UBC Math Circle 2022 Problem Set 2

1. Let
$$(1 + x + x^2)^n = a_0 + a_1 x + a_2 x^2 + \cdots + a_{2n} x^{2n}$$
be an identity in x. Find $a_0 + a_2 + a_4 + \cdots + a_{2n}$ in terms of n.

> **Solution:** (Joanna Weng)
>
> Substituting $x = \pm 1$, we see that
> $$1 = a_0 - a_1 + a^2 - a_3 + \cdots - a_{2n-1} + a_{2n},$$
> $$3^n = a_0 + a_1 + a^2 + a_3 + \cdots + a_{2n-1} + a_{2n},$$
> which added together gives
> $$3^n + 1 = 2(a_0 + a_2 + a_4 + \cdots + a_{2n})$$
> $$\implies a_0 + a_2 + a_4 + \cdots + a_{2n} = \frac{3^n + 1}{2}.$$

2. Let $f(x) = x^2 - 2$. For each $n \in \mathbb{N}$, we let $f^{\circ n} = f \circ f \circ \ldots \circ f$ (n times). Prove that for each $n \in \mathbb{N}$ there exist 2^n real numbers x such that $f^{\circ n}(x) = x$. (Hint: Let x be a real number such that $f^{\circ n}(x) = 0$ or ± 2 and consider what happens to x under $f^{\circ(n+1)}$.)

> **Solution:** (Oakley Edens)
>
> First we prove the following lemma.
>
> **Lemma 1.** *For every integer $n \geq 1$ there exists an ordered list of real numbers $L_n = \{x_1 < \ldots < x_{2^n+1}\}$ in the interval $[-2, 2]$ such that $f^{\circ n}(x_i) = -2$ if i is even and $f^{\circ n}(x_i) = 2$ if i is odd.*
>
> *Proof (Lemma 1).* The base case $n = 1$ is clear since $L_1 = \{-2, 0, 2\}$ is such a list. Next, suppose it is true for $n \leq m$ for some m. By the induction hypothesis, there exists a list $L_m = \{x_1, \ldots, x_{2^m+1}\}$ satisfying the desired property. Since $f^{\circ m}$ is continuous, by the intermediate value theorem there exists a $y_i \in (x_i, x_{i+1})$ for every $1 \leq i \leq 2^m$, for which $f^{\circ m}(y_i) = 0$. Define $L_{m+1} = \{x_1, y_1, x_2, y_2, \ldots, y_{2^m}, x_{2^m+1}\}$. L_{m+1} is clearly an ordered list containing real numbers in the interval $[-2, 2]$ with $|L_{m+1}| = |L_m| + 2^m = 2^{m+1} + 1$. Finally, note that the odd positions in this list are occupied by the elements $\{x_i\}$ while the even positions are occupied by the elements $\{y_i\}$. It follows immediately that $f^{\circ(m+1)}(x_i) = f(f^{\circ m}(x_i)) = (\pm 2)^2 - 2 = 2$ while $f^{\circ(m+1)}(y_i) = f(f^{\circ m}(y_i)) = (0)^2 - 2 = -2$. Thus L_{m+1} is the desired list. □

Now we prove the main result. Fix $n \geq 1$ and let $L_n = \{x_1, \ldots, x_{2^n+1}\}$ be an ordered list of real numbers with the property stated in Lemma 1. Since x_i and x_{i+1} are in $[-2, 2]$ for each $1 \leq i \leq 2^n$, it follows that $f^{\circ n}(x_i) - x_i < 0$ if and only if $f^{\circ n}(x_{i+1}) - x_{i+1} \geq 0$ with equality only when $x_{i+1} = 2$. Then by the intermediate value theorem, the function $f^{\circ n}(x) - x$ has a root in each interval $(x_i, x_{i+1}]$ where $1 \leq i \leq 2^n$, which implies that it has at least 2^n real roots. Since $\deg(f^{\circ n}(x) - x) = 2^n$, the fundamental theorem of algebra says that $f^{\circ n}(x) - x$ can have at most 2^n roots. Thus $f^{\circ n}(x) - x$ has precisely 2^n real roots.

3. Let S be a subset of $\mathbb{R}^2$. It is called *convex* if for (a, b), $(c, d) \in S$, the line segment joining (a, b) and (c, d) lies entirely in S. It is *centrally symmetric* if whenever $(a, b) \in S$, then $(-a, -b) \in S$. Prove that if the area of a convex and centrally symmetric set S is greater than 4, then S contains a point of $\mathbb{Z}^2$ other than $(0, 0)$. (Hint: Consider the map $(x, y) \mapsto (x \bmod 2, y \bmod 2)$ on S. Can this map be injective if the area of S is greater than 4?)

