4400-001 - SPRING 2022 - WEEK 5 (2/08, 2/10)
ROOTS OF POLYNOMIALS AND QUADRATIC NUMBERS

Some of these exercises can be found in Savin - Chapter 3.

Exercise 1 (recommended). Pascal's triangle and binomial coefficients. We write $\binom{n}{k}$ and say "n choose k", for the number of possible ways to choose a set of k objects from a set of n objects. For example, $\binom{4}{2} = 6$, because there are six size 2 subsets of $\{a, b, c, d\}$:

$$\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \text{ and } \{c, d\}.$$

Pascal's triangle is formed by starting with a row with a single 1, then iteratively forming new rows with one more entry whose first and last entries are both both 1s and whose middle entries are given by adding the two entries above. The first four rows are:

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & 1 & & 1 & & \\ & 1 & & 2 & & 1 & \\ 1 & & 3 & & 3 & & 1 \end{array}$$

(1) Write out the first 12 rows of Pascal's triangle, then reduce it moduolo $3, 5, 7$, and 11. What do you notice about the $p + 1$st row for the reduction mod p?

(2) If we number the rows starting at 0 and the entries in each row starting at 0, then the kth entry in the nth row of Pascal's triangle is $\binom{n}{k}$. Try to justify this claim conceptually using the definition of $\binom{n}{k}$ above without writing down any formulas (hint: assume it holds for the nth row, then explain why it holds for the $n + 1$st row).

(3) From the definition of binomial coefficients above, justify the formula

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}.$$

Using this formula, give another justification for the pattern you noticed in (2).

(4) Use (3) and (2) to explain the pattern you noticed in (1).

Exercise 2 (required). Roots and factorization. Let $\mathbb{K}$ be a field.

(1) Let $a \in \mathbb{K}$ and let $f(x) \in \mathbb{K}[x]$.

   (a) Show that the remainder when dividing $f(x)$ by $x - a$ is $f(a)$ (hint: name the coefficients of f, i.e. write $f(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_0$, and then start doing the long division).

   (b) Deduce that $(x - a) | f(x)$ if and only if $f(a) = 0$.

   (c) Use this to explain why a degree n polynomial with coefficients in $\mathbb{K}$ can have at most n roots in $\mathbb{K}$.

(2) Describe an algorithm to find the prime factorization of any polynomial in $\mathbb{F}_p[x]$. Your algorithm should terminate in finite time for any polynomial.

(3) Find an irreducible degree 4 polynomial in $\mathbb{F}_3[x]$.

(4) Construct a field with 81 elements.

(5) (Challenge, not to turn in). Describe an algorithm to find the prime factorization of any polynomial in $\mathbb{Q}[X]$. Your algorithm should terminate in finite time for any polynomial. You may use without justification the fact that if $f(x)$ is monic with integer coefficients, then the prime factors of $f(x)$ also have integer coefficients.

Exercise 3 (required). Quadratic numbers.

1. Write down the times tables for: $\mathbb{F}_3[x]/(x^2+1)$ and $\mathbb{Z}[i]/(3)$. Notice anything?
2. Recall that for D a squarefree integer, the norm function N on $\mathbb{Q}[\sqrt{D}]$ is defined by
$$N(a+b\sqrt{D}) = (a+b\sqrt{D})(a-b\sqrt{D}) = a^2-b^2D.$$
Show that for any $x, y \in \mathbb{Q}[\sqrt{D}]$, $N(xy) = N(x)N(y)$.
3. Find the multiplicative inverse of $2+5i$ in $\mathbb{Z}[i]/(31)$. Does $2+5i$ have a multiplicative inverse in $\mathbb{Z}[i]/(29)$?
4. Find the multiplicative inverse of $7-3\sqrt{5}$ in $\mathbb{Z}[\sqrt{5}]/(11)$ and $\mathbb{Z}[\sqrt{5}]/(17)$.
5. Is the golden ratio, $\frac{1+\sqrt{5}}{2}$, a quadratic integer?
6. Describe the rational numbers a and b such that $a+b\sqrt{5}$ is a quadratic integer.

Exercise 4 (Challenge). A failure of unique factorization.

1. What are the units in $\mathbb{Z}[\sqrt{-5}]$?
2. Find two distinct prime factorizations of 6 in $\mathbb{Z}[\sqrt{-5}]$ (two factorizations are distinct if the prime factors are not the same up to multiplication by a unit and reordering).

Hint: use the norm.

Exercise 5 (Challenge). Continued fractions and quadratic numbers. We have seen that for $\alpha \in \mathbb{R}$, the continued fraction expansion of α is finite if and only if α is a rational number. In an exercise, we have also seen that for at least some square roots the continued fraction expansion eventually repeats. This is a general phenomenon: show that the continued fraction expansion of $\alpha \in \mathbb{R}$ is eventually repeating if and only if α is a quadratic number.