GAUSSIAN PRIMES

1. Gaussian Primes

What are the primes in \( \mathbb{Z}[i] \)? Most of you have shown that if \( a \in \mathbb{Z} \) is a prime if and only if \( a \) is a prime in \( \mathbb{Z} \) and \( a \equiv 3 \pmod{4} \). So for example 7 is a prime in \( \mathbb{Z}[i] \). Since the units are 1, \(-1\), \(i\) and \(-i\), we have that \(-7\), \(7i\) and \(-7i\) are also primes. So \( \alpha = a + ib \) with \( a = 0 \) or \( b = 0 \) is a prime exactly when the nonzero one is a positive prime in \( \mathbb{Z} \) congruent to 3 modulo 4, or its negation.

What numbers of the form \( \alpha = a + ib \), with \( a \neq 0 \neq b \), are primes? The answer is precisely when \( v(\alpha) = a^2 + b^2 \) is a prime in \( \mathbb{Z} \). Several of you already proved that if \( v(\alpha) = a^2 + b^2 \) is a prime in \( \mathbb{Z} \), the \( \alpha \) is prime in \( \mathbb{Z}[i] \). Below is a sketch of a proof of the other direction. Your job is to fill in the details. In particular identify the theorems in the book (or another book) that are used in the steps.

Suppose \( \alpha = a + ib \) is a prime in \( \mathbb{Z}[i] \). Let \( I = \langle a + ib \rangle \) be the ideal it generates. Since \( \alpha \) is prime and \( \mathbb{Z}[i] \) is an integral domain, \( I \) is irreducible and hence maximal. Thus \( F = \mathbb{Z}[i]/I \) is a field. Now \( a^2 + b^2 \in I \) (why?). So in \( \mathbb{Z}[i]/I \), \( a^2 + b^2 \) is 0. Thus \( F \) has finite characteristic, which must be a prime, \( p \). Since \( p = 0 \) in \( F \), \( p \in I \). So \( p = (a + ib)(c + id) \) for some \( c \) and \( d \). Let \( \beta = c + id \). Taking norms (ie., valuations) we get

\[ p^2 = v(p) = v(\alpha)v(\beta) \]

So \( v(\alpha) = p \) or \( p^2 \). But if \( v(\alpha) = p^2 \) then \( \beta \) is a unit. But then \( \alpha \) is a unit times \( p \). So \( \alpha \) is one of \( p \), \(-p\), \( ip \) or \(-ip \). But this contradicts our assumption \( \alpha = a + ib \) with \( a \neq 0 \neq b \).

Date: March 14, 2013.