $s = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}$ – разложение на простые множители. Докажите, что существуют n остатков по модулю p, имеющих показатели $p_1^{k_1}, p_2^{k_2}, \ldots, p_n^{k_n}$ соответственно.

IV. Докажите существование остатка, имеющего показатель s.

V. Покажите, что $s = p-1$ (не забудьте про ключевую лемму!). Закончите доказательство теоремы.

Упр4. А сколько этих самых первообразных корней по модулю p существует? **Указание.** Уже можно пользоваться существованием хотя бы одного!

Упр5. Докажите, что для любого простого p числа $1, 2, \ldots, p-1$ можно расставить по кругу так, что для любых трех последовательных a, b и c разность $b^2 - ac$ делится на p.

Далее везде p – нечетное простое число, g – какой-нибудь первообразный корень по модулю p.

Определение: Ненулевой остаток a по модулю p называется *квадратичным вычетом*, если существует такой остаток x, что $x^2 \equiv a \pmod{p}$. В противном случае он называется *квадратичным невычетом*.

Упр6. Покажите, что g^k, является квадратичным вычетом тогда и только тогда, когда k четно.

Упр7. Покажите, что по модулю p существует ровно $(p-1)/2$ квадратичных вычетов и столько же невычетов.

Упр8. Покажите, что произведение двух квадратичных вычетов – вычет; произведение вычета на невычет – невычет; произведение двух невычетов – вычет.

Определение: *Символом Лежандра* $\left(\frac{a}{p}\right)$ называется выражение, обозначаемое, равное 1, если a – квадратичный вычет по модулю p, –1, если a – невычет по модулю p и 0, если $a = 0$.

Упр9. Докажите, что

а) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$.

б) $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Зад10. Докажите, что
а) $p-1$ – квадратичный вычет по модулю $p \Leftrightarrow p \equiv 1 \pmod 4$;
б) если p делит число вида x^2+1, то $p \equiv 1 \pmod 4$;
в) если нечетное натуральное n делит число вида x^2+1, то $n \equiv 1 \pmod 4$.

Зад11. (**Теорема Жирара**) Простое число $p \equiv 3 \pmod 4$, а целые числа x и y таковы, что $x^2 + y^2$ делится на p. Тогда x и y делятся на p.

Зад12. Докажите, что существует бесконечно много простых чисел вида **а)** $4k+3$; **б)** $4k+1$.

Зад13. Решите в целых числах уравнение $(a^2-1)(b^2-1) = 4c^2 + (2c+1)^2$.

Зад14. Решите в целых числах уравнение $x^3 + 7 = y^2$.
Подсказка: добавьте к обеим частям равенства по 1.

Зад15. Докажите, что для $p > 3$ сумма квадратичных вычетов по модулю p делится на p.

Для самостоятельного решения

КВ1. Покажите, что уравнение $4xy - x - y = z^2$ не имеет решений в натуральных числах, но имеет бесконечно много решений в целых числах.

КВ2. Петя возвел каждое из чисел 1, 2, …, 100 в степень k и сложил все получившиеся результаты. При каких k то, что получилось, будет делиться на 101?

КВ3. (***Еще одно доказательство существования первообразных корней***)
а) Докажите, что если $p - 1$ кратно простому числу m, то существует ровно $\varphi(m) = m - 1$ остатков по модулю p, принадлежащих показателю m (то есть имеющих показатель m).
б) Теперь обобщите результат на составные m.
Указание. Вспомните, чему равна сумма функций Эйлера по делителям числа m.