UBC Math Circle 2023 Problem Set 1 Solutions

Problem 1.

The sequence given by $x_0 = a, x_1 = b$, and

$$x_{n+1} = \frac{1}{2}(x_{n-1} + \frac{1}{x_n})$$

is periodic.

Prove that $ab = 1$.

Solution: manipulate the equation:

$$x_{n+1}x_n = \frac{1}{2}(x_n x_{n-1} + 1), x_{n+1}x_n + K = \frac{1}{2}(x_n x_{n-1} + 1) + K \overset{!}{=} \frac{1}{2}(x_n x_{n-1} + K)$$

$$\implies K + \frac{1}{2} = \frac{K}{2} \implies K = -1$$

thus

$$x_{n+1}x_n - 1 = \frac{1}{2}(x_n x_{n-1} - 1) = \frac{1}{2^n}(ab - 1)$$

but since x_n is periodic, $x_{n+1}x_n = ab$ for some arbitrary large index n, then $ab - 1 = \frac{1}{2^n}(ab - 1) \implies ab = 1$. □

Problem 2. Chebyshev polynomials $T_n(x), U_n(x)$ are defined by $T_0(x) = 1, T_1(x) = x, T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$ and $U_0(x) = 1, U_1(x) = 2x, U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x)$, and they are determined by the equalities

$$\cos(n\theta) = T_n(\cos(\theta)), \quad \frac{\sin((n+1)\theta)}{\sin\theta} = U_n(\cos\theta)$$

For $n \geq 1$, try to prove

$$\frac{T_n(x)}{\sqrt{1-x^2}} = \frac{(-1)^n}{1 \cdot 3 \cdot 5 \cdots (2n-1)} \frac{d^n}{dx^n}(1-x^2)^{n-\frac{1}{2}}$$

$$U_n(x)\sqrt{1-x^2} = \frac{(-1)^n(n+1)}{1 \cdot 3 \cdot 5 \cdots (2n+1)} \frac{d^n}{dx^n}(1-x^2)^{n+\frac{1}{2}}$$

Solution: For the first identity we first divide and get

$$\frac{T_{n+1}(x)}{\sqrt{1-x^2}} = 2x\frac{T_n(x)}{\sqrt{1-x^2}} - \frac{T_{n-1}(x)}{\sqrt{1-x^2}}$$

As for the recurrence relation, we compute

$$\frac{d^{n+1}}{dx^{n+1}}(1-x^2)^{n+1-\frac{1}{2}} = \frac{d^n}{dx^n}\frac{d}{dx}(1-x^2)^{n+1-\frac{1}{2}}$$

$$= \frac{d^n}{dx^n}(n+1-\frac{1}{2})(1-x^2)^{n-\frac{1}{2}}(-2x)$$

$$= -(2n+1)x\frac{d^n}{dx^n}(1-x^2)^{n-\frac{1}{2}} - n(2n+1)\frac{d^{n-1}}{dx^{n-1}}(1-x^2)^{n-\frac{1}{2}}$$

dividing $1 \cdot 3 \cdots (2n+1)(-1)^{n+1}$ we end up

$$\frac{(-1)^{n+1}}{1 \cdot 3 \cdots (2n+1)} \frac{d^{n+1}}{dx^{n+1}} (1-x^2)^{n+1-\frac{1}{2}}$$

$$= \frac{(-1)^n}{1 \cdot 3 \cdots (2n-1)} x \frac{d^n}{dx^n} (1-x^2)^{n-\frac{1}{2}} - \frac{n(-1)^{n-1}}{1 \cdot 3 \cdots (2n-1)} \frac{d^{n-1}}{dx^{n-1}} (1-x^2)^{n-\frac{1}{2}}$$

where we are thrilled to realize that the second term on the last line before would have to be $U_{n-1}(x)\sqrt{1-x^2}$.

