Что такое закон взаимности? 1/8/2011

К. Конрад Задание 1

1. Проверьте следующие вычисления, используя квадратичный закон взаимности:
$$\left(\frac{7}{31}\right) = 1, \quad \left(\frac{30}{67}\right) = -1, \quad \left(\frac{42}{101}\right) = -1.$$

2. Используя квадратичный закон взаимности, покажите:

   (a) для $p \neq 2$, $-2 \equiv \square \bmod p \iff p \equiv 1, 3 \bmod 8$,

   (b) для $p \neq 2$ или 3, $3 \equiv \square \bmod p \iff p \equiv 1, 11 \bmod 12$,

   (c) для $p \neq 2$ или 3, $-3 \equiv \square \bmod p \iff p \equiv 1 \bmod 3$,

   (d) для $p \neq 2$ или 3, $6 \equiv \square \bmod p \iff p \equiv 1, 5, 19, 23 \bmod 24$.

3. Имеет ли решение сравнение $x^2 + x + 2 \equiv 0 \bmod 29$? (Подсказка: квадратичная формула.)

4. Если m и n взаимно простые числа, то покажите для любого целого a, что $a \equiv \square \bmod mn \iff a \equiv \square \bmod m$ и $a \equiv \square \bmod n$.

5. Докажите сравнение Эйлера ($a^{(p-1)/2} \equiv (\frac{a}{p}) \bmod p$ для нечетного простого числа p) двумя методами:

   (a) Рассмотрение корней многочлена $x^{p-1} - 1 = (x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1)$ в поле $\mathbf{Z}/p\mathbf{Z}$.

   (b) Группа $(\mathbf{Z}/p\mathbf{Z})^\times$ – циклична. (Подсказка: какие степени образующего являются квадратами?)

6. В $(\mathbf{Z}/p\mathbf{Z})^\times$, где p нечетное простое число, докажите, что произведение двух неквадратов равно квадрату двумя методами:

   (a) Сравнение Эйлера.

   (b) Группа $(\mathbf{Z}/p\mathbf{Z})^\times$ – циклична. (Подсказка: какие степени образующего являются квадратами?)

7. Докажите эквивалентность следующих двух вариантов квадратичного закона взаимности:

- Вариант Гаусса: для всех разных нечетных простых p и q,

$$p \text{ или } q \equiv 1 \bmod 4 \Longrightarrow \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right),$$
$$p \text{ и } q \equiv 3 \bmod 4 \Longrightarrow \left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).$$

  Также

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{если } p \equiv 1 \bmod 4, \\ -1, & \text{если } p \equiv 3 \bmod 4, \end{cases} \quad \left(\frac{2}{p}\right) = \begin{cases} 1, & \text{если } p \equiv 1, 7 \bmod 8, \\ -1, & \text{если } p \equiv 3, 5 \bmod 8. \end{cases}$$

- Вариант Эйлера: для каждого ненулевого целого d и нечетных простых p и q, которые не делят $2d$,

$$p \equiv q \bmod 4d \implies \left(\frac{d}{p}\right) = \left(\frac{d}{q}\right),$$
$$p \equiv -q \bmod 4d \implies \left(\frac{d}{p}\right) = (\operatorname{sign} d)\left(\frac{d}{q}\right).$$

  (Подсказка: для Гаусс $\Rightarrow$ Эйлер: сведите к случаю $d = -1, 2$, или нечетному простому. Для Эйлер $\Rightarrow$ Гаусс: пусть $d = (p \pm q)/4$, где $\pm$ выбран т.ч. $d \in \mathbf{Z}$.)

8. Пусть p – нечетное простое и n – целое, которое не равно совершенному квадрату.

   (a) Покажите, что если p или $-p$ имеет вид $x^2 - ny^2$ для некоторых целых x и y, то $(\frac{n}{p}) = 1$.

   (b) Покажите, что обратное утверждение части (a) верно при условии, что кольцо $\mathbf{Z}[\sqrt{n}]$ имеет однозначное разложение на множители. (Напр., $n = -1, 2, -2, 3$.)

   (c) Проверьте, что $(\frac{3}{11}) = 1$ и $-11 = x^2 - 3y^2$ для некоторых конкретных целых x и y, но невозможно писать $11 = x^2 - 3y^2$ для целых x и y. (Это показывает, что вообще нужно включить $-p$ в части (a).)

