2012 PUMaC Power Round

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

1 Rules and Reminders

These rules supersede any rules appearing elsewhere about the Power Round:

1. On any problem, you may use without proof any **result** or **remark** from earlier in the test, even if it's a problem your team has not solved. You may cite results from conjectures or subsequent problems only if your team solved them independently of the problem where you wish to cite them. You may not cite parts of your proof of other problems: if you wish to use a lemma in multiple problems, please reproduce it in each one.
2. It is not necessary to do the problems in order, although it is a good idea to read all the problems, so that you know what is permissible to assume when doing each problem. However, please collate the solutions in order in your solution packet. Each problem should start on a new page, and solutions should be written on one side of the paper only. Each page should also have on it the team name and problem number.
3. Using computer programs, calculators, and Mathematica (or similar programs), is allowed. This year, however, **print and online references are not allowed**.
4. No communication with humans outside your team about the content of these problems is allowed. If you have any questions regarding the test, please contact us at once at pumac@math.princeton.edu.

2 Background

We write

1. $\mathbb{Z}$ for the set of integers.
2. $\mathbb{Q}$ for the set of rational numbers.
3. $\mathbb{C}$ for the set of complex numbers.

For convenience, let $\mathbb{Z}^+$ be the set of positive integers. We write $\mathbb{Z}[X]$ for the set of polynomials in X with coefficients in $\mathbb{Z}$, and more generally, $\mathbb{Z}[X_1, \ldots, X_n]$ for the set of polynomials in $X_1, \ldots, X_n$ with integer coefficients. Similar notation is used for $\mathbb{Q}$ and $\mathbb{C}$. We write $n \in \mathbb{Z}^+$ to denote that n is a member of $\mathbb{Z}^+$.

Recall that, like real numbers, complex numbers have a notion of absolute value: by definition, $|a + bi| = \sqrt{a^2 + b^2}$. For all $z_1, z_2 \in \mathbb{C}$, we have $|z_1 z_2| = |z_1||z_2|$ and $|z_1 + z_2| \leq |z_1| + |z_2|$, just like for real numbers.

2.1 Definition. Let f be a polynomial in $X_1, \ldots, X_n$ whose coefficients are not all zero. If f consists of one term, then the *degree* of f, written $\deg f$, is the sum of the exponents of the X_j's. In general, $\deg f$ is the maximum degree among all terms of f.

For instance, if $f(X) = a_0 + a_1 X + \ldots + a_d X^d$ and $a_d \neq 0$, then $\deg f = d$ as usual. Henceforth, we always assume $a_d \neq 0$ when writing a polynomial in this form. We say that $a_d X^d$ is the *leading term* of f, and a_d is the *leading coefficient*. Note that the degree of the 0 polynomial is *undefined*.

2.2 Definition. A polynomial $f(x_1, x_2, \ldots, x_n)$ is *homogeneous* if (and only if) each of its terms, individually, has the same degree as the others. Equivalently, f is homogeneous if

$$f(\lambda x_1, \lambda x_2, \ldots, \lambda x_n) = \lambda^{\deg f} f(x_1, x_2, \ldots, x_n)$$

for any $\lambda \neq 0$.

2.3 Definition. A number is *algebraic* if it is the root of a nonzero polynomial in $\mathbb{Q}[X]$. All numbers that are not algebraic are *transcendental*. We write $\overline{\mathbb{Q}}$ for the set of algebraic numbers.

2.1 Remark. Important! $\overline{\mathbb{Q}}$ is a subset of $\mathbb{C}$. More precisely, every polynomial in $\mathbb{Q}[X]$ splits completely into linear factors in $\mathbb{C}[X]$. The *multiplicity* of α as a root of a polynomial is the exponent to which $(X - \alpha)$ appears in the linear factorization of that polynomial in $\mathbb{C}[X]$.

2.4 Definition. Let $\alpha \in \overline{\mathbb{Q}}$. The *degree* of α, written $\deg \alpha$, is the minimum degree among degrees of all nonzero polynomials in $\mathbb{Q}[X]$ that have α as a root.

2.5 Definition. A polynomial in one variable is *monic* if its leading coefficient is 1. A number is an *algebraic integer* if it is the root of a monic polynomial in $\mathbb{Z}[X]$.

