2012 PUMaC Power Round
Solutions

Princeton University

Why are numbers beautiful? It's like asking why is Beethoven's Ninth Symphony beautiful. If you don't see why, someone can't tell you. I know numbers are beautiful. If they aren't beautiful, nothing is.

Paul Erdös

Our problems and their solutions are heavily based on Sections 1.1-1.2 of Martin Klazar's informal online notes on number theory, [1]. The concept for this Power Round was to present an elementary proof of Thue's theorem on Diophantine approximation. The maximum score possible was **110 points**.

2 Background (22 points)

2.1 (4 points)

Let $f, g \in \mathbb{C}[X]$ such that $f \neq 0$, and let $\alpha, \beta \in \mathbb{C}$.

(1) Show that
$$|f(\alpha)| \leq (1 + \deg f)\|f\| \cdot \max(1, |\alpha|)^{\deg f}$$

(1) Show that $\|\alpha f + \beta g\| \leq |\alpha|\|f\| + |\beta|\|g\|$. where the notation $f + g$ is the sum of the polynomials f and g.

(2) Prove $\|fg\| \leq (1 + \deg f)\|f\|\|g\|$, where fg is the product of polynomials f and g.

Solution. Let $f(X) = a_0 + a_1X + \ldots + a_mX^m$, $g(X) = b_0 + b_1X + \ldots + b_nX^n$.

1. $|f(\alpha) \leq \sum_{j=0}^{m} |a_j||\alpha|^j \leq \|f\| \sum_{j=0}^{m} |\alpha|^j \leq \|f\|(1 + m)\max(1, |\alpha|)^m$.

2. $\|\alpha f + \beta g\| = \max_j |\alpha a_j + \beta b_j|$, where $|\alpha a_j + \beta b_j| \leq |\alpha||a_j| + |\beta||b_j| \leq |\alpha|\|f\| + |\beta|\|g\|$.
3. The coefficient of X^k in fg is $\sum_{i+j=k} a_i b_j$, a sum of $\leq m+1$ terms, each of which is $\leq \|f\|\|g\|$.

□

2.2 (3 points)

Suppose $f(X) = (X-\alpha)^r g(X)$, where $\alpha \in \mathbb{C}$ is nonzero, $r \in \mathbb{Z}^+$, and $g \in \mathbb{C}[X]$ is nonzero. Prove that

$$\|g\| < (1 + \deg g)(2\max(1, |\alpha|^{-1}))^{\deg f} \|f\|$$

Solution. Let $m = \deg f$ and $n = \deg g$ as before. By geometric series expansion,

$$\frac{1}{(X-\alpha)^r} = \frac{1}{(-\alpha)^r} \frac{1}{(1 - X/\alpha)^r} = (-\alpha)^{-r} \sum_{j=0}^{\infty} \binom{j+r-1}{j} (X/\alpha)^j$$

Then $\|g\| \leq \|(-\alpha)^r \sum_{j=0}^{n} 2^{n+r} (X/\alpha)^j\| \|f\|$, after using the strict inequality $\binom{j+r-1}{j} < 2^{n+r}$. Apply part 3 from Problem 2.1, where we know $m = n+r$. □

2.3 (5 points)

(3) Let $f, g \in \mathbb{Q}[X]$ such that $g \neq 0$. Prove that there exist $q, r \in \mathbb{Q}[X]$ such that

$$f(X) = q(X)g(X) + r(X)$$

and either $r = 0$ or $\deg r < \deg g$. If $r = 0$, then we say g *divides* f.

(2) Why does the same statement hold with $f, g, q, r \in \mathbb{C}[X]$? Deduce that α is a root of $f \in \mathbb{C}[X]$ if and only if $f(X) = (X-\alpha)q(X)$ for some $q \in \mathbb{C}[X]$.

Solution. As is standard, we abbreviate $f = f(X)$, etc.

1. If $f = 0$, then we pick $q = r = 0$. Suppose that $f \neq 0$. Consider the set of polynomials
$$S = \{p = f - qg : q \in \mathbb{Q}[X]\}$$
If $0 \in S$, then we are done, so suppose S contains only nonzero elements. We know S is nonempty because it contains $p = f$. Let $r = f - qg$ be of minimal degree in S. If $s = \deg r - \deg g \geq 0$, then we can subtract off a constant multiple of $X^s g(X)$ from r to produce another element of S of degree strictly lower than r, contradicting minimality of r. Therefore, $\deg r < \deg g$ as needed.
2. Part 1 holds for $\mathbb{C}[X]$ because the trick of scaling $X^s g(X)$ to cancel the leading term of r still works there. For the second part of the problem, put $g(X) = X - \alpha$ in part 1.