9. Докажите формулу для символа Лежандра $(\frac{2}{p})$ используя $\mathbf{Z}[i]$, где $2 =$

$-i(1+i)^2$, поэтому

$$2^{(p-1)/2} = (-i)^{(p-1)/2}(1+i)^{p-1} = (-i)^{(p-1)/2}\frac{(1+i)^p}{1+i}.$$

(Подсказка: вычислите $(1+i)^p$ в кольце $\mathbf{Z}[i]/(p)$, которое имеет характеристику p.)

10. (a) Получите каждую часть закона взаимности символа Якоби (т.е., главный закон и каждый дополнительный закон) из соответствующей части закона взаимности символа Лежандра, используя индукцию по числу простых множителей знаменателя символа Якоби.

    (b) Используйте главный закон взаимности символа Якоби и дополнительный закон символа Якоби $(\frac{-1}{n})$ для того, чтобы доказать дополнительный закон символа Якоби $(\frac{2}{n})$! В частности, с использованием символа Якоби возможно получить дополнительный закон для символа Лежандра $(\frac{2}{p})$ из главного закона символа Лежандра для нечетных простых чисел и дополнительного закона символа $(\frac{-1}{p})$.

    (Подсказка: Имеем $(\frac{2}{n}) = (\frac{2+n}{n})$ и главный закон взаимности символа Якоби возможно использовать в правой части. Из этого выведите соотношение между символами Якоби $(\frac{2}{n+2})$ и $(\frac{2}{n})$ для произвольного положительного нечетного числа n.)

11. Проверьте, что $(\frac{1649}{2011}) = 1$ из закона взаимности символа Лежандра и тоже из закона взаимности символа Якоби (число 2011 – простое и $1649 = 17 \cdot 97$).

12. Пусть d – ненулевое целое, которое не равно совершенному квадрату. Имеем групповой гомоморфизм $(\mathbf{Z}/4d\mathbf{Z})^\times \to \{\pm 1\}$ по правилу $n \mapsto (\frac{d}{n})$, где $n > 0$ и $(\frac{d}{n})$ – символ Якоби. (То, что $(\frac{d}{n})$ – функция от $n \bmod 4d$, когда $n > 0$ и НОД$(n, 4d) = 1$ – следствие закона взаимности символа Якоби.)

    (a) Покажите, что $(\frac{d}{n}) = -1$ для половины вычетов $n \bmod 4d$ в группе $(\mathbf{Z}/4d\mathbf{Z})^\times$. (Подсказка: во-первых покажите, что $(\frac{d}{n}) = -1$ для некоторого n.)

    (b) Теорема Дирихле об арифметических прогрессиях утверждает, что для взаимно простых чисел a и m, множество всех простых p т.ч.

$p \equiv a \bmod m$ имеет плотность $1/\varphi(m)$:

$$\lim_{x\to\infty} \frac{|\{p : p \le x, p \equiv a \bmod m\}|}{|\{p : p \le x\}|} = \frac{1}{\varphi(m)}.$$

Иными словами, простые числа, которые не делят m, равномерно распределны по модулю m. Из этого и предыдущей части получите то, что $\{\text{простые } p : (\frac{d}{p}) = 1\}$ имеет плотность $\frac{1}{2}$. (Подсказка: Запишите условие $(\frac{d}{p}) = 1$ как условия сравнений на $p \bmod 4d$. Смотрите примеры во втором вопросе.)

13. Предыдущий вопрос влечет, что если $d \equiv x^2 \bmod p$ для всех p, то d – совершенный квадрат в $\mathbf{Z}$. Это не верно для некоторых высших степеней, в частности восьмой степени: покажите, что $16 \equiv x^8 \bmod p$ для всех простых p, но конечно 16 не равно восьмой степени как целое. (Подсказка: Имеем тождество многочленов

$$x^8 - 16 = (x^4 - 4)(x^4 + 4) = (x^2 - 2)(x^2 + 2)(x^2 + 2x + 2)(x^2 - 2x + 2).$$

Покажите, что для всяких простых p, по крайней мере один множитель в правой имеет корень по модулю p.)