Setting

$$t_{n+1}(x) := \frac{(-1)^{n+1}}{1 \cdot 3 \cdots (2n+1)} \frac{d^{n+1}}{dx^{n+1}} (1-x^2)^{n+1-\frac{1}{2}}$$

$$u_{n-1}(x) := \frac{n(-1)^{n-1}}{1 \cdot 3 \cdots (2n-1)} \frac{d^{n-1}}{dx^{n-1}} (1-x^2)^{n-\frac{1}{2}}$$

and we wanna show $t_n(x) = \frac{T_n(x)}{\sqrt{1-x^2}}, u_n(x) = \sqrt{1-x^2}U_n(x)$. Omitting the base case checks, assuming it holds true for all $k < n$, using the inductive hypothesis we get

$$t_n(x) = x\frac{T_{n-1}(x)}{\sqrt{1-x^2}} - \sqrt{1-x^2}U_{n-2}(x)$$

it is easy to check by the trignometric definition that

$$T_{n+1}(x) = xT_n(x) - (1-x^2)U_{n-1}(x)$$

which would yield $t_n(x) = \frac{T_n(x)}{\sqrt{1-x^2}}$.

On the other hand the inductive step to $u_{n-1}(x)$ is done by checking $u_{n-1}(x)$ and $\sqrt{1-x^2}U_{n-1}(x)$ has the same derivatives and coincide at $x = 1$. It is easy to check that both equal 0 at $x = 1$, and

$$\frac{d}{dx}\sqrt{1-x^2}U_{n-1}(x) = \frac{-x}{\sqrt{1-x^2}}U_{n-1}(x) + \sqrt{1-x^2}U_{n-1}^{'}(x)$$

by the inductive hypothesis and simple observation

$$u_{n-1}^{'}(x) = -nt_n(x) = \frac{-nT_n(x)}{\sqrt{1-x^2}}$$

so we are left to check that

$$-xU_{n-1}(x) + (1-x^2)U_{n-1}'(x) = -nT_n(x)$$

which according to the trignometric relationship translates to

$$-\cos(x)\frac{\sin(nx)}{\sin(x)} + \sin^2(x)\frac{n\cos(nx)\sin(x) - \cos(x)\sin(nx)}{\sin^2(x)}\frac{1}{\sin(x)} = -n\cos(nx)$$

which is also easy to check. And we are done with the induction step, the proof is complete. □

Problem 3.

Let $\mathbb{Q}[\zeta_5] = \{a_0 + a_1\zeta_5 + a_2\zeta_5^2 + a_3\zeta_5^3 + a_4\zeta_5^4 : a_i \in \mathbb{Q}\}$ and $\mathbb{Z}[\zeta_5] = \{a_0 + a_1\zeta_5 + a_2\zeta_5^2 + a_3\zeta_5^3 + a_4\zeta_5 : a_i \in \mathbb{Z}\}$, where ζ_5 is a primitive 5th root of unity. Note that $\mathbb{Q}[\zeta_5]$ is a field (equipped with $+$ and $\cdot$ from $\mathbb{C}$ it is closed under addition/multiplication and has additive/multiplicative inverses) while $\mathbb{Z}[\zeta_5]$ is a ring (it is closed under addition/multiplication, has additive inverses but not necessarily multiplicative inverses).

(a) Define $\sigma_1 : \mathbb{Q}[\zeta_5] \to \mathbb{Q}[\zeta_5]$ by $\sigma_1(z) = z$ and $\sigma_2 : \mathbb{Q}[\zeta_5] \to \mathbb{Q}[\zeta_5]$ by $\sigma_2(\sum_{i=0}^4 a_i\zeta_5^i) = \sum_{i=0}^4 a_i\zeta_5^{2i}$. Note the following properties of σ_i: $\sigma_i(z+w) = \sigma_i(z) + \sigma_i(w)$ and $\sigma_i(zw) = \sigma_i(z)\sigma_i(w)$. (These are two of the four field automorphisms on $\mathbb{Q}[\zeta_5]$, with the other two being $\overline{\sigma}_i$). We have a map $N : \mathbb{Q}[\zeta_5] \to \mathbb{R}$ given by $N(z) = |\sigma_1(z)\sigma_2(z)|^2$. (In fact you can check that $N(z) \in \mathbb{Q}$). Prove that for any $a, b \in \mathbb{Z}[\zeta_5]$ with $b \neq 0$, there exist $q, r \in \mathbb{Z}[\zeta_5]$ such that $a = qb + r$ and $N(r) < N(b)$.

