MAS/320 Number Theory: Coursework 4

Franco VIVALDI

http://www.maths.qmw.ac.uk/~fv/teaching/nt/nt.html

This coursework will be assessed and count towards your final mark for the course

DEADLINE: Wednesday of week 10, at 1:00 pm.

CONTENT: Quadratic forms.

MicroESSAY : Write an essay on quadratic forms. (Approximately 100 words, and no mathematical symbols.)

Problem 1. Divide the following forms in to indefinite and positive definite, whence determine which ones are reduced (k is a non-zero integer)

$a)$ $(-11,-5,1)$ $b)$ $(3,-1,3)$ $c)$ $(2,-1,3)$

$d)$ $(k^2,-k,|k|)$ $e)$ $(2,6,-5)$ $f)$ $(k,1,-k)$.

Problem 2. Consider the following forms

$a)$ x^2+5y^2 $b)$ $29x^2-32xy+9y^2$ $c)$ $3x^2+14xy+18y^2$

$d)$ $-5x^2+y^2$ $e)$ $3x^2+2xy+2y^2$ $f)$ $81x^2-284xy+249y^2$

(a) Prove that b and f are equivalent to a, that c is equivalent to e but not to a, and that d is not equivalent to any of the other forms.

(b) Represent the prime 29 with a (by inspection). Determine the unimodular transformation that transforms f into a, and use it to represent 29 with f.

(c) Determine the unimodular transformation that transforms b into f.

Problem 3. Find all the reduced positive definite forms of discriminant

(a) $D=-15$ (b) $D=-56$.

Problem 4. Find all the reduced indefinite quadratic forms equivalent to $(76,-58,11)$.

Problem 5. For the following discriminants, find all the reduced indefinite forms, divide them into their chains, and compute the class number

(a) $D=60$ (b) $D=28$.

Problem 6. This exercise is concerned with the problem of *composition of forms* (Gauss, 1801).

(a) Let $Q(x, y) = x^2 + y^2$. Verify the following identity

$$Q(a, b)\, Q(c, d) = Q(ac + bd, ad - bc), \tag{1}$$

which says that if m and n are sums of two squares, so is their product mn (make sure you believe this).

(b) Represent 5, 13, 17 and 29 as a sum of two squares (by inspection), hence, by repeated use of (1), represent $32045 = 5 \cdot 13 \cdot 17 \cdot 29$ as a sum of squares.

(c) Discover an analogue of formula (1) for the form $Q(x, y) = x^2 + Dy^2$

$$Q(a, b)\, Q(c, d) = Q(\,?\,,\,?\,). \tag{2}$$

(d) Represent 4 and 7 by the form $Q(x, y) = x^2 - 53y^2$, using continued fractions, and hence use formula (2) to represent $28 = 4 \cdot 7$.

(e)* There are two equivalence classes of quadratic forms for the discriminant $D = -24$, represented by $Q_1(x, y) = x^2 + 6y^2$ (the principal form) and $Q_2(x, y) = 2x^2 + 3y^2$, respectively. We write $Q_i * Q_j = Q_k$ (for $i, j, k = 1, 2$) if the product of a number representable by Q_i and one representable by Q_j is representable by Q_k. Prove the composition formulae

$$Q_1 * Q_1 = Q_1 \qquad Q_2 * Q_2 = Q_1 \qquad Q_1 * Q_2 = Q_2. \tag{3}$$

(You have already proved the first formula in part (c). The operation $*$ gives the equivalence classes of discriminant -24 the structure of a commutative group, called the *class group*.)

Problem 7. This exercise is concerned with the factorization of *quadratic integers*, which are numbers of the form $m + n\sqrt{D}$, with m, n integers, and D not a square.

(a) Let $\mathbf{Z}[\sqrt{-2}]$ be the set of numbers of the form $m + n\sqrt{-2}$, with m and m integers. Within this set, the integer 33 can be factored in two different ways, as follows

$$33 = 3 \cdot 11 = (1 + 4\sqrt{-2}) \cdot (1 - 4\sqrt{-2}). \tag{4}$$

Show that each product can be decomposed further, into the product of the same *four* distinct factors. [*Hint:* represent 3 and 11 by the form $Q(x, y) = x^2 + 2y^2$ (by inspection), whence determine $\alpha,\, \beta \in \mathbf{Z}[\sqrt{2}]$ such that $3 = \alpha\, \alpha'$, $11 = \beta\, \beta'$, $1 + 4\sqrt{-2} = \alpha\, \beta$, $1 - 4\sqrt{-2} = \alpha'\, \beta'$, where the prime denotes algebraic conjugation.]

(b)* Let $\mathbf{Z}[\sqrt{-6}]$ be the set of numbers of the form $m + n\sqrt{-6}$, with m and m integers. Prove that the fundamental theorem of arithmetic (unique factorization into primes) fails in $\mathbf{Z}[\sqrt{-6}]$, by showing that the following two distinct decompositions of 55

$$55 = 5 \cdot 11 = (7 + \sqrt{-6}) \cdot (7 - \sqrt{-6}).$$

cannot be resolved by further factorization. [*Hint:* with reference to (3), note that 5 and 11 are not representable by the form Q_1, although their product is.]