MATH 311, FALL 2020 PRACTICE MIDTERM 2

OCTOBER 28

Each problem is worth 10 points.

Problem 1. Define an elliptic curve and give the addition law for points on an elliptic curve. Prove that the addition law is commutative.

Solution. Let $f(x, y)$ be a cubic polynomial with real coefficients. $C_f(\mathbb{R})$ is an elliptic curve if $f(x, y)$ is irreducible over $\mathbb{R}$ with no singular point in $\mathbb{P}_2(\mathbb{R})$. Declare a point on the curve 0. Define a binary operation on points by AB is the third point on the line connecting AB, counted with multiplicity. Evidently $AB = BA$. Then $A + B = 0(AB)$. Notice $0(AB) = 0(BA)$ so the addition is commutative.

Problem 2.

a. Define the Hamiltonians used in the proof of Lagrange's theorem on the sum of four squares.
b. Prove that if q_1 and q_2 are Hamiltonians, the norm of q_1q_2 is the product of the norms.

Solution.

a. The Hamiltonians are the $\mathbb{Z}$-linear span of $1, i, j, k$ where i, j, k generate the quaternion group $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$.
b. The norm of a Hamiltonian $q = a + bi + cj + dk$ is $N(q) = a^2 + b^2 + c^2 + d^2$. The norm identity can be proved by expanding the product and collecting terms, but an easier proof is as follows. Define $\overline{q} = a - bi - cj - dk$. The conjugate satisfies $\overline{q_1q_2} = \overline{q_2} \cdot \overline{q_1}$. Then $q\overline{q} = \overline{q\overline{q}} = N(q)$ is an integer. Now we can check $N(q_1q_2) = q_1q_2\overline{q_1q_2} = q_1q_2\overline{q_2} \cdot \overline{q_1} = q_1N(q_2)\overline{q_1} = N(q_1)N(q_2)$.

Problem 3.

a. State the principle of inclusion and exclusion.

b. A permutation $\sigma : \{1, 2, ..., n\} \to \{1, 2, ..., n\}$ is a derangement if $\sigma(j) \neq j$ for all j. Using the principle of inclusion and exclusion or otherwise, calculate the number of permutations of $\{1, 2, ..., n\}$ which are derangements.

Solution.

a. The inclusion and exclusion principle states that if $S_1, S_2, ..., S_n$ are subsets of a finite set S, then

$$\left| S \setminus \bigcup_{i=1}^{n} S_i \right| = |S| - \sum_i |S_i| + \sum_{i<j} |S_i \cap S_j| - ... + (-1)^n |S_1 \cap S_2 \cap ... \cap S_n|.$$

b. Let $E_i = \{\sigma : \sigma(i) = i\}$. Thus we wish to count $|S_n \setminus_{j=1}^{n} E_j|$. Since for $j_1 < j_2 < ... < j_k$, $E_{j_1} \cap ... \cap E_{j_k}$ fixes $j_1, ..., j_k$ and permutes the remaining $n-k$ indices, this set has size $(n-k)!$. There are $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ ways of picking k fixed indices. Thus the number of derangements is

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Problem 4. Given infinite continued fraction $\langle a_0, a_1, a_2, ...\rangle$ define recursive sequences

$$h_{-2} = 0,\ h_{-1} = 1,\ h_i = a_i h_{i-1} + h_{i-2}$$
$$k_{-2} = 1,\ k_{-1} = 0,\ k_i = a_i k_{i-1} + k_{i-2}.$$

Explain why $r_n = \frac{h_n}{k_n}$ gives the sequence of convergents to the continued fraction and prove that (r_n) converges.

Solution. We have $h_0 = a_0$, $k_0 = 1$ so $r_0 = \frac{h_0}{k_0}$ is the first convergent. Assume inductively that $\langle a_0, a_1, ..., a_n\rangle = \frac{h_n}{k_n}$. Then

$$\begin{aligned} r_{n+1} &= \langle a_0, a_1, ..., a_n, a_{n+1}\rangle \\ &= \frac{(a_n + \frac{1}{a_{n+1}})h_{n-1} + h_{n-2}}{(a_n + \frac{1}{a_{n+1}})k_{n-1} + k_{n-2}} \\ &= \frac{a_{n+1}(a_n h_{n-1} + h_{n-2}) + h_{n-1}}{a_{n+1}(a_n k_{n-1} + k_{n-2}) + k_{n-1}} = \frac{h_{n+1}}{k_{n+1}}. \end{aligned}$$

We have

$$\begin{pmatrix} h_{n-1} & h_n \\ k_{n-1} & k_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_{n+1} \end{pmatrix} = \begin{pmatrix} h_n & h_{n+1} \\ k_n & k_{n+1} \end{pmatrix}$$

and thus

$$\begin{pmatrix} h_{n-1} & h_n \\ k_{n-1} & k_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & a_0 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix}.$$

It follows that $h_{n-1}k_n - h_n k_{n-1} = (-1)^n$. Thus

$$r_n - r_{n-1} = \frac{h_n k_{n-1} - h_{n-1} k_n}{k_{n-1} k_n} = \frac{(-1)^{n-1}}{k_{n-1} k_n}.$$

Since $k_{n-1}k_n$ increases to infinity with n, the limit of (r_n) exists by the alternating series test applied to the successive differences.