(b) We call an element $p \in \mathbb{Z}[\zeta_5]$ prime if whenever $p \mid ab$ for $a, b \in \mathbb{Z}[\zeta_5]$, we have either $p \mid a$ or $p \mid b$. Use (a) to prove that every $z \in \mathbb{Z}[\zeta_5]$ may be written uniquely as $z = p_1^{a_1} \dots p_n^{a_n}$ where the p_i are prime and the $a_i \geq 1$ up to rearrangement and multiplication by unit elements u satisfying $N(u) = 1$ (that is two representations are considered equivalent if one can get from one to the other by rearranging terms and multiplying by units).

(c) Use (b) to prove that the equation $x^5 + y^5 = z^5$ has no solutions in nonzero integers.

Proof.

(a) Let $\zeta = \zeta_5$. Let $z = \sum_{i=0}^4 u_i\zeta^i$. Then $\sqrt{N(z)} = \sqrt{|\sigma_1(z)|^2|\sigma_2(z)|^2} \leq \frac{1}{2}(|\sigma_1(z)|^2 + |\sigma_2(z)|^2)$ by AM-GM. A computation shows that $\frac{1}{2}(|\sigma_1(z)|^2 + |\sigma_2(z)|^2) = \frac{1}{4}\sum_{0\leq i<j\leq 4}(u_i - u_j)^2$. We now prove the following lemma: For any choice of five real numbers $\{u_i\}_{0\leq i\leq 4}$ one can find real numbers $\{v_i\}_{0\leq i\leq 4}$ such that $u_i - v_i \in \mathbb{Z}$ for all i and such that $\sum_{0\leq i<j\leq 4}(v_i - v_j)^2 < 4$. Note that for any $v \in \mathbb{R}$, we have

$$\sum_{0\leq i<j\leq 4}(v_i - v_j)^2 = 5\sum_{i=0}^4 (v_i - v)^2 - \left(\sum_{i=0}^4 (v_i - v)\right)^2 \leq 5\sum_{i=0}^4 (v_i - v)^2$$

We note that we can choose the v_i such that $u_i - v_i \in \mathbb{Z}$, the v_i all lie in an interval of length < 1 such that the there are k, l with $|v_k - v_l| \leq \frac{1}{5}$. Indeed, we can choose the v_i satisfying the first two conditions by taking $0 \leq v_i < 1$. If the smallest interval containing the v_i has length $\leq \frac{4}{5}$ then the third condition is clearly satisfied. Otherwise, the smallest interval has length between $\frac{4}{5}$ and 1. We may then subtract 1 from the largest of the v_i, clearly the other two conditions are still satisfied. Take $v = \frac{v_k + v_l}{2}$. Then $|v_k - v| \leq \frac{1}{10}$ and $|v_l - v| \leq \frac{1}{10}$. To the remaining v_i, we may add or subtract 1 until $|v_i - v| \leq \frac{1}{2}$. The v_i still satisfy the condition $u_i - v_i \in \mathbb{Z}$. Moreover,

$$\sum_{0\leq i<j\leq 4}(v_i - v_j)^2 \leq 5\sum_{i=0}^4 (v_i - v)^2 \leq 5(\frac{1}{10^2} + \frac{1}{10^2} + \frac{1}{2^2} + \frac{1}{2^2} + \frac{1}{2^2}) = \frac{77}{20} < 4.$$

