4400-001 - SPRING 2022 - WEEK 12 (4/5, 4/7)
GAUSSIAN INTEGERS AND SUMS OF TWO SQUARES

Some of these exercises can be found in Savin - Chapter 8.

Exercise 1 (required). Sums of two squares and descent.

(1) Use $13 = 3^2 + 2^2$ and $17 = 4^2 + 1^2$ to write $221 = 13 \cdot 17$ as a sum of two squares.

(2) Use descent to find x, y such that $x^2 + y^2 = 61$ starting from $11^2 + 1^2 = 2 \cdot 61$.

(3) Use descent to find x, y such that $x^2 + y^2 = 881$ starting with $84^2 + 89^2 = 17 \cdot 881$.

(4) Suppose $p \equiv 1 \mod 4$ and g is a primitive root mod p. Show $a = g^{\frac{p-1}{4}}$ satisfies $a^2 \equiv -1 \mod p$.

(5) Represent 73 as a sum of two squares using the following two steps:
   (a) Use the primitive root 5 in $\mathbb{F}_{73}$ and part (4) to find a such that $a^2 + 1 = m \cdot 73$.

   (b) Use the method of descent to find a solution.

Exercise 2 (required). Euclidean algorithm and prime factorization in $\mathbb{Z}[i]$.

(1) Find the gcd of $11 + 7i$ and $5 + 3i$ in $\mathbb{Z}[i]$

(2) Factor $11 + 3i$ in $\mathbb{Z}[i]$ into indecomposable Gaussian integers.
Hint: use the norm to guess factors.

(3) Compute the gcd of $11 + i$ and 61 in $\mathbb{Z}[i]$ to find $x + yi$ such that $x^2 + y^2 = 61$.

(4) Compute the gcd of $9 + 7i$ and 13 in $\mathbb{Z}[i]$ to find $x + yi$ such that $x^2 + y^2 = 13$.

(5) Compute the gcd of $7 + 3i$ and 29 in $\mathbb{Z}[i]$ to find $x + yi$ such that $x^2 + y^2 = 29$.

Exercise 3. Primes of the form $x^2 + 2y^2$.

(1) Use quadratic reciprocity to find a necessary condition for a prime p to have an expression

$$p = x^2 + 2y^2 \text{ for } x \text{ and } y \text{ integers}$$

(2) Show

$$(x^2 + 2y^2)(u^2 + 2v^2) = (xu + 2yv)^2 + 2(yu - xv)^2.$$

(3) Note that -2 is a square modulo 11 – indeed, $8^2 + 2 = 6 \cdot 11$. Use this information and the method of descent to construct a solution to $x^2 + 2y^2 = 11$.

(4) What about primes of the form $x^2 + 3y^2$?

It get harder and more interesting to understand primes of the form $x^2 + ny^2$ for larger n – so interesting, in fact, that there's a beautiful book dedicated to it – **Cox, Primes of the form $x^2 + ny^2$.**

Exercise 4. Some interesting related constructions.

(1) Show that unique factorization into indecomposables does not hold in $\mathbb{Z}[\sqrt{-5}]$.
Hint: Gives two different factorizations of 6 into indecomposables that do not differ by a unit.

(2) Construct infinitely many solutions to $x^2 - 3y^2 = 1$.
Hint: Show that if $x^2 - 3y^2 = 1$ then $x + \sqrt{3}y$ is a unit in $\mathbb{Z}[\sqrt{3}]$.