Theory of Computation: Problem Set 1

WEDNESDAY, 17 JANUARY 2024

Name: ______________________________

1. Prove by induction that,

$$1^3 + 2^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$$

This problem is from André Weil, *Number Theory for Beginners*.

2. You shall prove using the steps below, that for p and odd prime, p divides $2^p - 2$. For instance, for $p = 3$, then $2^3 - 2 = 6$, and 6 is divisible by 3. This proof is from the book *Shape* by Jordan Ellenberg. I will walk you through the proof.

   Consider a necklace with n beads, and the beads are either white or black. To keep track, let the beads be numbered $0, 1, 2, \ldots, n-1$. A coloring is a map from the integers 0 to $n-1$ to the set $\{0, 1\}$. Consider action σ_1 of rotating necklace one position clockwise,

$$(\sigma_1 C)(i) = C((i-1) \bmod n).$$

   Define $\sigma_i = \sigma_1 \circ \sigma_{i-1}$ for $i > 1$, and σ_0 to be the identity.

   Example: The all white necklace is the map $C_w(i) = 0$ for all i, and all black is $C_b(i) = 1$ for all i. Since it makes no matter on a necklace of one color if it beads are moved forward $\sigma_i C_w = C_w$ and $\sigma_i C_b = C_b$ for all i.

   Example: For each δ there is a necklace white beads except bead δ is black,

$$C_\delta(i) = \begin{cases} 1 & \text{if } i = \delta \\ 0 & \text{else.} \end{cases}$$

   Then $\sigma_i C_\delta = C_{i+\delta}$.

   We define the orbit $\mathcal{O}$ of a coloring to all possible colorings by rotations from that coloring,

$$\mathcal{O}(C) = \{ \sigma_i(C) \mid i = 0, 1, \ldots, n-1 \}$$

   Examples: The orbit of C_w has only one coloring it it. The orbit of a C_δ has n colorings in it.

   An illuminating case is for $n = 4$ (not prime) and the coloring,

$$C(i) = \begin{cases} 1 & \text{if } i = 0 \text{ or } 2 \\ 0 & \text{else} \end{cases}$$

   Then $\mathcal{O}(C) = \{ C, \sigma_1 C \}$.

(a) List all orbits for a necklace with 4 beads.

HINT: The sizes of the orbits are 1, 1, 2, 4, 4 and 4.

(b) List all orbits for a necklace with 5 beads.

(c) Consider the minimum integer $i > 0$ such that for a coloring C, $\sigma_i C = C$. Prove that i divides n.

HINT: If $\sigma_i C = C$ then $\sigma_{2\,i} C = C$ and certainly $\sigma_n C = C$.

(d) For n a prime, prove n divides $2^n - 2$.

HINT: If n is a prime, what are the allowable orbit sizes, and how does this group up the 2^n different colorings into orbits.

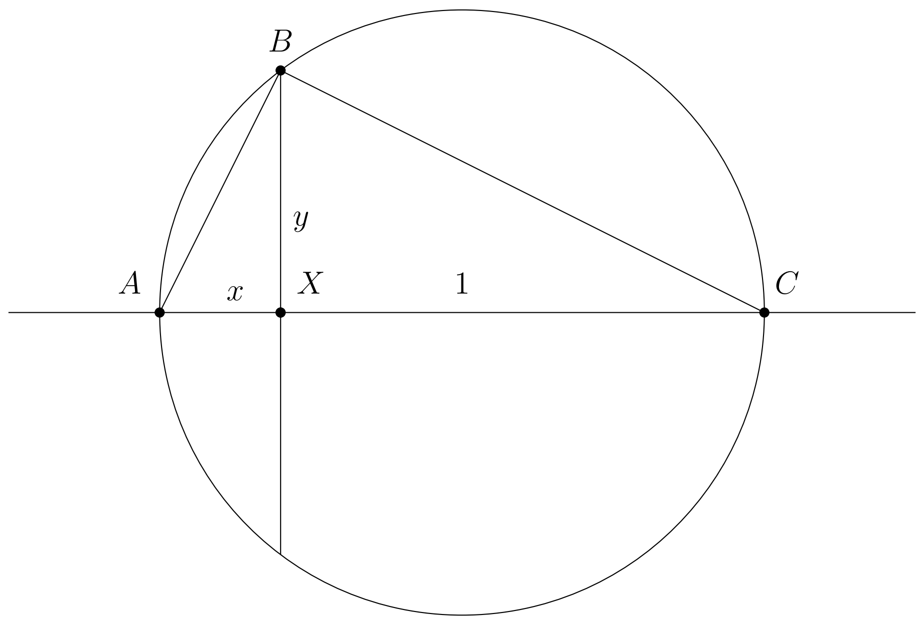
3. We will prove the method by which ancient mathematicians calculated the square root using a ruler and compass construction. Let $x < 1$ be a length.