□

2.4 (6 points)

Let $f(X) = a_0 + a_1 X + \ldots + a_d X^d$. For all $0 \leq k \leq d$, let

$$D_k f = \sum_{j=0}^{d} \binom{j}{k} a_j X^{j-k}$$

where

$$\binom{j}{k} = \frac{j!}{k!(j-k)!}$$

for $0 \leq k \leq j$, and equals 0 otherwise.
We abbreviate by writing $Df = D_1 f$.

(2) Show that $\|D_k f\| \leq 2^d \|f\|$ for all $0 \leq k \leq \deg f$.

(1) Show that $k! D_k(f) = D_1^{(k)}(f)$, where $D_1^{(k)}$ denotes the composition of D_1 with itself k times.

(3) Show that if $D_0(f)(\alpha) = D_1(f)(\alpha) = \ldots = D_{k-1}(f)(\alpha) = 0$, then f has a root of multiplicity at least k at α.

Solution. $\binom{j}{k} \leq 2^j$, whence $\|D_k f\| \leq 2^d \|\sum_{j=k}^{d} a_j X^{j-k}\| \leq 2^d \|f\|$. TO DO: Solutions to parts 2 AND 3. □

2.5 (4 points)

Suppose $f, g \in \mathbb{C}[X]$ are nonzero such that

$$fDg = gDf$$

(1) Show that $\deg f = \deg g$.

(3) Show that f, g differ by a constant multiple.

Solution. Let $m = \deg f$ and $n = \deg g$. Using the Fundamental Theorem of Algebra, $f = A(x - a_1) \ldots (x - a_m)$ and $g = B(x - b_1) \ldots (x - b_n)$, for some coefficients $A, B, a_i, b_j \in \mathbb{C}$.

1. Expand fDg and gDf separately. The leading coefficients are mAB and nBA, respectively, where $AB \neq 0$, so $m = n$.

2. It is possible to solve this problem by bashing out the computations. We give a rather slicker proof: First show $D(f_1 f_2) = f_1 D f_2 + f_2 D f_1$ for all $f_1, f_2 \in \mathbb{C}[X]$, by writing out both sides. Then

$$\frac{D(f_1 f_2)}{f_1 f_2} = \frac{Df_1}{f_1} + \frac{Df_2}{f_2}$$

Since $(Df)/f = (Dg)/g$ and $DA = DB = 0$, we apply the above lemma to the linear factors of f and g to obtain

$$\frac{1}{X-a_1} + \ldots + \frac{1}{X-a_m} = \frac{1}{X-b_1} + \ldots + \frac{1}{X-b_n}$$

Since $m = n$, it suffices to prove that the a_j and b_j are the same up to ordering. We know $\{a_j\}$ and $\{b_j\}$ are at least the same *set* of numbers, because both sides must blow up in absolute value when X gets very close to a root on one side. To show that the roots occur with the same *multiplicity* on both sides, cancel out all common linear factors from f and g to obtain new polynomials f_0 and g_0, respectively, which do not share any linear factors. Repeating the above argument for f_0, g_0 shows $f_0 = g_0 = 1$, as needed.

□

3 Algebraic Numbers (32 points)

3.1 (7 points)

Let $\alpha \in \overline{\mathbb{Q}}$.

(1) Show that if $a, b \in \mathbb{Q}$ with $a \neq 0$, then $\beta = a\alpha + b$ is algebraic and $\deg \beta = \deg \alpha$.

(1) Show there exists $a \in \mathbb{Z}^+$ such that $a\alpha$ is an algebraic integer.

(1) Suppose α is an algebraic integer. Show that if $b \in \mathbb{Z}$, then $\alpha + b$ is an algebraic integer.

