Что такое закон взаимности? 2/8/2011

К. Конрад Задание 2

1. Если $p \equiv q \bmod 4a$ для общего ненулевого целого a и разных простых p и q, которые не делят $4a$, то из квадратичного закона взаимности следует, что разрешимость сравнений $x^2 \equiv a \bmod p$ и $x^2 \equiv a \bmod q$ – эквивалентна. Слушатель на вчерашней лекции задал вопрос: если мы знаем, что эти сравнения разрешуемые, легко ли получить решение одного из этих сравнений, зная решения другого? Покажите, что если бы такой алгоритм существовал, то мы бы получили доказательство квадратичного закона взаимности. (Подсказка: Пусть p и q всякие разные нечетные простые и пусть $a = (p \pm q)/4$, где знак $\pm$ выбран, т.ч. $p \pm q \equiv 0 \bmod 4$.)

2. Пусть $\alpha = a + bi \in \mathbf{Z}[i]$, где a и b целые.

   (a) Покажите, что $(1+i) \mid \alpha$ тогда и только тогда, когда $a \equiv b \bmod 2$.

   (b) Предположим, что α нечетное, т.е., $a \not\equiv b \bmod 2$. Покажите, что α примарно тогда и только тогда, когда a – нечетное, b – четное, и $a - 1 \equiv b \bmod 4$.

   (c) Когда α – нечетное, проверьте следующую таблицу, которая показывает примарное кратное числа α в зависимости от вычетов чисел a и b по модулю 4.

$a \bmod 4$	$b \bmod 4$	примар. кратное
1	0	α
3	0	$-\alpha$
1	2	$-\alpha$
3	2	α
0	1	$-i\alpha$
0	3	$i\alpha$
2	1	$i\alpha$
2	3	$-i\alpha$

3. Проверьте следующее вычисление символов Лежандра на $\mathbf{Z}[i]$: $(\frac{1+2i}{2+3i}) = 1$ и $(\frac{1-2i}{2+3i}) = -1$. Тогда в первом случае найдите решение в $\mathbf{Z}[i]$ сравнения $x^2 \equiv 1 + 2i \bmod 2 + 3i$. (Используйте примарные простые в $\mathbf{Z}[i]$!)

4. Проверьте пример закона взаимности символов Гильберта: $\prod_v (10, 7)_v = 1$. То есть, вычислите символы Гильберта $(10, 7)_v$ для всех v и проверьте то, что их произведение равно 1.

5. Проверьте то, что $(31, 82)_v = 1$ для всех v. Какое рациональное решение имеет уравнение $31x^2 + 82y^2 = 1$? (Замечание: Это уравнение не имеет *целых* решений, но сравнение $31x^2 + 82y^2 \equiv 1 \bmod m$ имеет решение для всякого модуля m.)

6. Пусть F – поле, характеристика которого не равна двум.

   (a) Покажите, что квадратичная форма $x^2 - y^2$ на F универсальна, т.е., для всех $c \in F$, уравнение $x^2 - y^2 = c$ имеет решение для некоторых $x, y \in F$. (Для некоторых полей F характеристики 2, это не верно.)

   (b) Для ненулевых элементов a и b в F, покажите с помощью части (a), что $a = x^2 - by^2$ для некоторых x и y в F тогда и только тогда, когда $b = x^2 - ay^2$ для некоторых x и y в F. (Конечно, x и y в первом уравнении не совпадают с x и y во втором уравнении!)

   (c) Для $a \in F^\times$, покажите, что $ax^2 + ay^2 = 1$ имеет решение в F тогда и только тогда, когда $ax^2 - y^2 = 1$ имеет решение в F.

7. Пусть F – поле, характеристика которого не равна двум. Для ненулевых a и b в F, пусть $(a, b)_F = 1$, когда уравнение $ax^2 + by^2 = 1$ имеет решение x и y в F и $(a, b)_F = -1$ иначе.

   - Если $a \neq \square$ в $F^\times$, то покажите, что $(a, b)_F$ – мултипликативная функция от b тогда и только тогда, когда $[F^\times : \mathrm{N}_{E/F}(E^\times)] \leq 2$, где $E = F(\sqrt{a})$. (Подсказка: Если $[F^\times : \mathrm{N}_{E/F}(E^\times)] \geq 3$, то выбирите b_1 и $b_2 \in F^\times - \mathrm{N}_{E/F}(E^\times)$ такие, что $b_1 \not\equiv b_2^{-1} \bmod \mathrm{N}_{E/F}(E^\times)$. Рассмотрите $(a, b_1)_F$, $(a, b_2)_F$ и $(a, b_1 b_2)_F$.)
   - Если каждая подгруппа группы $F^\times$ индекса два имеет вид $\mathrm{N}_{E/F}(E^\times)$ для некоторого квадратичного расширения E/F, то покажите, что

каждый нетривиальный гомоморфизм $\chi\colon F^\times \to \{\pm 1\}$ имеет вид $\chi(x) = (a,x)_F$ для некоторого $a \in F^\times$.

В частности, когда $F = \mathbf{Q}_p$ для всякого p, бывает, что подгруппы индекса два в $F^\times$ совпадают с группами $\mathrm{N}_{E/F}(E^\times)$ для квадратичных расширений E/F. Поэтому нетривиальные групповые гомоморфизмы $\chi\colon \mathbf{Q}_p^\times \to \{\pm 1\}$ имеют вид $\chi(x) = (a,x)_p$ для некоторого $a \in \mathbf{Q}_p$.

8. Покажите, что для всяких разnых простых $p, q \equiv 3 \bmod 4$, дробь p/q невозможно писать в виде $r^2 + s^2$ для рациональных r и s. В частности, заключите, что группа $\mathrm{N}_{\mathbf{Q}(i)/\mathbf{Q}}(\mathbf{Q}(i)^\times)$ имеет бесконечный индекс в группе $\mathbf{Q}^\times$. (Вообще, для всякого числового поля $K \neq \mathbf{Q}$, $\mathrm{N}_{K/\mathbf{Q}}(K^\times)$ имеет бесконечный индекс в группе $\mathbf{Q}^\times$.)

9. Покажите, что единственное нетривиальное мультипликативное соотношение среди символов Гильберта $(\cdot,\cdot)_v$ для всех $v \in V_\mathbf{Q}$ – закон взаимности Гильберта. То есть, если последовательность показателей $\{e_v\} \in \{0,1\}$ удовлетворяет тождеству $\prod_v (a,b)_v^{e_v} = 1$ для всех ненулевых рациональных a и b, то $e_v = 0$ для всех v (тривиальное соотношение) или $e_v = 1$ для всех v (закон взаимности Гильберта). (Подсказка: рассмотрите случая, когда a и b равны -1, 2, или нечетным простым для того, чтобы показать, что $e_v \equiv e_w \bmod 2$ для всех v и w в $V_\mathbf{Q}$. В некоторых случаях удобно использовать теорему Дирихле об арифметических прогрессиях.)