   (a) Using a ruler, draw a line AC that is divided point X such that the length of AX is x and the length of XC is 1.

   (b) Draw a circle with AC as the diameter. This can be done by bisecting AC and then setting the compass down with its point on the point of bisection and pencil on A or C.

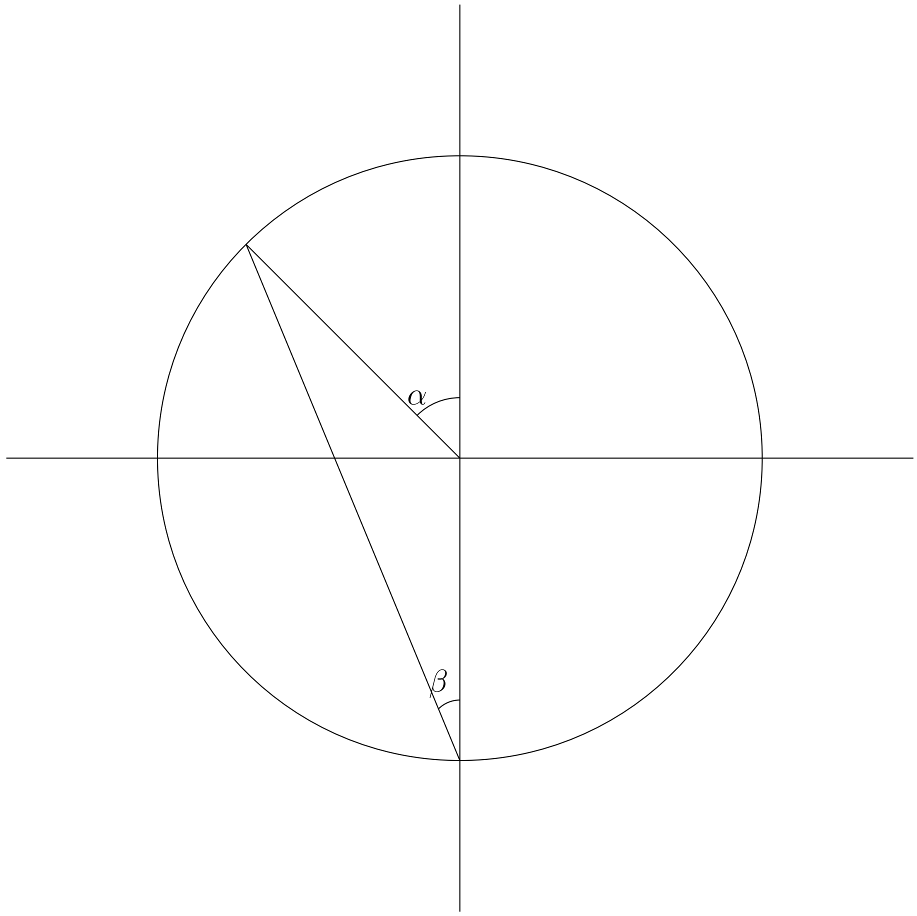
   (c) At point X erect a perpendicular. This can be done with a ruler and compass construction.

   (d) The length XB is the square root of the length AX.