(4) Suppose α is an algebraic integer, such that $f(\alpha) = 0$ for some monic polynomial $f \in \mathbb{Z}[X]$ of degree d. Let $r \in \mathbb{Z}$ be nonnegative. Prove that we can write

$$\alpha^r = \sum_{j=0}^{d-1} a_{r,j}\alpha^j$$

for some $a_{r,j} \in \mathbb{Z}$ with $|a_{r,j}| \leq (1 + \|f\|)^r$.

Solution. By definition, α is the root of some polynomial $f(X) = a_0 + a_1 X + \ldots + a_d X^d \in \mathbb{Q}[X]$.

1. $\beta/a - b/a$ is a root of f. Expanding the polynomial in β shows β is algebraic.

2. Let a be the common denominator of the a_j. Then

$$(a\alpha)^n + \sum_{j=0}^{d-1} a^{d-j} a_j (a\alpha)^j = 0$$

where $a^{d-j} a_j \in \mathbb{Z}$ for all j, so $a\alpha$ is an algebraic integer.

3. If α is an algebraic integer, then we can choose f so that it is monic with coefficients in $\mathbb{Z}$. Let $\beta = \alpha + b$. Then $\beta - b$ is a root of f, so expanding the polynomial in β shows β is an algebraic integer.

4. (*Following Klazar*) Again, choose f to be monic with $a_j \in \mathbb{Z}$ for all j. If $r = 0$, then we put $c_{0,0} = 1$ and $c_{0,j} = 0$ for all $j > 0$. Now induct on r to prove that

$$\alpha^r = \alpha(\alpha^{r-1}) = \sum_{j=0}^{d-1}(c_{r-1,j-1} - c_{r-1,d-1}a_j)\alpha^j$$

where $c_{r-1,-1} = 0$, using the substitution $\alpha^d = -\sum_{j=0}^{d-1} a_j\alpha^j$. So $c_{r,j} = c_{r-1,j-1} - c_{r-1,d-1}a_j$. By induction,

$$|c_{r,j}| \le |c_{r-1,j-1}| + |c_{r-1,d-1}||a_j|\text{`}(1 + \max_j |a_j|)^r$$

$\square$

3.2 (7 points)

Let $f \in \mathbb{Z}[X]$.

(3) Suppose $g \in \mathbb{Z}[X]$. Show that if the product fg is not simple, then at least one of f or g is not simple.

(2) Suppose instead $g \in \mathbb{Q}[X]$. Show that if f is simple and $fg \in \mathbb{Z}[X]$, then $g \in \mathbb{Z}[X]$.

(2) Conclude that if a polynomial in $\mathbb{Z}[X]$ does not factor into two nonconstant polyomials in $\mathbb{Z}[X]$, then it cannot factor into two nonconstant polynomials in $\mathbb{Q}[X]$.

Solution. Let $f(X) = a_0 + a_1X + \ldots + a_mX^m$, $g(X) = b_0 + b_1X + \ldots + b_nX^n$.

1. We show the contrapositive: Suppose f, g are simple. There exists a prime number p such that $p \nmid a_j, b_k$ for some j, k. We can choose j and k to be minimal. The coefficient of X^{j+k} in fg is $a_jb_k + \sum_{i=0}^{j-1} a_ib_{j+k-i} + \sum_{i=0}^{k-1} a_{j+k-i}b_i$. Here, p divides each of the sums but not a_jb_k, so the whole expression is not divisible by p. So no prime p divides all of the coefficients of fg, as needed.

2. Let b be the least common denominator of the rational coefficients b_j in lowest terms. Then $bg(X) \in \mathbb{Z}[X]$ is simple. From part 1, we deduce that bfg is simple, but $fg \in \mathbb{Z}[X]$, whence $b = 1$. Therefore, $g \in \mathbb{Z}[X]$.

3. If $f \in \mathbb{Z}[X]$ factors into two nonconstant polynomials in $\mathbb{Q}[X]$, then let a be the least common denominator of the coefficients in lowest terms of one of them. By multiplying that polynomial through by a and dividing the other by a, we obtain the situation in part 2, so that the new polynomials must both belong to $\mathbb{Z}[X]$.

□

3.3 (12 points)

Let $\alpha \in \overline{\mathbb{Q}}$, and let $f \in \mathbb{Q}[X]$ be nonzero.

(2) Show that the roots of m_α all have multiplicity 1, or in other words, that they are pairwise distinct.

