Elementary Number Theory

Math 175, Section 30, Autumn 2010
Shmuel Weinberger (shmuel@math.uchicago.edu)
Tom Church (tchurch@math.uchicago.edu)
www.math.uchicago.edu/~tchurch/teaching/175/

Homework 6

Due Thursday, November 18 in class.

Question 1. The primes less than 100 are:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, \text{ and } 97.$$

Those that are congruent to $1 \pmod 4$ are **5**, **13**, **17**, **29**, **37**, **41**, **53**, **61**, **73**, **89**, and **97**. Write each of these primes as a sum of two squares. For example, $13 = 9 + 4 = 3^2 + 2^2$. (The squares less than 100 are 1, 2, 4, 9, 16, 25, 36, 49, 64, and 81.)

We proved in Theorem 3.31 that any prime p such that $p \equiv 1 \pmod 4$ can be written as $p = a^2 + b^2$ for some a and b. In the rest of this homework you will use Gaussian integers to give a quicker and simpler proof of this theorem. You will also prove that p can be *uniquely* expressed as the sum of two squares, which we did not prove in class.

Question 2. Prove that if p is a prime with $p \equiv 1 \pmod 4$, the ring $\mathbb{Z}[i]/(p)$ is not a field. (Hint: find more than two roots in $\mathbb{Z}[i]/(p)$ of the polynomial $P(x) = x^2 + 1$.)

Question 3. Prove that if p is a prime in $\mathbb{Z}$ and there is no element $x \in \mathbb{Z}[i]$ with norm $N(x) = p$, then p is irreducible in $\mathbb{Z}[i]$.

Question 4. Using Questions 2 and 3, prove that if p is a prime with $p \equiv 1 \pmod 4$, then p can be written as $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Question 5. Prove that p can be *uniquely* written as $p = a^2 + b^2$: if we can also write $p = c^2 + d^2$, then either $a = \pm c$ and $b = \pm d$, or vice versa.

Question 6. Let p and q be primes with $p \equiv 1 \pmod 4$ and $q \equiv 1 \pmod 4$. How many distinct ways are there of writing $pq = a^2 + b^2$? (Assume $a > b > 0$ to avoid double-counting.)