Putnam and Beyond:
Notes and Solutions

John McCuan

September 7, 2024

Contents

1 Methods of Proof **5**
1.1 Proof by way of contradiction 5

2 Fall 2024 **9**
2.1 Thursday August 22, 2024, 5PM to 7PM Skiles 255 9
2.2 September 29 10
2.2.1 Induction 10
2.2.2 Probability 10
2.3 September 5 12
2.3.1 Main Problem 12
2.3.2 Another similar problem 16
2.3.3 Another relatively easy problem 17

Chapter 1

Methods of Proof

1.1 Proof by way of contradiction

Let $n \in \mathbb{N} = \{1, 2, 3, \ldots\}$ be a natural number. Let $\mathcal{C}$ be a nonempty collection of sets for which the following hold:

1. Each set in $\mathcal{C}$ contains n elements.
2. If $k \in \{1, 2, \ldots, n+1\}$ and $\mathcal{U}$ is a subcollection of $\mathcal{C}$ with k elements, then the intersection of the sets in $\mathcal{U}$ is nonempty.

Show the intersection of all the sets in $\mathcal{C}$ is nonempty.

Proof: Assume by way of contradiction that the intersection of all the sets in $\mathcal{C}$ is empty. Let E be one of the sets in $\mathcal{C}$. Then

$$E = \{x_1, x_2, \ldots, x_n\}.$$

Since the intersection of all the sets in $\mathcal{C}$ is empty, there must be one set E_1 for which $x_1 \notin E_1$. Similarly, for each $j = 2, 3, \ldots, n$, there must be (at least) one set E_j in $\mathcal{C}$ for which $x_j \notin E_j$. Then the intersection

$$E \cap E_1 \cap E_2 \cap \cdots \cap E_n = \phi.$$

This is a contradiction because the collection $\{E, E_1, E_2, \ldots, E_n\}$ is a subcollection of $\mathcal{C}$ containing at least one element and no more than $n + 1$ elements.

Notes: The original problem was stated somewhat differently and somewhat ambiguously. It was not clear, for example, if the original collection $\mathcal{C} = \{E_1, E_2, \ldots, E_s\}$

was allowed to be empty or not. Of course, it could be argued that the use of the symbol s here implies $s \geq 1$ and hence the set $\mathcal{C}$ must have at least one element. Of course, it could be argued that the notation assumes $s \geq 2$ as well, and that is presumably not what is meant.

At any rate, my statement of the problem is an attempt to make the assertion clearer. It also allows the possibility to relax various hypotheses: What if the collection $\mathcal{C}$ is allowed to be empty? What if the conclusion of a nonempty intersection in the second hypothesis only holds if $\mathcal{U}$ is a subcollection with precisely $n+1$ (distinct) elements?

Problem 1 (Problem 1.1) Show $\sqrt{2}+\sqrt{3}+\sqrt{5}$ is irrational.

Solution: Assume by way of contradiction that

$$\sqrt{2}+\sqrt{3}+\sqrt{5} = \frac{m}{n} \in \mathbb{Q} = \left\{ \frac{p}{q} : p \in \mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\},\ q \in \mathbb{N} \right\}.$$

We can also assume $(m,n) = 1$, that is m and n have no common factors. Note also that $m > 0$ since $\sqrt{2}+\sqrt{3}+\sqrt{5} > 0$.

Then,

$$n(\sqrt{2}+\sqrt{3}) = m - n\sqrt{5},$$

so

$$n^2(5+2\sqrt{6}) = m^2 + 5n^2 - 2mn\sqrt{5} \qquad \text{or} \qquad 2n^2\sqrt{6} = m^2 - 2mn\sqrt{5}.$$

Therefore,

$$n\sqrt{6} + m\sqrt{5} = \frac{m^2}{2n} \in \mathbb{Q}.$$

Then

$$6n^2 + 5m^2 + 2nm\sqrt{30} = \frac{m^4}{4n^2} \qquad \text{and} \qquad \sqrt{30} = \frac{1}{2nm}\left(\frac{m^4}{4n^2} - 6n^2 - 5m^2\right) = \frac{p}{q} \in \mathbb{Q}.$$