(2) Suppose f does not factor into two nonconstant polynomials in $\mathbb{Q}[X]$. Show the roots of f are pairwise distinct algebraic numbers, each of degree $\deg f$.

(2) Suppose α is a root of multiplicity m of f. Prove $\deg f \geq m \deg \alpha$.

(3) Suppose $p/q \in \mathbb{Q}$ is in lowest terms, and is a root of multiplicity m of f. Also, suppose $f \in \mathbb{Z}[X]$ and has leading coefficient a. Prove $q^m \leq |a|$.

(3) Show that if α is an algebraic integer, then $m_\alpha \in \mathbb{Z}[X]$.

Hint: See Problem 2.3! Also, on parts 4 and 5, use Problem 3.2.

Solution.

1. Via the identity $D(fg) = fDg + gDf$ from Section 2, we can prove that α remains a root of Dm_α if and only if its multiplicity as a root of m_α is ≥ 2. But $\deg Dm_\alpha < \deg m_\alpha$, violating the minimality of m_α.

2. If α is a root of f, then m_α divides f, so $\deg f = \deg m_\alpha$ for all such α. Therefore, the multiplicity of α as a root of f is the same as its multiplicity as a root of m_α, that is to say 1. Moreover, the degree of α is $\deg m_\alpha$ by definition.

3. Follows from part 2 of Problem 2.5 by induction on m.

4. $q^m(X - p/q)^m = q^m X^m + \ldots + (-p)^m$ is simple, as $\gcd(p, q) = 1$. Since $(X - p/q)^m$ occurs in the factorization of f, we deduce that $q^m(X - p/q)^m$ divides f in $\mathbb{Q}[X]$, meaning there exists $g \in \mathbb{Q}[X]$ with

$$q^m(X - p/q)^m g(X) = f(X)$$

   But by Problem 3.2, $g \in \mathbb{Z}[X]$. Comparing leading coefficients, $q^m \mid a$ as needed.

5. There exists monic $f \in \mathbb{Z}[X]$ with $f(\alpha) = 0$, where we know $m_\alpha g = f$ for some $g \in \mathbb{Q}[X]$ by the remark after the definition of m_α. There exists nonzero $a \in \mathbb{Z}$ such that $am_\alpha \in \mathbb{Z}[X]$ and is simple. Then $f = (am_\alpha)(a^{-1}g)$, whence $a^{-1}g \in \mathbb{Z}[X]$ by part 2 of Problem 3.2. But f is monic. So $a = 1$ and therefore $m_\alpha \in \mathbb{Z}[X]$.

□

3.4 (6 points)

For all $1 \le i \le m$, let

$$f_i(X_1, \ldots, X_n) = a_{i,1}X_1 + \ldots + a_{i,n}X_n \in \mathbb{Z}[X_1, \ldots, X_n]$$

where $n > m$ and $|a_{i,j}| \le A$ for all i, j for some fixed $A > 0$. Prove that there exist $x_1, \ldots, x_n \in \mathbb{Z}$, satisfying

$$f_1(x_1, \ldots, x_n) = \ldots = f_m(x_1, \ldots, x_n) = 0$$

such that $|x_j| \le \lfloor (nA)^{m/(n-m)} \rfloor$ for all j and $x_j \neq 0$ for some j. We use the notation $\lfloor s \rfloor$ to denote the greatest integer not greater than s.

Hint: Use the Pigeonhole Principle. That is, if there are N pigeonholes and M pigeons, where $M > N$, then at least one pigeonhole must get > 1 pigeon.

Solution. Let $a_i = \sum_{j=1}^n \max(0, a_{i,j})$ and $b_i = \sum_{j=1}^n \min(0, a_{i,j})$. For all integer $r \ge 0$, there are $(r+1)^n$ n-tuples $(x_1, \ldots, x_n)$ in the n-dimensional "box" $\{0, \ldots, r\}^n$. The m-tuple $(f_1, \ldots, f_m)$ is a function on this box, with values in the m-dimensional box

$$\mathcal{B} = \prod_{i=1}^{m} \{b_i r, \ldots, a_i r\}$$

(Above, $\prod$ is a shorthand notation for $\times \ldots \times$, and the terms of the product are again sets.)