And the v_i satisfy the second condition as well. Returning to our original problem, let $a, b \in \mathbb{Z}[\zeta]$ with $b \neq 0$. Since $\mathbb{Q}[\zeta]$ is a field, we may write $\frac{a}{b}$ as $\sum_{i=0}^4 u_i\zeta^i$ with $u_i \in \mathbb{Q}$. By the lemma above, there exist $v_i \in \mathbb{R}$ such that $u_i - v_i \in \mathbb{Z}$ and such that $\frac{1}{4}\sum_{0\leq i<j\leq 4}(v_i - v_j)^2 < 1$. Since $u_i \in \mathbb{Q}$, it follows that $v_i \in \mathbb{Q}$. Let $c = \sum_{i=0}^4 v_i\zeta^i$. Then $c \in \mathbb{Q}[\zeta]$, $\frac{a}{b} - c \in \mathbb{Z}[\zeta]$ and $N(c) < 1$ by the result above. Let $q = \frac{a}{b} - c$ and $r = bc$. Clearly $a = qb + r$ and since $N(z)$ is multiplicative, it follows that $N(r) = N(bc) < N(b)$ as desired.

(b) We call an element $a \in \mathbb{Z}[\zeta]$ irreducible if a is not a unit and $a = bc$ with $b, c \in \mathbb{Z}[\zeta]$ implies that one of b, c is a unit (that is $b^{-1}, c^{-1} \in \mathbb{Z}[\zeta]$ or equivalently $N(b) = 1$ or $N(c) = 1$. These conditions are equivalent since if $b \in \mathbb{Z}[\zeta]$ then $N(b) \in \mathbb{N} \cup \{0\}$ and $N(b^{-1}) = N(b)^{-1}$. In the other direction, if $N(b) = 1$ then letting $c = \overline{\sigma_1(b)}|\sigma_2(b)|^2$, we see that $bc = N(b) = 1$). We claim that irreducible elements are the same as prime elements. It is clear that every prime is irreducible. Conversely, if p is irreducible and $p \mid ab$ but $p \nmid a, b$ then choosing a, b minimizing $N(a) + N(b)$, we may write $a = pq + r$ where $N(r) < N(p) \leq N(a)$. Multiplying through by b, we see that $ab = bpq + br$. It follows that $p \mid br$ where now $N(b) + N(r) < N(a) + N(b)$. By minimality, $p \mid b$ or $p \mid r$. In the former case, we are done. In the latter case, since $N(r) < N(p)$, it follows that $r = 0$ and $p \mid a$.

To show existence of factorizations, Note that if a_0 is not irreducible, then $a_0 = p_1 a_1$, where neither p_1 nor a_1 is a unit. This condition implies $1 < N(p_1), N(a_1) < N(a_0)$. Repeating this process on p_1 or a_1 and so on, we get that the norms of the factors are strictly decreasing sequences of positive integers. Hence the process must eventually terminate. This happens only when all the factors are irreducible. By the lemma above, all irreducible elements are prime. Next, to show uniqueness, suppose that $a = p_1 \ldots p_n = q_1 \ldots q_m$ are two factorizations which differ (in more than just order and multiplication by units). We may assume that $N(a)$ is minimal among elements having more than one factorization. Then $p_1 \mid a = q_1 \ldots q_m$ and since p_1 is prime, it follows that $p_1 \mid q_i$ for some i. Without loss of generality, we may assume $i = 1$. Since q_1 is irreducible and $q_1 = p_1 r$, it follows that r is a unit. Hence $\frac{ar^{-1}}{p_1} = \frac{a}{q_1}$ has two different factorizations. Since $N(p_1) = N(q_1) > 1$ (since neither are units), this contradicts the minimality of a. Hence $\mathbb{Z}[\zeta]$ has unique factorization into primes.