Again we take $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ with $(p,q) = 1$; we in fact know $p \in \mathbb{N}$. Then

$$30q^2 = p^2,$$

so p divides $30q^2 = (2)(3)(5)q_1^2 q_2^2 \cdots q_k^2$ where q has prime factorization $q = q_1 q_2 \cdots q_k$, each q_j for $j = 1, 2, \ldots, k$ is prime, but the prime factors $q_1, q_2, \ldots, q_k$ are not necessarily distinct. If p similarly has prime factorization $p_1 p_2 \cdots p_\ell$, then p_1 also divides

$30q^2 = (2)(3)(5)q_1^2q_2^2\cdots q_k^2$. Clearly, p_1 must also divide $q_1^2q_2^2\cdots q_k^2$, but then p_1 is a common factor of p and q, and this is a contradiction because p and q have no commone factors.

To see this a slightly different way, one can assert first, based on the condition $(p, q) = 1$, that $p_1 \neq q_j$ for $j = 1, 2, \ldots, k$. Therefore,

$$p_1 \in \{2, 3, 5\}\backslash\{q_1, q_2, \ldots, q_k\}.$$

That is,

$$abq^2 = p_1p_2^2\cdots p_\ell^2$$

where $\{a, b\} = \{2, 3, 5\}\backslash\{p_1\}$. This is a contradiction because we know p_1 does not divide abq^2.

Notes: Gelca and Andrescu improve/simplify the argument given above by starting the analysis of the relation $30q^2 = p^2$ by dividing by the prime factor 2: It must be the case that 2 divides p. Therefore,

$$(2)(15)q^2 = (2)^2(p/2)^2 \qquad \text{or} \qquad 15q^2 = 2(p/2)^2.$$

It then follows that 2 divides q, so p and q have the common factor 2 contradicting $(p, q) = 1$. They refer to this as "Pythagoras' method for proving $\sqrt{2}$ is irrational."

Perhaps a bit cleaner presentation may be based on the observation that typical algebraic manipulations of rational numbers give rational numbers, that is, the rational numbers $\mathbb{Q}$ is a **field**, so $\mathbb{Q}$ is closed under the operations of arithmetic. Thus, if

$$\sqrt{2} + \sqrt{3} + \sqrt{5} = r \in \mathbb{Q}$$

then

$$2 + 2\sqrt{6} + 5 = r^2 - 2r\sqrt{5} + 5 \qquad \text{so that} \qquad \sqrt{6} - r\sqrt{5} = \frac{r^2}{2}$$

and

$$6 - 2r\sqrt{30} + 5r^2 = \frac{r^4}{4} \qquad \text{and} \qquad \sqrt{30} = \frac{1}{2r}\left(6 + 5r^2 - \frac{r^4}{4}\right) \in \mathbb{Q}.$$

One may then proceed with the assumption

$$\sqrt{30} = \frac{p}{q} \in \mathbb{Q}$$

and obtain a contradiction as above.

More lengthy or less clean routes to the same conclusion $\sqrt{30} \in \mathbb{Q}$ may be followed by grouping a different way before squaring, for example,

$$\sqrt{2} + \sqrt{5} = r - \sqrt{3}$$

or not grouping at all:

$$2 + 3 + 5 + 2\sqrt{6} + 2\sqrt{10} + 2\sqrt{15} = r^2$$

and squaring again with

$$\sqrt{6} + \sqrt{10} + \sqrt{15} = s = \frac{1}{2}(r^2 - 10)$$

so that

$$31 + 2\left(2\sqrt{15} + 3\sqrt{10} + 5\sqrt{6}\right) = s^2.$$

Chapter 2

Fall 2024

Here is a record of some problems considered duing the Fall semester of 2024.

