MATH 350, SPRING 2023

HOMEWORK 8, DUE MARCH 31

(1) This problem extends Fermat's Christmas theorem from primes to arbitrary positive integers. In other words, we completely answer the question: which integers can be written as a sum of two squares?

  (a) Write $a^2 + b^2 = (a + bi)(a - bi)$ and $c^2 + d^2 = (c + di)(c - di)$, then show that $(a^2 + b^2)(c^2 + d^2)$ is the norm of a Gaussian integer. Conclude that a product of sums of squares is a sum of squares.

  (b) Deduce that if the prime factorization of n contains only even powers of primes congruent to 3 modulo 4, then $n = x^2 + y^2$ for some integers x and y.

  (c) Recall that for a rational prime p, the following three conditions are equivalent:
  - p is of type (I) in $\mathbb{Z}[i]$.
  - p is prime in $\mathbb{Z}[i]$.
  - $p \equiv 3 \mod 4$.

  Show that for any $p \equiv 3 \mod 4$, if $p^e \mid a^2 + b^2$ and $p^{e+1} \nmid a^2 + b^2$, then e is even.

(2) Let p be an odd prime, and let a be a primitive root modulo p. Explain why $\left(\dfrac{a}{p}\right) = -1$. Write each element of $\Phi(p)$ as a power of a, then use Euler's Criterion to give yet another proof of Wilson's Theorem.

(3) Compute the following Legendre symbols

$$\left(\frac{3}{7}\right), \left(\frac{2}{37}\right), \left(\frac{-5}{29}\right), \left(\frac{24}{37}\right), \left(\frac{23}{37}\right), \left(\frac{62}{71}\right)$$

(4) A permutation matrix is a matrix whose entries are all either zero or one, and which has exactly one nonzero entry in each column and exactly one nonzero entry in each row. Show that that a permutation matrix permutes the standard basis vectors.

(5) Show that the determinant of a permutation matrix is the sign of the corresponding permutation.

(6) How is a permutation matrix related to its inverse? How are their signs related?

(7) Let r be a primitive root modulo p. Show that multiplication by r is an odd permutation on $\Phi(p)$. If f is a permutation, let f^n denote $f \circ f \circ \cdots \circ f$ (n times). Argue that $\text{sign}(f^n) = (\text{sign}(f))^n$ for all n. Then deduce another proof of Zolotarev's Lemma.

The following two problems are entirely optional, and no credit will be awarded for tuning them in. Try them for fun if you are interested.

(8) Problem 8 from Chapter 8 (pages 220-221)

(9) This problem provides another definition of determinants.

(a) For a matrix with exactly one nonzero entry in each row and column, define the determinant to be the product of the nonzero entries times the sign of the corresponding permutation. For such matrices, explain why this definition agrees with the definition of determinant that you already know.

Now define the determinant of an $n \times n$ matrix A to be the sum

$$\sum_f \left(\prod_i a_{i,f(i)} \right) (-1)^{\mathrm{sign}(f)}$$

Here f ranges over the permutations on $\{1, 2, \ldots n\}$. In other words, we consider the nonzero entries of each permutation matrix, then multiply the corresponding entries of A. We add up those products arising from even permutations and subtract those products arising from odd permutations.

(b) Show that this definition produces the familiar formulas for 2×2 and 3×3 matrices.

(c) Verify that this definition satisfies the following properties

(i) The determinant of the identity matrix is 1.

(ii) Multiplying a row by a (not necessarily nonzero) scalar multiplies the determinant by that scalar.

(iii) The determinant is additive in each row: That is, if A B, and C are all identical except in the j^{th} row, and the j^{th} row of C is the sum of the j^{th} rows of A and B, then the determinant of C is the sum of the determinants of A and B.

(iv) Swapping two rows multiplies the determinant by -1.

(v) A matrix in which one row is a scalar multiple of another has determinant 0.

(vi) Adding a multiple of one row to another does not change the determinant.*Hint: Use part (iii).*