(c) Suppose x, y, z is a solution in nonzero integers to $x^5 + y^5 = (x+y)(x+\zeta y)(x+\zeta^2 y)(x+\zeta^3 y)(x+\zeta^4 y) = z^5$. We may assume without loss of generality that $\gcd(x, y, z) = 1$. We treat only the case $5 \nmid x, y, z$. If $-z \equiv x \equiv y \pmod{5\mathbb{Z}}$, then $-2z^5 \equiv z^5 \pmod{5}$, a contradiction. Hence replacing $x^5 + y^5 = z^5$ with $x^5 + (-z)^5 = (-y)^5$ as necessary, we may assume that $x \not\equiv y \pmod{5}$. Suppose $(x + \zeta^i y)$ and $(x + \zeta^j y)$ share a common factor c for $i \neq j$. Then $c \mid (\zeta^i - \zeta^j)y$ and $c \mid (\zeta^i - \zeta^j)x$ as well as $c \mid z$. Note that $N(\zeta^i - \zeta^j) = 5$ for all $i \neq j$. Thus $N(c) \mid 5N(x) = 5x^4$, $N(c) \mid 5N(y) = 5y^4$ and $N(c) \mid N(z) = z^4$. It follows that $N(c) \mid \gcd(5x^4y^4, z^4) = 1$. Thus c is a unit. It follows that $x + y, \ldots, x + \zeta^4 y$ are all relatively prime. Using unique factorization, it follows that there exist $t \in \mathbb{Z}[\zeta]$ and units u such that $x + \zeta y = ut^5$. Let $t = \sum_{i=0}^4 a_i \zeta^i$. Note that $t^5 \equiv \sum_{i=0}^4 a_i^5 \pmod{5\mathbb{Z}[\zeta]}$ (where the notation states that $t^5 = \sum_{i=0}^4 a_i^5$ differs by a multiple of 5 in $\mathbb{Z}[\zeta]$, this is clear by expanding). It follows that $t^5 \equiv \overline{t}^5 \pmod{5\mathbb{Z}[\zeta]}$. Since u is a unit, a theorem of Kronecker implies that $\frac{u}{\overline{u}} = \zeta^i$ for some i. Hence $x + \zeta y = ut^5 \equiv \zeta^i \overline{u} t^5 \equiv \zeta^i \overline{u} \sum_{i=0}^4 a_i^5 \pmod{5\mathbb{Z}[\zeta]}$. Similarly, $x + \zeta^{-1} y \equiv \zeta^{-i} \overline{u} \sum_{i=0}^4 a_i^5 \pmod{5\mathbb{Z}[\zeta]}$. Then $\zeta^{-i}(x + \zeta y) \equiv \zeta^i (x + \zeta^{-1} y) \pmod{5\mathbb{Z}[\zeta]}$ or $x + \zeta y - \zeta^{2i} x - \zeta^{2i-1} y \equiv 0 \pmod{5\mathbb{Z}[\zeta]}$. If $1, \zeta, \zeta^{2i}, \zeta^{2i-1}$ are all distinct, then this implies that $5 \mid x, y$, a contradiction. This leaves three options: $1 = \zeta^{2i}$, $1 = \zeta^{2i-1}$ or $\zeta = \zeta^{2i-1}$. In the first case, the equation above collapses to $\zeta y - \zeta^{-1} y \equiv 0 \pmod{5\mathbb{Z}[\zeta]}$, hence $5 \mid y$. In the second case, it instead becomes $(x - y) - (x - y)\zeta \equiv 0 \pmod{5\mathbb{Z}[\zeta]}$. Hence $5 \mid x - y$ and $x \equiv y \pmod{5}$, contradicting our initial choice. Finally, in the last case, the equation collapses to $x - \zeta^2 x \equiv 0 (\text{mod } 5\mathbb{Z}[\zeta])$ and $5 \mid x$.

□