Math 5230 - Algebraic Number Theory (Fall 2012) Due in MSB 318
Problem Set 1 9/7/12 at 4 PM

One soon realizes that in this rich domain of higher arihtmetic one can only penetrate through completely new roads... that to that end a specific expansion of the whole field of higher arithmetic is an essential necessity. Gauss

1. Use norms to discover prime factorizations of $3 + 7i$ and $23 + 14i$ in $\mathbf{Z}[i]$.

2. Use algebraic properties of $\mathbf{Z}[\sqrt{-2}]$ to prove for prime numbers p in $\mathbf{Z}$ that $p = x^2 + 2y^2$ for some x and y in $\mathbf{Z}$ if and only if $-2 \equiv \square \bmod p$.

3. Prove $\mathbf{Z}[\sqrt{3}]$ is Euclidean with respect to the absolute value of the norm. (Hint: $|x^2 - 3y^2| \leq \max(x^2, 3y^2)$ because x^2 and $3y^2$ are on the same side of 0.) What goes wrong if you try to prove $\mathbf{Z}[\sqrt{-3}]$ is Euclidean with respect to the norm?

4. (Quadratic Units)

   a) Generalize the argument from class that the smallest unit > 1 in $\mathbf{Z}[\sqrt{2}]$ is $1 + \sqrt{2}$ to show the following: if $d > 0$ is not a perfect square and $u := a + b\sqrt{d}$ is a unit in $\mathbf{Z}[\sqrt{d}]$ which is greater than 1, the integer coefficients a and b are both positive.

   b) Use part a to find the smallest unit > 1 in $\mathbf{Z}[\sqrt{d}]$ for $d = 3, 6, 7,$ and 34. In particular, describe all the units in $\mathbf{Z}[\sqrt{3}]$ and $\mathbf{Z}[\sqrt{6}]$.

   c) Give an example of a unit $\neq \pm 1$ in $\mathbf{Z}[\sqrt{d}]$ for the following values of d: $5, 8, 10, 11, 12$.

5. (Factoring in quadratic rings)

   a) In $\mathbf{Z}[\sqrt{6}]$, $2 \cdot 3 = \sqrt{6}^2$ is a square and 2 and 3 have no common factors except units (after all, their difference is 1). Can you show 2 and 3 are unit multiples of squares in $\mathbf{Z}[\sqrt{6}]$?

   b) In $\mathbf{Z}[\sqrt{-6}]$, $2 \cdot (-3) = \sqrt{-6}^2$ is a square and 2 and -3 have no common factors except units (their sum is -1). Can you show 2 and -3 are unit multiples of squares in $\mathbf{Z}[\sqrt{-6}]$?

6. a) Use algebraic properties of $\mathbf{Z}[\sqrt{2}]$ and $\mathbf{Z}[\sqrt{3}]$ to prove for prime numbers p in $\mathbf{Z}$ that

$$\pm p = x^2 - 2y^2 \text{ for some } x \text{ and } y \text{ in } \mathbf{Z} \iff 2 \equiv \square \bmod p,$$
$$\pm p = x^2 - 3y^2 \text{ for some } x \text{ and } y \text{ in } \mathbf{Z} \iff 3 \equiv \square \bmod p.$$

   (Saying $\pm p = x^2 - dy^2$ here means either p or $-p$ has this form, not that both must.)

   b) Is it true that

$$p = x^2 - 2y^2 \text{ for some } x \text{ and } y \text{ in } \mathbf{Z} \iff 2 \equiv \square \bmod p?$$

   What about, for $p \neq 3$,

$$p = x^2 - 3y^2 \text{ for some } x \text{ and } y \text{ in } \mathbf{Z} \iff 3 \equiv \square \bmod p?$$