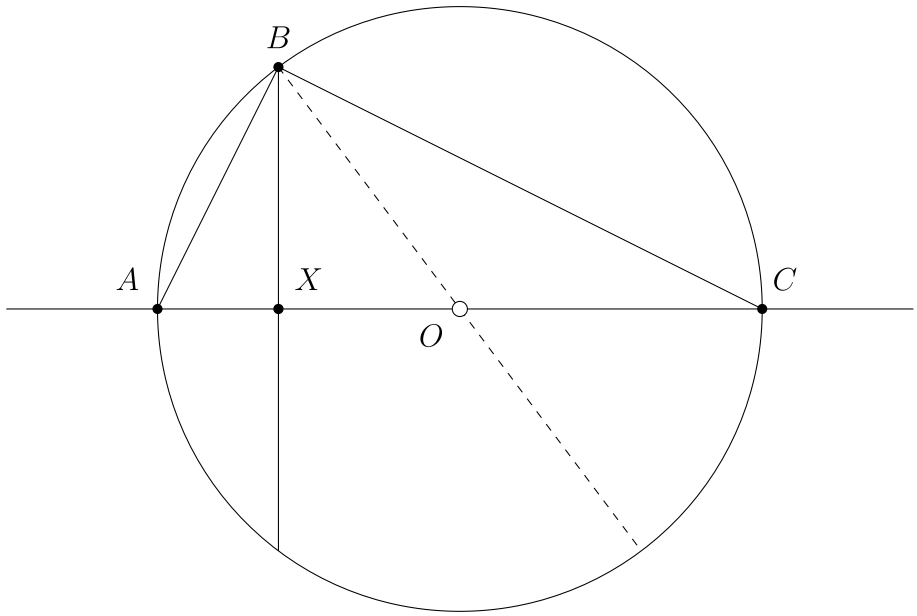
I will walk you through the proof in three steps.

STEP 1: Prove that in the following diagram, $\alpha = 2\,\beta$.



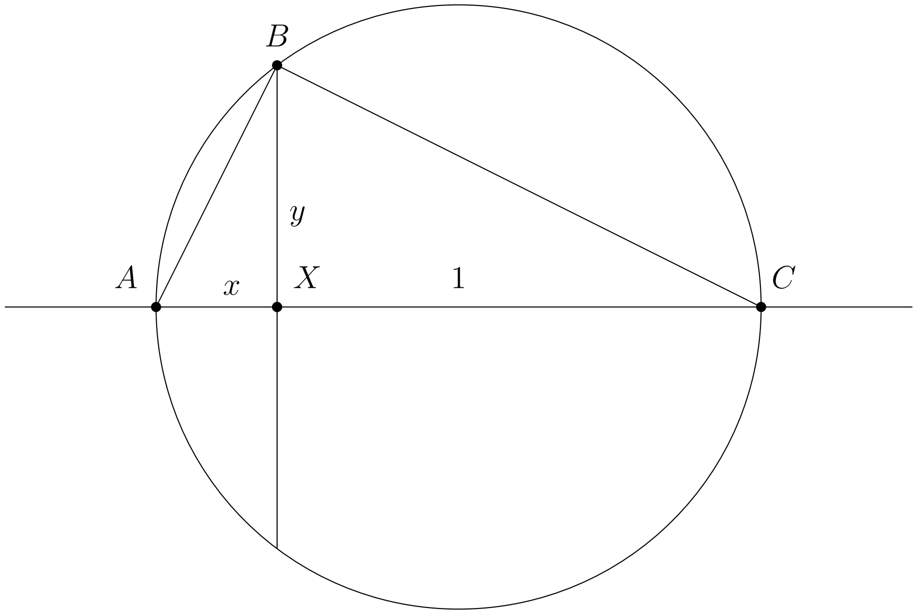
HINT: There is an isosceles triangle. Remember that the angles of a triangle add up to π.

STEP 2: Prove that angle ABC is a right angle.



HINT: The line from B through the center O of the circle gives angle ABC as the sum of two angles ABO and OBC, for which step 1 applies.

STEP 3: Show $x = y^2$, where $x = |AX|$ and $y = |BX|$.



HINT: From the right triangle ABC we have $|AB|^2 + |BC|^2 = |AC|^2$.
ANOTHER HINT: From the right triangle ABX we have another expression for $|AB|^2$.
ANOTHER HINT: $|AC|^2 = (x+1)^2$.