ELEMENTARY NUMBER THEORY

PROBLEMS ON QUADRATIC FORMS

(1) Take a negative discriminant and compute the class number.

Here is a small table with some examples: If $\Delta = 1 - 4m$, then the principal form is $(1, 1, m)$. As you can see, if $m = 2n$ is even (this happens if and only if $\Delta \equiv 1 \bmod 8$), then the class number is at least 3 since we also have the reduced forms $(2, \pm 1, n)$.

Δ	$h(\Delta)$	reduced forms
-23	3	$(1,1,6), (2,\pm1,3)$
-27	1	$(1,1,7)$
-31	3	$(1,1,8), (2,\pm1,4)$
-35	2	$(1,1,9), (3,1,3)$
-39	4	$(1,1,10), (2,\pm1,5), (3,3,4)$
-43	1	$(1,1,11)$
-47	5	$(1,1,12), (2,\pm1,6), (3,\pm1,4)$
-51	2	$(1,1,13), (3,3,5)$
-55	4	$(1,1,14), (2,\pm1,7), (4,3,4)$

Now consider the discriminants $\Delta = 4m$ with negative $m \equiv 3 \bmod 4$:

Δ	$h(\Delta)$	reduced forms
-20	2	$(1,0,5), (2,2,3)$
-36	2	$(1,0,9), (2,2,5)$
-52	2	$(1,0,13), (2,2,7)$
-68	4	$(1,0,17), (2,2,9), (3,\pm2,6)$
-84	4	$(1,0,21), (2,2,11), (3,0,7), (5,4,5)$

Finally, consider $\Delta = 4m$ with negative even m:

Δ	$h(\Delta)$	reduced forms
-24	2	$(1,0,6), (2,0,3)$
-32	2	$(1,0,8), (3,2,3)$
-40	2	$(1,0,10), (2,0,5)$
-48	2	$(1,0,12), (3,0,4)$
-56	4	$(1,0,14), (2,0,7), (3,\pm2,5)$
-64	2	$(1,0,16), (4,4,5)$

(2) Take some primitive positive definite form and reduce it.

Examples: $(123, 91, 17) \sim (3, 1, 7)$; $(73, 58, 14) \sim (13, 2, 14)$. You will not have to memorize the reduction algorithm, but you must be able to apply it.

(3) Assume that $p = x^2 + 21y^2$ for some prime p. Show that $p \equiv 1 \bmod 3$, $p \equiv 1 \bmod 4$, and $p \equiv 1, 2, 4 \bmod 7$.

This is actually something I could have asked in midterm 2.

If you consider $p = 2x^2 + 2xy + 11y^2$ for odd primes, then you should be able to show that $p \equiv 2 \bmod 3$ (hint: multiply through by 2 and complete squares), $p \equiv 3 \bmod 4$ (hint: $p = 2x(x + y) + 11y^2$), and $p \equiv 1, 2, 4 \bmod 7$.

Do something similar for the other reduced forms of discriminant -84.

(4) Show that $2 \cdot 3 = -\sqrt{-6} \cdot \sqrt{-6}$ is an example of nonunique factorization in $\mathbb{Z}[\sqrt{-6}\,]$.

The only units in complex quadratic fields are ± 1, with the exception of $\Delta = -3$ and $\Delta = -4$. In this case, the only units are ± 1, and the factors clearly do not differ by units.

It remains to show that they are irreducible. Assume that $2 = \alpha\beta$; taking norms gives $4 = N\alpha N\beta$. Since α and β must be nonunits for the factorization to be nontrivial, we must have $N\alpha = N\beta = 2$. But with $\alpha = x + y\sqrt{-6}$ this gives $x^2 + 6y^2 = 2$, a contradiction. The other cases are just as simple.

(5) Show that $2 = \sqrt{2} \cdot \sqrt{2} = (2 + \sqrt{2}\,)(2 - \sqrt{2}\,)$ is not an example of nonunique factorization.

Hint: the factor differ by units.

(6) Show that $6 = 2 \cdot 3 = (3 + \sqrt{3}\,)(3 - \sqrt{3}\,)$ is not an example of nonunique factorization.

Hint: the factors are not irreducible.