2.1 Thursday August 22, 2024, 5PM to 7PM Skiles 255

I think I started with "proof by contradiction" as a kind of subject from Gelca and Andrescu. Perhaps I started with suggesting someone show the following:

> There are infinitely many primes.

This is apparently called Euclid's theorem. (Who knew?)

A more interesting problem is given as an example by Gelca and Andrescu. The version I posed is a modified version which is even a little harder I think.

> If
>
> $$P(x) = a_0 + a_1 x + \cdots + a_n x^n$$
>
> is a polynomial with $P(j)$ a prime number for $j = 1, 2, 3, \ldots$, then P is a constant polynomial.

I pointed out that the version posed by Gelca and Andrescu with $P(0)$ included as a prime value is easier.

I think that is more or less what we talked about during the first meeting.

2.2 September 29

2.2.1 Induction

On this day we considered showing the sum of the first n natural numbers is given by

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}.$$

This is sometimes called Gauss' formula; it can be proved by induction.

We also considered similar formulas for squares

$$\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}.$$

and cubes

$$\sum_{j=1}^{n} j^3 = \left(\sum_{j=1}^{n} j\right)^2 = \frac{n^2(n+1)^2}{4}.$$

A more interesting induction problem was Fermat's little theorem:

> If p is a prime number and n is a positive integer, then
>
> $$p \mid n^p - n.$$

2.2.2 Probability

Problem B4 from the 1985 Putnam exam was proposed by (I believe) Shikhar Ahuja:

> If a point P is chosen "at random" on the unit circle $\mathbb{S}^1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$, and another point Q is chosen "at random" in the unit disk $B_1(\mathbf{0}) = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 < 1\}$, what is the "probability" that the coordinate rectangle[1] having the segment PQ as diagonal lies entirely in the closed disk $\overline{B_1(\mathbf{0})} = B_1(\mathbf{0}) \cup \mathbb{S}^1$?

Madeline Greco offered the following solution:

[1] i.e., rectangle with sides parallel to the coordinate axes

The answer is the average value of the probability Π that given $P \in \mathbb{S}^1$ the rectangle lies in $\overline{B_1(\mathbf{0})}$. Taking $P = (\cos t, \sin t)$ with $0 \leq t < 2\pi$, the average is

$$\frac{1}{2\pi} \int_0^{2\pi} \Pi \, dt,$$

and the probability Π is the area of the rectangle determined by P and $-P$ divided by the area of the disk:

$$\Pi = \frac{4|\cos t \sin t|}{\pi}.$$

Thus the answer is

$$\begin{aligned} \frac{2}{\pi^2} \int_0^{2\pi} |\cos t \sin t| \, dt &= \frac{8}{\pi^2} \int_0^{\pi/2} \cos t \sin t \, dt \\ &= \frac{4}{\pi^2} \int_0^{\pi/2} \sin(2t) \, dt \\ &= -\frac{2}{\pi^2} \cos(2t) \Big|_{t-0}^{\pi/2} \\ &= \frac{4}{\pi^2}. \end{aligned}$$

I attempted to offer an alternative to Madeline's "average" explanation by suggesting the use of some form of the law of joint probability and the law of total probability. Thus, it is perhaps possible to think of the answer rather as a sum of the probabilities associated with choices of points P around $\mathbb{S}^1$, or more properly intervals partitioning $\mathbb{S}^1$ rather than their average. Specifically, if $A_1, A_2, \ldots, A_k$ is a partition of $\mathbb{S}^1$ by small arcs with each arc A_j containing a point P_j for $j = 1, 2, \ldots k$, then for any P chosen in A_j (my suggestion is) the probability associated with the square determined by P and Q falling within $\overline{B_1(\mathbf{0})}$ is **approximately**

$$\Pi_j = \frac{4|\cos t_j \sin t_j|}{\pi}$$

where $P_j = (\cos(t_j), \sin(t_j))$. Thus, by the "**law of joint probability**," the probability that P is chosen in A_j **and** the rectangle determined by P and Q is in the closure of the disk is (approximately) the product

$$\frac{\text{length } A_j}{2\pi} \, \Pi_j.$$

Summing these values according to the "**law of joint probability**"

$$\sum_{j=1}^{k} \frac{\text{length } A_j}{2\pi} \ \Pi_j = \sum_{j=1}^{k} \frac{\text{length } A_j}{2\pi} \ \frac{4|\cos t_j \sin t_j|}{\pi}$$
$$= \frac{2}{\pi^2} \sum_{j=1}^{k} |\cos t_j \sin t_j| \ \text{length } A_j.$$