Set $r = \lfloor (nA)^{m/(n-m)} \rfloor$. Since $n > m$, we have $(r+1)^n > ((r+1)nA)^m > (rnA+1)^m$, whence

$$\#\mathcal{B} = \prod_{i=1}^{m} (ra_i - rb_i + 1) \le (rnA+1)^m < (r+1)^m$$

By the Pigeonhole Principle, two of our n-tuples are mapped to the same m-tuple by $(f_1, \ldots, m)$. Their difference $(x_1, \ldots, x_n)$ is nonzero, meaning $x_i \neq 0$ for some i, and is mapped to $(0, \ldots, 0)$, so that $|x_i| \le r$ for all i.

Note: Thanks to Kevin Li for pointing out that when all f's are zero, we cannot both satisfy $|x_j| \le \lfloor (nA)^{m/(n-m)} \rfloor$ for all j and $x_j \neq 0$ for some j. This problem may be fixed by either making A take on only integer values or making at least one f_i nonzero. $\square$

4 Main Results (56 points)

The problems in this section are very hard, so do not be discouraged if you get stuck on some—or all!—of them. In what follows, let $I = [-1/2, +1/2]$.

4.1 (4 points)

Let $0 < \epsilon < 1/2$. Show that if, for all α which are algebraic integers in I of degree $d \geq 3$,

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{1+\epsilon+d/2}}$$

has only finitely many solutions for the rational p/q in lowest terms, then, for all α which are algebraic integers (not necessarily in I) of degree $d \geq 1$, it also has only finitely many solutions for the rational p/q in lowest terms.

Solution. Let us first show that the existence of only finitely many solutions for p/q is equivalent to the existence of a constant $c(\alpha, \epsilon)$ such that

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha, \epsilon)}{q^{1+d/2+\epsilon}}$$

for all $\frac{p}{q} \neq \alpha$. This fact, which we will call Lemma 4.1, will be used both here and in the solution to 4.5.

First we assume that there are finitely many solutions to

$$\left|\alpha - \frac{p}{q}\right| < 1/q^{1+\delta+d/2}$$

then clearly their exists a lower bound C such that

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{C}{q^{1+\delta+d/2}}$$

where C is $\min(c_i)$ and each $c_i > 0$ is chosen such that

$$\left|\alpha - \frac{p_i}{q_i}\right| \geq \frac{c_i}{q_i^{1+\delta+d/2}}$$

. Finitely many c_i implies positive minimum, so C is positive.

Conversely, if we start with the existence of $C(\alpha, \delta)$ for all $0 < \delta < \epsilon$ such that

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{C(\alpha, \delta)}{q^{1+\delta+d/2}}$$

for all $\frac{p}{q} \neq \alpha$. Then when

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{1+\epsilon+d/2}}$$

we have $0 < C(\alpha, \delta) < q^{\delta-\epsilon}$, which for $\delta < \epsilon$ can only be true for finitely many $\frac{p}{q}$. This proves our lemma.

So equivalently, we have to produce a constant $c(\alpha, \epsilon)$ depending only on α and ϵ, such that

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha, \epsilon)}{q^{1+d/2+\epsilon}}$$

for all $\frac{p}{q} \neq \alpha$. If $\alpha \notin \mathbb{R}$, we know that $|\alpha - \frac{p}{q}| \geq \text{Im}(\alpha) > 0$ and for large enough q we get a contradiction. Thus q is bounded, and for fixed q, the number of choices for p are finite (by the inequality) and so we have finitely many solutions in total. Thus we are reduced to $\alpha \in \mathbb{R}$. If $d = 1$, we have that $\alpha = \frac{a}{b}$ where a, b are integers. For $\frac{p}{q} \neq \alpha$, we see that

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{qb} \geq \frac{1}{bq^{3/2+\epsilon}}$$

and pick $c(\alpha, \epsilon) = \frac{1}{b}$. For $d = 2$, we have $\alpha' \in \mathbb{R}$, $\alpha' \neq \alpha$ such that $P(x) = x^2 + ax + b = (x - \alpha)(x - \alpha')$ and $a, b \in \mathbb{Z}$. For $\frac{p}{q} \in \mathbb{Q}$, we have $|P(\frac{p}{q})| \geq \frac{1}{q^2}$. If $|\alpha - p/q| < 1$, we have

$$\left|\alpha - \frac{p}{q}\right| = \frac{P(p/q)}{|\alpha' - p/q|} > \frac{1}{(1 + |\alpha - \alpha'|)q^2}$$

