Math 254A, UC Berkeley, Fall 2001 (Kedlaya)
Lecture 1: The Gaussian Integers
August 27, 2001

Reference. Neukirch, Section 1.1.

Jargon watch. A ring R is *euclidean* if there exists a function $f : R \to \mathbb{Z}_{\geq 0}$ such that:

(a) For $\alpha \in R$, $f(\alpha) = 0$ if and only if $\alpha = 0$.

(b) For $\alpha, \beta \in R$, $f(\alpha\beta) = f(\alpha)f(\beta)$.

(c) For any $\alpha, \beta \in R$, with β nonzero, there exist $\gamma, \delta \in R$ with $\alpha = \beta\gamma + \delta$ and $f(\delta) < f(\beta)$.

For example, take $R = \mathbb{Z}$ and $f(x) = |x|$.

A *unit* of a ring R is an element with a multiplicative inverse. An element α of a ring R is *irreducible* if it not a unit, and whenever β and γ are elements of R whose product is α, one of β or γ is a unit. (Neukirch also calls these elements "prime", but this is a bad habit, as we'll see later.) A ring R is *factorial* if it has no zero divisors (i.e., $\alpha\beta = 0$ implies $\alpha = 0$ or $\beta = 0$), every element can be factorized as a product of irreducible elements, and this factorization is unique up to multiplying elements by units. For example, $\mathbb{Z}$ is factorial, as is the ring $\mathbb{C}[x]$ of polynomials in one variable over the complex numbers (or any other field, for that matter).

Outline of lecture.

1. Do administrative stuff: describe course, homework, exams, grading. Hand out most recent version of course description, and Problem Set 1. Then get to work.

2. Recall statement of Fermat's two squares theorem in the prime case. Point out that $p = a^2 + b^2$ iff $p = (a + bi)(a - bi)$.

3. Define ring $\mathbb{Z}[i]$. Note that the only units are ± 1, $\pm i$.

4. Prove $\mathbb{Z}[i]$ is euclidean.

5. Note that for R euclidean, for any $x, y \in R$, the set $\{\alpha x + \beta y : \alpha, \beta \in R\}$ has an element that divides all of the others.

6. Conclude that $p \equiv 1 \pmod 4$ is the sum of two squares. Yay!

7. Point out that R euclidean implies that every ideal in R is principal, and that every ideal being principal implies unique factorization.