The last expression is a Riemann sum for the integral

$$\frac{2}{\pi^2} \int_0^{2\pi} |\cos t \sin t| \, dt$$

suggested by Medeline as an average. It is certainly true that the Riemann sum converges to the integral as the "norm" of the partitition, that is

$$\max\{\text{length}(A_j) : j = 1, 2, \ldots, k\}$$

tends to zero. There is another assumption here however, namely that the limiting value of the sums converges to the desired probability value.

2.3 September 5

2.3.1 Main Problem

I believe Wesley Lu suggested the following problem from the 2019 Asia-Pacific Math Olympiad which was the first problem on that exam:

> Find all functions $f : \mathbb{N} \to \mathbb{N}$ satisfying
>
> $$f(n) + m \qquad \text{divides} \qquad n^2 + f(n)f(m) \qquad \text{for all } n, m \in \mathbb{N}.$$

Several people made contributions and Wesley gave a hint. Here is some kind of summary solution with comments/notes.
STEP 1. Taking $n = p$ prime and $m = f(p)$ the divisibility condition gives some $k \in \mathbb{N}$ for which

$$2kf(p) = p^2 + f(p)f(f(p)).$$

This means

$$[2k - f(f(p))]f(p) = p^2.$$

That is, $f(p)$ divides p^2. Since p is prime, this means $f(p) = 1$ or $f(p) = p$ or $f(p) = p^2$.
STEP 2. If $f(p) = 1$ for some prime, then taking $m = n = p$ in the original relation gives

$$k(1 + p) = p^2 + 1$$

for some $k = k(p) \in \mathbb{N}$. Clearly $k > 1$, and it follows that

$$(k - 1)(1 + p) = p^2 - p = p(p - 1).$$

This is a contradiction because there can be no factor of $1 + p$ on the right. In particular, $1 + p$ is not divisible by p, so we know $k - 1$ must be divisable by p. This implies

$$\left(\frac{k-1}{p}\right)(1 + p) = p - 1,$$

but this is nonsense because the left side here is larger than $p-1$, specifically $p+1 > p - 1$ and $(k - 1)/p \geq 1$. Therefore, we know it is not the case that $f(p) = 1$.
STEP 3. If $f(p) = p^2$, then we can again take $m = n = p$ in the original relation so that

$$k(p^2 + p) = p^2 + p^4 \qquad \text{or} \qquad k(p + 1) = p(p^2 + 1)$$

for some $k = k(p) \in \mathbb{N}$. Again $k > 1$. It follows that p must divide k. Writing $\ell = k/p \in \mathbb{N}$, one finds

$$\ell(p + 1) = p^2 + 1.$$

Here $\ell > 1$ and

$$(\ell - 1)(p + 1) = p^2 - p = p(p - 1).$$

As observed in **STEP 2** there is no factor of $p + 1$ on the right.
STEP 4. We conclude from the contradictions of **STEP 2** and **STEP 3** that $f(p) = p$ whenever p is a prime number.

We note also that the identity funtion $\mathrm{id}_{\mathbb{N}} : \mathbb{N} \to \mathbb{N}$ by $\mathrm{id}_{\mathbb{N}}(n) = n$ for all n does satisfy the original condition of the problem with

$$\mathrm{id}_{\mathbb{N}}(n) + m = n + m \qquad \text{and} \qquad n^2 + \mathrm{id}_{\mathbb{N}}(n)\mathrm{id}_{\mathbb{N}}(m) = n(n + m)$$

so that the latter is divisible by the former. Thus, $f(n) = \mathrm{id}_{\mathbb{N}}(n)$ is one possible function satisfying the required condition.