Solution: (Neo Huang)

Let f denote the map $(x, y) \mapsto (x \bmod 2, y \bmod 2)$. Observe that f maps points in S to points in the 2×2 square $[0, 2) \times [0, 2)$. Hence, the area of $f(S)$ is less than or equal to 4. We can show that is map is area preserving whenever it is injective since

$$\begin{aligned}
\text{Area}(f(S)) &= \sum_{(m,n)\in\mathbb{Z}^2} \text{Area}(f(S \cap ([2m, 2m+2) \times [2n, 2n+2)))) \\
&= \sum_{(m,n)\in\mathbb{Z}^2} \text{Area}(S \cap ([2m, 2m+2) \times [2n, 2n+2))) = \text{Area}(S),
\end{aligned}$$

where the second equality is because f restricted to each $[2m, 2m+2) \times [2n, 2n+2)$ is just a translation.

But S has an area greater than 4 and $f(S)$ has an area less than or equal to 4; hence, f cannot be injective. So there exist two points p_1 and p_2 in S such that $f(p_1) = f(p_2)$. But then $p_2 = p_1 + (2i, 2j)$ for some integers i and j not both zero. Since S is centrally symmetric, the point $-p_1$ is also in S. Furthermore, since S is convex, the line segment joining $-p_1$ and p_2 lies entirely in S. Therefore, the midpoint of this segment

$$\frac{1}{2}(-p_1 + p_2) = \frac{1}{2}(-p_1 + p_1 + (2i, 2j)) = (i, j)$$

lies in S. Since i and j are integers that are not both zero, it follows that S contains a point of $\mathbb{Z}^2$ other than $(0, 0)$.

4. (a) Suppose $\alpha \in \mathbb{C}$ is a root of some nonzero polynomial in $\mathbb{Q}[x]$. Write $\mathbb{Q}[\alpha]$ to denote the set $\{P(\alpha) \mid P \in \mathbb{Q}[x]\}$. Show that for any $\beta \in \mathbb{Q}[\alpha] \setminus \{0\}$, there exists $\gamma \in \mathbb{Q}[\alpha]$ such that $\beta\gamma = 1$. (You may assume that $\mathbb{Q}[\alpha]$ is a finite-dimensional $\mathbb{Q}$-vector space, a consequence of which is that there exists $n \in \mathbb{N}$ such that for all $v_1, \ldots, v_n \in \mathbb{Q}[\alpha]$, there exist $\lambda_1, \ldots, \lambda_n \in \mathbb{Q}$ not all zero such that $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$.)

Solution: (Victor Wang)

Let $\beta \in \mathbb{Q}[\alpha] \setminus \{0\}$. We show that there exists $\gamma \in \mathbb{Q}[\alpha]$ such that $\beta\gamma = 1$. Since $\mathbb{Q}[\alpha]$ is a finite-dimensional $\mathbb{Q}$-vector space, for some $n \in \mathbb{N}$ there is a nontrivial $\mathbb{Q}$-linear relation between $\beta^1, \ldots, \beta^n$ of the form $\lambda_1\beta^1 + \cdots + \lambda_n\beta^n = 0$ (note each $\beta^i \in \mathbb{Q}[\alpha]$). So β is the root of some nonzero polynomial in $\mathbb{Q}[x]$.

Therefore, there exists a nonzero polynomial $Q \in \mathbb{Q}[x]$ of minimum degree vanishing on β. Since $\beta \neq 0$, the constant term of Q is not zero, or else β would be a root of nonzero $\frac{1}{x}Q \in \mathbb{Q}[x]$ of smaller degree. Let c be the nonzero constant term of Q. Then $S = -\frac{1}{cx}(Q - c)$ is a polynomial in $\mathbb{Q}[x]$. Since $\beta \in \mathbb{Q}[\alpha]$, it follows that $S(\beta) \in \mathbb{Q}[\alpha]$. Then since $Q(\beta) = 0$, taking $\gamma = S(\beta)$, we see that $\beta\gamma = -\frac{\beta}{c\beta}(Q(\beta) - c) = 1$.

(b) Let $\alpha \in \mathbb{C}$ be a root of the polynomial $x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$. You may assume that α and $1 + \alpha + \alpha^2$ are nonzero. Write α^{-1} and $(1 + \alpha + \alpha^2)^{-1}$ as elements of $\mathbb{Q}[\alpha]$.

Solution: (Victor Wang)

Since $x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$ has a nonzero constant term and vanishes on α, by our solution to part (a), the inverse of α is $-\frac{1}{2}(\alpha^3 - 4\alpha)$.