and picking $c(\alpha, \epsilon) = \min\left(1, \dfrac{1}{1 + |\alpha - \alpha'|}\right)$ gives us the desired result. Finally when $\alpha \in \mathbb{R}$ and $|\alpha| > \frac{1}{2}$, pick integer n such that $n + \alpha \in I$ and observe that the finiteness of the set $\left\{\dfrac{p}{q} : |(\alpha + n) - \dfrac{p}{q}| < \dfrac{1}{q^{1+d/2+\epsilon}}\right\}$ is equivalent to the finiteness of the set $\left\{\dfrac{p'}{q} := \dfrac{p - n}{q} : |\alpha - \dfrac{p'}{q}| < \dfrac{1}{q^{1+d/2+\epsilon}}\right\}$. $\square$

4.2 (8 points)

Let $d, m, n \in \mathbb{Z}^+$ such that $d \geq 3$ and $1 < \frac{md}{n+1} < 2$, and let

$$\lambda = 1 - \frac{md}{2n + 2}$$

Let α be an algebraic integer in I of degree d. Show that there exist $P(X), Q(X) \in \mathbb{Z}[X]$ such that:

1. $\deg P$, $\deg Q \leq n$.
2. $\|P\|, \|Q\| \leq c_1^{n/\lambda}$, for some $c_1 > 1$ depending only on α.
3. $D_j(P + \alpha Q)(\alpha) = 0$ for all $0 \leq j < m$.
4. $P(X)/Q(X)$ is not constant in X.

Hint: Write down some linear equations and solve for the coefficients of P, Q using Problem 3.4!

Solution. We write $P(x) = \sum_{i=0}^n a_i x^i$ and $Q(x) = \sum_{i=0}^n b_i x^i$ and solve for the $2n+2$ unknown coefficients in a way that satisfies the above criteria. The third condition gives us that

$$\sum_{i=0}^{n} \binom{i}{j} (a_i \alpha^{i-j} + b_i \alpha^{i-j+1}) = 0$$

for $0 \le j < m$ where $\binom{i}{j} := 0$ for $j > i$. By the last part of Question 3.1, we have that

$$\sum_{k=0}^{d-1} \alpha^k \sum_{i=j}^{n} \binom{i}{j} (c_{i-j,k} a_i + c_{i-j+1,k} b_i) = 0$$

for $0 \le j < m$ and $c_{r,k} < c_0^r$ where $c_0 > 1$ depends only on α. This is true if and only if the coefficients of α^k are zero for $0 \le k < d$ in each of the above m equations and hence we get dm linear equations in the $2n+2$ unknowns a_i, b_i with integer coefficients $\binom{i}{j} c_{r,k}$ which are bounded in absolute value by $(2c_0)^n$. Since $(2n+2) > dm$, by Question 3.4, we have the existence of solutions a_i, b_i bounded in absolute value by

$$(2n+2) A^{md/(2n+2-md)} < (2n+2) A^{1/\lambda} \le (8c_0)^{n/\lambda}$$

which is the bound required by picking $c_1 = 8c_0$.

We are left to show that the polynomials are both not identically zero and not constant multiples of each other. Assume without loss of generality that $Q \neq 0$ but $P = cQ$ for a constant $c \in \mathbb{Q}$ (possibly 0). By condition 3, we have from 2.4 that $R(x) := (c + \alpha) Q(x)$ has at $x = \alpha$ a zero of multiplicity at least m since $D_j(R(x))(\alpha) = 0$ for $0 \le j < m$. Since $c \in \mathbb{Q}$, we have that $(c + \alpha) \neq 0$ and $Q(x) = (c + \alpha)^{-1} R(x)$ has at $x = \alpha$ a zero of order at least m. This gives us $\deg(Q) = n \ge md > n + 1$ since $\lambda < 0.5$, a contradiction.

□

4.3 (10 points)

Let $d, n, \lambda, m, \alpha, P, Q, c_1$ be as in the previous problem. Let $u = p/q$ and $v = r/s$ be rational numbers in lowest terms such that $q, s \ge 2$ and

$$|\alpha - u| < \frac{1}{q^\mu} \text{ and } |\alpha - v| < \frac{1}{s^\mu}$$

for some $\mu > 1$. Prove that for all $0 \le j < m$,

$$|D_j(P + vQ)(u)| \le c_2^{n/\lambda} \left(\frac{1}{q^{\mu(m-j)}} + \frac{1}{s^\mu} \right)$$

for some $c_2 > 1$ depending only on α.