It is perhaps natural to conjecture at this point that the identity is the only such function. At any rate that is what we proceed to show:

Take $n = p$ prime and $m \in \mathbb{N}$ arbitrary. Then the original relation reads

$$k(p+m) = p^2 + pf(m) = p[p + f(m)]$$

where $k = k(p, m) \in \mathbb{N}$. Consider m fixed so $k = k(p)$, and consider primes p for which $p > m$. For these primes, p does not divide $p + m$, so p must divide k and setting $\ell = k/p \in \mathbb{N}$ we find

$$\ell(p+m) = p + f(m)$$

Since $p + f(m) \geq p + m$, we know $f(m) \geq m$. Thus, either $f(m) = m$ for $f(m) > m$.

In the latter case, $\ell > 1$ and we can write

$$(\ell - 1)(p+m) = f(m) - m.$$

In particular, since $\ell - 1 \geq 1$, this means

$$(p+m) \leq f(m) - m$$

for all large enough primes. Since the right side $f(m) - m$ is fixed independent of the prime p, we obtain a contradiction for p any prime larger than $f(m) - 2m$.

We conclude $f(m) = m$ for all $m \in \mathbb{N}$ and $f = \mathrm{id}_{\mathbb{N}}$. $\square$

Note on $f(1)$ The argument of **STEP 4** shows $f(1) = 1$ in particular.

Let's consider this special case: Taking $n = p$ prime and $m = 1$ the relation satisfied by f gives

$$k(p+1) = p^2 + pf(1) = p[p + f(1)].$$

The argument is slightly simpler at this point. We know immediately that p does not divide $p + 1$ and therefore must divide k. With $\ell = k/p$ and

$$\ell(p+1) = p + f(1),$$

we also know immediately that either $f(1) = 1$ or $f(1) > 1$. In the latter case $\ell > 1$ and

$$(\ell - 1)(p+1) = f(1) - 1.$$

This means $p + 1 \leq f(1) - 1$ for all primes, and we get a contradiction. Of course, we can simply say $f(1) \geq 1$ so that $\ell - 1 \geq 0$. The cases then split as $\ell = 1$, in which case $f(1) = 1$ directly from the relation, and $\ell > 1$, in which case we get the contradiction.

Taking $m = n = 1$ in the original condition leads to the conclusion $f(1) = 1$ more directly:

$$k[f(1) + 1] = 1 + [f(1)]^2.$$

If $f(1) = 1$, then $k = 1$, but if $f(1) > 1$, then $k > 1$ and we can subtract $f(1) + 1$ from both sides to obtain

$$(k - 1)[f(1) + 1] = [f(1)]^2 - f(1) = f(1)[f(1) - 1].$$

This means $k - 1$ must be divisible by $f(1)$ or $(k - 1)/f(1) = \ell \in \mathbb{N}$ and

$$\ell[f(1) + 1] = f(1) - 1$$

which is nonsense because $f(1) - 1 < f(1) + 1 \leq \ell[f(1) + 1]$.

Note on STEP 1: Taking n a general natural number and $m = f(n)$ leads to the more general assertion $f(n)$ divides n^2 for all $n \in \mathbb{N}$. We only used this assertion in the case $n = p$ is prime, and in fact Wesley gave the nice hint to try to use this more general divisibility in the case when "n^2 has a minimal number of divisors."

Here is the general argument: The divisibility condition gives some $k \in \mathbb{N}$ for which

$$2kf(n) = n^2 + f(n)f(f(n)).$$

This means

$$[2k - f(f(n))]f(n) = n^2.$$

That is, $f(n)$ divides n^2.

NOTE on divisibility: The condition m divides n for any integers in $\mathbb{Z}$ means there exists an integer $k \in \mathbb{Z}$ such that $km = n$. When restricted to natural the numbers $n, m \in \mathbb{N}$ the condition of divisibility is often expressed as

$$m \mid n,$$

and this kind of divisibility has several properties we have used above and are nice to know.