Here's an example. Let $\alpha = \sqrt{3}$. Note that α is a root of the polynomial $f(X) = X^2 - 3$. Since α is not the root of a linear polynomial with rational coefficients, α is an *algebraic number* of *degree* 2. Since f is monic and has integer coefficients, α is actually an *algebraic integer*.

2.6 Definition. Let $f = a_0 + a_1X + \ldots + a_dX^d \in \mathbb{C}[X]$. Define

$$\|f\| = \max\{|a_0|, \ldots, |a_d|\}$$

2.2 Remark. If S is a set, then $\max S$ is the maximum among the elements of S.

The following problems will not only develop our intuition for $\|f\|$, but will also be useful later in the test.

2.1 (4 points)

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

1. **(1)** Show that
$$|f(\alpha)| \leq (1 + \deg f)\|f\| \cdot \max(1, |\alpha|)^{\deg f}$$
2. **(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.
3. **(2)** Prove $\|fg\| \leq (1 + \deg f)\|f\|\|g\|$, where fg is the product of polynomials f and 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

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

2.3 (5 points)

1. **(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. **(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 $q \in \mathbb{C}[X]$.

2.4 (6 points)

Let $f(X) = a_0 + a_1X + \ldots + a_dX^d$. 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 $Df = D_1 f$.

1. **(2)** Show that $\|D_k f\| \leq 2^d \|f\|$ for all $0 \leq k \leq \deg f$.
2. **(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. **(3)** Show that if $D_0(f)(\alpha) = D_1(f)(\alpha) = ... = D_{k-1}(f)(\alpha) = 0$, then f has a root of multiplicity at least k at α.

2.3 Remark. You should verify the fact $D(fg) = fDg + gDf$ and use it for part 3, though it carries no individual point value.

2.5 (4 points)

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

$$fDg = gDf$$

1. **(1)** Show that $\deg f = \deg g$.
2. **(3)** Show that f, g differ by a constant multiple.

3 Algebraic Numbers

3.1 (7 points)

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

1. **(1)** Show that if $a, b \in \mathbb{Q}$ with $a \neq 0$, then $\beta = a\alpha + b$ is algebraic and $\deg \beta = \deg \alpha$.
2. **(1)** Show there exists $a \in \mathbb{Z}^+$ such that $a\alpha$ is an algebraic integer.
3. **(1)** Suppose α is an algebraic integer. Show that if $b \in \mathbb{Z}$, then $\alpha + b$ is an algebraic integer.

4. **(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 $|a_{r,j}| \leq (1 + \|f\|)^r$.

3.1 Definition. A polynomial $f \in \mathbb{Z}[X]$ is *simple* if there do not exist an integer $a > 1$ and a polynomial $g \in \mathbb{Z}[X]$ such that $f(X) = ag(X)$. For example, the 0 polynomial is not simple.

3.2 (7 points)

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

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

3.2 Definition. For all $\alpha \in \overline{\mathbb{Q}}$, let $m_\alpha \in \mathbb{Q}[X]$ be a monic polynomial of lowest degree among all polynomials that have α as a root.

3.1 Remark. Verify that m_α divides any polynomial in $\mathbb{Q}[X]$ that has α as a root. (This will not be graded.)

3.3 (12 points)

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

1. **(2)** Show that the roots of m_α all have multiplicity 1, or in other words, that they are pairwise distinct.
2. **(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 $\deg f$.
3. **(2)** Suppose α is a root of multiplicity m of f. Prove $\deg f \geq m \deg \alpha$.
4. **(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 $q^m \leq |a|$.
5. **(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.

3.4 (6 points)

For all $1 \leq i \leq m$, 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 $|a_{i,j}| \leq A$ 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 $|x_j| \leq \lfloor (nA)^{m/(n-m)} \rfloor$ 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.

4 Main Results

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 $I = [-1/2, +1/2]$, the set of *real* numbers with absolute values of at most $1/2$.

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.

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!

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 $q, s \geq 2$ and

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

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

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

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

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

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 $h \leq 1 + (c_3/\lambda)n/\log q$, where $c_3 > 0$ depends only on α. Note that $\log q = \log_e q$.

Hint: Recall part 4 of Problem 3.3.

4.5 (22 points)

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

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

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.