PROBLEMS FROM THE HISTORY OF MATHEMATICS – FINAL EXAM –

DUE FRIDAY, 5/11/2018

Exercise 1. Let A be a convex polyhedron. Prove that Euler's formula $V - E + F = 2$ holds for A, in which V, E, and F denote the number of vertices, edges, and faces of A, respectively. *Hint: Induction.*

Exercise 2. Derive Machin's formula,

$$\frac{\pi}{4} = 4 \arctan \frac{1}{5} - \arctan \frac{1}{239},$$

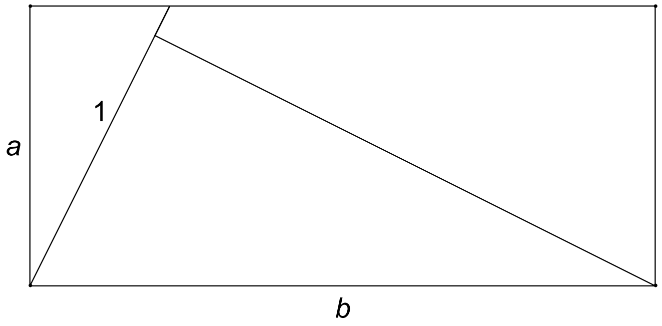
by relating each quantity to the argument of a complex number.

Exercise 3. Suppose that Λ is a saturated sphere packing in $\mathbb{R}^n$.

a. Show that the packing of spheres with centers at the points in Λ and radii equal to 2 covers $\mathbb{R}^n$.
b. Show that the sphere packing density in $\mathbb{R}^n$ is at least 2^{-n}.

Exercise 4. The Wallace–Bolyai–Gerwien Theorem states that two polygonal figures can be dissected into each other if and only if they have equal area. One way to show this is to prove that every figure of area X can be dissected into a rectangle of side lengths 1 and X. This exercise shows two steps of this process.

a. Prove that any triangle can be dissected into rectangles. *Hint: First show that any triangle can be dissected into two right triangles.*
b. Prove that the $a \times b$ rectangle can be dissected into a $1 \times ab$ rectangle. *Hint: First consider the case $a < 1 < b$. Study the figure below:*



Exercise 5. The Kronecker–Weber theorem states that any algebraic number with an abelian Galois group can be written as a sum of rational multiples of roots of unity. In particular, any quadratic irrational should have this property. Show that this follows from the following result of Gauss:

Theorem (Gauss)**.** *Let p be prime. We have*

$$\sum_{n=0}^{p-1} e^{2\pi i n^2/p} = \begin{cases} \sqrt{p}, & p \equiv 1 \mod 4 \\ i\sqrt{p}, & p \equiv 3 \mod 4 \end{cases}.$$

Sums like these were first studied by Gauss and are named *Gauss sums* in his honor. They are key to one of Gauss' proofs of Quadratic Reciprocity.

Exercise 6. In this exercise, we verify Motzkin's claim that the polynomial

$$P(x,y) = x^4y^2 + x^2y^4 + 1 - 3x^2y^2$$

is not a sum of squares of polynomials, despite being non-negative.

a. Prove that $P(x,y) \geq 0$ on $\mathbb{R}^2$. *Hint: The AM-GM Inequality.*
b. Suppose that $P(x,y) = \sum f_j(x,y)^2$. Prove that each f_j is of the form
$$f_j(x,y) = a_j + b_jxy + c_jx^2y + d_jxy^2.$$
c. Derive a contradiction to (b) by comparing coefficients.

Exercise 7. Use the fundamental theorem of algebra and the Brahmagupta–Fibonacci identity to prove that every non-negative polynomial $f(x) \in \mathbb{R}[x]$ may be written as a sum of squares of polynomials.

Exercise 8. The RSA cryptosystem, which appeared in 1976, was one of the first *public key cryptosystems.* Public key cryptosystems allow one-way transmission of encrypted data between parties who have never met. In this exercise, we see how the RSA scheme works.

a. Suppose that Alice wants to send a message to Bob. Beforehand, Bob prepares his public key by choosing two large primes p and q. He publishes pq and some k which is coprime to $\varphi(pq)$.
b. To send the message $m \bmod pq$, Alice computes $m^k \bmod pq$. (Any would-be eavesdropper is unable to recover m from m^k, since this amounts to the Discrete Log Problem.)
c. To decrypt the message, Bob computes u such that
$$ku + \varphi(pq)v = 1.$$
Why is $(m^k)^u \equiv m \bmod pq$?
d. An attacker who knows p and q could easily compute $\varphi(pq)$ and decrypt Alice's message the same way that Bob did. Prove that an attacker who only knows pq and $\varphi(pq)$ can generate p and q without brute force factoring. (In other words, show that computing $\varphi(pq)$ is just as hard as factoring pq. Factorization is considered a hard problem without quantum computers.)