First of all if $m \mid n$, then we always know $m \leq n$ with $m = n$ if and only if $k = 1$. In particular if $km = n$ with $k > 1$, then we know $m \mid n - m$. We used this observation several times above.

Another simple fact about divisibility is that if $m \mid n = n_1 n_2$ for some $n_1, n_2 \in \mathbb{N}$ with m and n_1 relatively prime, i.e., $(m, n_1) = 1$, then $m \mid n_2$. To see this, write $km = n_1 n_2$. Since $(m, n_1) = 1$, it must be that $n_2 \mid k$, thus,

$$\frac{k}{n_1} m = n_2.$$

Another general observation is that two consecutive integers are relatively prime. We used this when one of the integers is a prime number. If m and $m + 1$ have a common factor $\ell > 1$, then we can write $m = k_1 \ell$ and $m + 1 = k_2 \ell$. This means

$$1 = m + 1 - m = (k_2 - k_1)\ell > 1$$

which is a contradiction. In particular, $p + 1$ and p are relatively prime as are $p - 1$ and p when p is prime. More generally, if p is a prime and $m < p$, then p does not divide $p + m$. In fact,

$$\frac{p+m}{p} = 1 + \frac{m}{p}$$

so this observation follows directly from the division (algorithm).

There may be some other handy facts we have used, but I'm not seeing them at the moment. You can perhaps run across them by attempting a solution using the notation $m \mid n$ as seemed to be the preference for the arguments presented in class. It is a good exercise to go back and justify carefully manipulations using this notation; if you are not careful with it, you can make errors. For example, it was asserted in class that if $f(n) \mid n^2$ for an integer $m = n$, then $m = n$ or $m = n^2$. This is not correct, and I think even for a prime $n = p$ we neglected to consider the possibility that $m = f(p) = 1$, though I did consider that possibility in the solution above.

2.3.2 Another similar problem

Wesley's problem reminded me of a problem mentioned by Gelca and Andrescu, and I offered a simpler version of that problem as an alternative:

> If $f : \mathbb{N} \to \mathbb{N}$ is strictly increasing, that is, $f(m) < f(n)$ for $m, n \in \mathbb{N}$ with $m < n$, $f(2) = 2$, and
>
> $$f(mn) = f(m)f(n) \qquad \text{for all } m, n \in \mathbb{N},$$
>
> then show $f(n) = n$ for all $n \in \mathbb{N}$, that is f is the identity function on $\mathbb{N}$.

I already had a suspicion that the answer to Wesley's problem was that the only such function was the identity function, but I didn't know how to prove it. This one really is much easier however.

I'd like to ask a similar question: What is the motivation for the condition

$$f(n) + m \qquad \text{divides} \qquad n^2 + f(n)f(m)$$

in the Asia-Pacific problem?

Wesley asked me about the motivation for the condition $f(mn) = f(m)f(n)$. A function satisfying this condition is said to be "multiplicative," and there are various functions in number theory that are multiplicative including something called Euler's totient function, which you can look up. Gelca and Andrescu aslo mention that Paul Erdös proved a more general version of the assertion above for general increasing

The actual version from Gelca and Andrescu doesn't give the condition above but rather that the condition $f(mn) = f(m)f(n)$ holds when m and n are relatively prime, which is the same thing as saying m and n have no common divisors except $k = 1$ or that the greatest common factor of m and n is $k = 1$. This condition is also expressed by writing $(m, n) = 1$ or $GCD(m, n) = 1$. I have never seen it expressed as $GCF(m, n) = 1$, but I don't know why.

2.3.3 Another relatively easy problem

I also suggested another simple induction problem from Gelca and Andrescu:

> Show that if $n \in \mathbb{N}$ and $x \in \mathbb{R}$, then
>
> $$|\sin(nx)| \leq n|\sin x|.$$

No one gave a solution for this.