To compute the inverse of $1 + \alpha + \alpha^2$, we will need a different approach since it is difficult to find a polynomial in $\mathbb{Q}[x]$ vanishing $1 + \alpha + \alpha^2$. We will apply the Euclidean (division) algorithm to polynomials in $\mathbb{Q}[x]$. By the division algorithm, $x^4 - 4x^2 + 2 = (x^2 - x - 4)(x^2 + x + 1) + (5x + 6)$. Again by the division algorithm, $x^2 + x + 1 = \left(\frac{1}{5}x - \frac{1}{25}\right)(5x + 6) + \frac{31}{25}$.

So

$$\begin{aligned}
1 &= \frac{25}{31}(x^2 + x + 1) - \frac{25}{31}\left(\frac{1}{5}x - \frac{1}{25}\right)(5x + 6) \\
&= \frac{25}{31}\left[1 + \left(\frac{1}{5}x - \frac{1}{25}\right)(x^2 - x - 4)\right](x^2 + x + 1) \\
&\quad - \frac{25}{31}\left(\frac{1}{5}x - \frac{1}{25}\right)(x^4 - 4x^2 + 2).
\end{aligned}$$

Evaluating the above expression at α, we deduce that

$$(1+\alpha+\alpha^2)^{-1} = \frac{25}{31}\left[1+\left(\frac{1}{5}\alpha-\frac{1}{25}\right)(\alpha^2-\alpha-4)\right]$$
$$= \frac{1}{31}(5\alpha^3-6\alpha^2-19\alpha+29).$$

5. Let $P(z) = a_d z^d + \cdots + a_1 z + a_0$ be a polynomial with complex coefficients. The *reverse* of P is defined by

$$P^*(z) = \overline{a_0} z^d + \overline{a_1} z^{d-1} + \cdots + \overline{a_d}.$$

(a) Prove that

$$P^*(z) = z^d \overline{P\left(\frac{1}{\bar{z}}\right)}.$$

Solution: (Arvin Sahami)
Observe that

$$\overline{P\left(\frac{1}{\bar{z}}\right)} = \bar{a_0} + \bar{a_1}\frac{1}{z} + ... + \bar{a_d}\frac{1}{z^d},$$

which implies that $P^*(z) = z^d \overline{P\left(\frac{1}{\bar{z}}\right)}$.

(b) Let m be a positive integer and let $q(z)$ be a monic nonconstant polynomial with complex coefficients. Suppose that all roots of $q(z)$ lie inside or on the unit circle. Prove that all roots of the polynomial

$$Q(z) = z^m q(z) + q^*(z)$$

lie on the unit circle.

Solution: (Arvin Sahami)
Let $\{z_i\}$ be the roots of q. Then we can write $q(x) = (z-z_1)...(z-z_n)$ where $|z_i| \leq 1$. Taking the reverse of q we get

$$q^*(z) = z^n \overline{q\left(\frac{1}{\bar{z}}\right)} = z^n\left(\frac{1}{z}-\bar{z_1}\right)...\left(\frac{1}{z}-\bar{z_n}\right) = z^n\left(\frac{1-z\bar{z_1}}{z}\right)...\left(\frac{1-z\bar{z_n}}{z}\right)$$
$$= (1-z\bar{z_1})\cdots(1-z\bar{z_n}).$$

Setting $Q(z) = 0$, we get

$$z^m q(z) = -q^*(z) \implies z^m(z - z_1)...(z - z_n) = -(1 - z\bar{z_1})...(1 - z\bar{z_n}) \quad (1)$$
$$\implies |z^m(z - z_1)...(z - z_n)| = |(1 - z\bar{z_1})...(1 - z\bar{z_n})| \quad (2)$$

Suppose $z = z_i$ for some $1 \leq i \leq n$. Then (1) implies that $1 - z_i z_j = 0$, which means that $|z| = |z_i| = |z_j| = 1$.

On the other hand, suppose that $z \neq z_i$. By (2), observe that

$$|z|^m = |z^m| = \frac{|1 - z\bar{z_1}|}{|z - z_1|} \cdots \frac{|1 - z\bar{z_n}|}{|z - z_n|}. \quad (3)$$

If $|z| \leq 1$, then $(1-|z|^2)(1-|z_i|^2) \geq 0$ for each $1 \leq i \leq n$. But then $|z|^2|z_i|^2-1 \geq |z|^2 + |z_i|^2$, which implies that

$$|1 - z\bar{z_i}|^2 = (1 - z\bar{z_i})(1 - \bar{z}z_i) \geq (z - z_i)(\bar{z} - \bar{z_i}) = |z - z_i|^2.$$

Hence, by (3), $|z|^m \geq 1$ so that $|z| \geq 1$. Since we assumed that $|z| \leq 1$, we see that $|z| = 1$ as desired.

A similar argument shows that $|z| = 1$ when $|z| \geq 1$.