Hint: Use the various facts about D_k and $\| \cdot \|$ from section 2.

Solution. Let $F(x,y) = P(x) + yQ(x)$. From the previous problem, we have that $F(x,a)$ has a zero of multiplicity at least m at α and so $F(x,y) = F(x,\alpha) + (y-\alpha)Q(x) = (x-\alpha)^m R(x) + (y-\alpha)Q(x)$, where $R \in \mathbb{C}[x]$. This gives us $D_j F(x,y) = (x-\alpha)^{m-j}S(x) + (y-\alpha)D_j Q(x)$ by $D(fg) = fD(g) + gD(f)$ and $D_j = j!D_1^{(j)}$ where $S \in \mathbb{C}[x]$. Now using results from section 2 and the fact that $|u|, |v| < 1$, we get

$$\begin{aligned} |D_j(F)(u,v)| &= |(u-\alpha)^{m-j}S(u) + (v-\alpha)D_j Q(u)| \\ &\le q^{-\mu(m-j)}(n+1)\|S\| + s^{-\mu}(n+1)\|D_j Q\| \end{aligned}$$

Now $\|D_j(Q)\| \le (2c_1)^{n/\lambda}$ and $D_j F(x,\alpha) = (x-\alpha)^{m-j}S(x)$. Thus, we get from results of section 2 that

$$\|S\| < (\deg S + 1)(2/|\alpha|)^{n-j}\|D_j F(x,\alpha)\| \le (16c_1/\alpha)^{n/\lambda}$$

since $\deg(S) \le n < 2^n$, $|\alpha| < 1$ and $\|D_j P\|, \|D_j Q\| \le (2c_1)^{n/\lambda}$. Since $2(n+1) \le 4^n$, the desired estimate follows by choosing $c_2 = 64c_1/|\alpha|$. □

4.4 (12 points)

Let $d, n, \lambda, m, \alpha, P, Q, u = p/q, v = r/s$ be as in the previous problem. Prove that

$$D_h(P + vQ)(u) \neq 0$$

for some $h \in \mathbb{Z}^+$ such that $h \le 1 + (c_3/\lambda)n/\log q$, where $c_3 > 0$ depends only on α. Note that $\log q = \log_e q$.

Hint: Recall part 4 of Problem 3.3.

Solution. Observe that $W := D(P)Q - D(Q)P \neq 0$ since P, Q are not proportional, by Question 2.5. We have $D^{(j)}(W) = \sum_{i=0}^{j} \binom{j}{i}(D^{(i+1)}(P)D^{(j-i)}(Q) - D^{(j-i)}(P)D^{(i+1)}(Q))$ by applying $D(fg) = fD(g) + gD(f)$ iteratively. Let h be the minimum positive integer such that $D_h(P + vQ)(u) \neq 0$. We know h exists since $P + vQ \neq 0$ as a polynomial and so for $0 \le j < h$, we have $(D_j(P) + vD_j(Q))(u) = 0$. Eliminating v gives the equations $(D_j(P)D_i(Q) - D_i(P)D_j(Q))(u) = 0$ for $0 \le i, j < h$ and thus $D_j(W) = (j!)^{-1}D^{(j)}(u) = 0$ for $0 \le j < h-1$ and hence W has a zero of order at least $h-1$ at $x = u$. We know from part 4 of 3.3 that $q^{h-1} \le \|W\|$ and

$$\|W\| \le 2n\|PQ\| \le 2n(2n+1)c_1^{2n/\lambda} \le (4c_1^2)^{n/\lambda},$$

implying the desired result when $c_3 = \log(4c_1^2)$.

□

4.5 (22 points)

Let $0 < \epsilon < 1/2$. Prove that for all $\alpha \in \overline{\mathbb{Q}}$ of degree $d \ge 1$,

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{1+\epsilon+d/2}}$$

has only finitely many solutions for the rational p/q in lowest terms.

Hint: Assume that there are infinitely many solutions. Let t be a an even integer such that $t > 4d/\epsilon - 2$ and let $\mu = 1 + \epsilon + d/2$. Given t, carefully select $n, \lambda, m, P, Q, u = p/q, v = r/s$ as in the above problems (u, v exist by the assumption of infinitely many solutions) and produce a contradiction between the results of Problems 4.3 and 4.4.

Solution. By 3.1.2, it suffices to show this theorem for algebraic integers β, since for any α we can let $\beta = k\alpha$, and if

$$\left|k\alpha - \frac{p}{q}\right| > \frac{c}{q^{1+\epsilon+d/2}}$$

for any fraction $\frac{p}{q} \neq k\alpha$, then

$$\left|\alpha - \frac{p}{kq}\right| > \frac{c/k}{q^{1+\epsilon+d/2}}$$

for any fraction $\frac{p}{kq} \neq \alpha$. Thus if we show c to exist in the first case, there are only finitely many solutions for p/q, by Lemma 4.1 in the solution for question 4.1.

Using Question 4.1, we reduce to the case of $d \geq 3$ and α is an algebraic integer in I. Assume that $\left|\alpha - \frac{p}{q}\right| < 1/q^{1+\epsilon+d/2}$ for infinitely many $\frac{p}{q} \in \mathbb{Q}$. Choosing approximation: Fix even t such that $\lambda = 2/(2+t) < \epsilon/2d$ and thus $0 < \lambda < \frac{1}{12}$ and $t \geq 24$. Let n run through the arithmetic progression defined by $n = i(t/2+1)d - 1$ for $i \in \mathbb{N}$ and let $m = (2n+2)(1-\lambda)/d = it$. Pick $c = \max(c_1^{1/\lambda}, c_2^{1/\lambda}, c_3^{1/\lambda})$ (from above) and set $\mu = 1 + \epsilon + d/2$ and $\delta = (1 + 2\epsilon/d)(1-\lambda) - 1$. Select two rational approximations $u = \frac{p}{q}$ and $v = \frac{r}{s}$ from the infinitely many available such that $(p,q) = (r,s) = 1$, $2 \leq q < s$ and

1. $|\alpha - u| < q^{-\mu}$
2. $|\alpha - v| < s^{-\mu}$
3. $\log q > 2cd\mu/\delta$
4. $\log s > (t + 2(\mu + t)/\delta)\log q$.

Pick $m = it$ such that

$$\frac{\log s}{\log q} - t \leq m < \frac{\log s}{\log q}$$

and $n = i(t/2+1)d - 1$. Pick polynomials P, Q using Problem 4.2 and pick minimal h such that $w := D_h(P + vQ)(u) \neq 0$.

Obtaining a contradiction: We get $m > 6t > 100$ from lower bounds on m and assumption (4) from above. Since $4n/d \geq 2(n+1)/d > m > 100$, we get $n > 25d$. From the previous problem, $n > 2d$ and we get $h < m$ because

$$h \leq 1 + cn/\log q < 1 + n/2d < n/d < \frac{11}{6}(n+1)/d < (2n+2)(1-\lambda)/d = m$$

. We have

$$(q^{n-h}s)^{-1} \leq |w| < c^n(q^{-\mu(m-h)} + s^{-\mu}) \leq (2c)^n q^{-\mu(m-h)}.$$

The first inequality follows from $w \neq 0$ and $q^{n-h}sw \in \mathbb{Z}$ since $D_hP, D_hjQ \in \mathbb{Z}[x]$ and have degrees atmost $n-h$. The second inequality follows from Problem 4.3 and that $s > q^m$. Taking logarithms we get

$$\mu m - \mu h + h - n \leq \frac{\log s}{\log q} + n\frac{\log(2c)}{\log q} \leq m + t + n\frac{\log(2c)}{\log q}$$

by the lower bound on m. Since

1. $h \leq (1 + cn/\log q)$ by 3.4,
2. $(\mu - 1)m - n > (\epsilon + d/2)2n(1-\lambda) - n = \delta n$, and
3. $\log q < 2cd\mu/\delta$,

the above statement reduces to $n \leq 2(\mu + t)/\delta$ which can't hold for large i. Hence the contradiction. $\square$

References

[1] Martin Klazar. Analytic and combinatorial number theory II (lecture notes). http://kam.mff.cuni.cz/, 2010.