FEATURE

10

MY FAVORITE PROBLEM

Bert and Ernie

Zachary Abel[†]
Harvard University '10
Cambridge, MA 02138
zabel@fas.harvard.edu

10.1 Allow Me to Introduce Myself

The primary driving force behind my mathematical career up to now—through recreation, competition, and research—has been problem solving. This problem solving process allows a two-way channel of communication between myself and my mathematical experience. First, solving a problem allows me to draw from my current cache of **intuitions**, **bits of knowledge** (or in the words of Scott Kominers, **knowledgecules**), and **ideas** that might be applicable to the current challenge, thus facilitating directed reflection into my current mathematical understanding. In turn, the effort exerted in solving (or at least working on) the problem only adds to this cache and strengthens this same understanding. This cyclic (singly generated!) process of reflection and growth turns the act of solving problems—and indeed of studying mathematics—into a beautiful and highly personal experience.

While perusing my problem repertoire searching for a "favorite," I had trouble pinpointing a leader because different partial orderings—trickiness, elegance, difficulty (unsolved?), cuteness...—lead to vastly different maximal elements. So I finally decided to choose a problem that best illustrates the process above: specifically, one that illustrates the powerfully personal nature of mathematical study.

And now, we present the problem:

Bert and Ernie. *Bert is thinking of an ordered quadruple of integers (a, b, c, d). Ernie, hoping to determine these integers, hands Bert a 4-variable polynomial $P(w, x, y, z)$ with integer coefficients, and Bert returns the value of $P(a, b, c, d)$. From this value alone, Ernie can always determine Bert's original ordered quadruple. Construct, with proof, one polynomial that Ernie could have used.*

To simplify discussion, allow me to strip the PBS language. The following problem is equivalent:

No More Bert and Ernie. *Find, with proof, a polynomial $P \in \mathbb{Z}[w, x, y, z]$ so that $P : \mathbb{Z}^4 \hookrightarrow \mathbb{Z}$ is injective.*

We are thus given two tasks: extract multiple pieces of information from a single integer (namely $P(a, b, c, d)$), and do so using integer polynomials. If we were dealing with polynomials but not necessarily integers, we could use a polynomial like

$$P(w, x, y, z) = w\sqrt{2} + x\sqrt{3} + y\sqrt{5} + z\sqrt{7}$$

[†]Zachary Abel, Harvard '10, is a computer science and mathematics concentrator. He is an avid problem solver and researcher, with interests in such varied fields as computational geometry, number theory, partition theory, category theory, and applied origami. He is a founding member of The HCMR and currently serves as Problems Editor, Issue Production Director, and Graphic Artist.

and rely on the fact that the set $\{\sqrt{n} \mid n \in \mathbb{N} \text{ is squarefree}\}$ is linearly independent over the rationals. Or, if we were restricted to integers but not to polynomials, we could easily set

$$P(w, x, y, z) = 2^w 3^x 5^y 7^z$$

and use unique factorization to recover the exponents. The difficulty arises from the combination.

This double condition forces a convergence of algebraic and number-theoretic ideas. Beyond that, however, anything goes: the problem does not further restrict the range of useful directions of exploration. Since a wide variety of ideas can be usefully applied to the problem, a solver reveals a great deal about his or her problem solving process simply by writing down the final proof.

10.2 Draw from Knowledgecules

Anyone who has asked about the cardinality of $\mathbb{N}^2$ (or $\mathbb{Q}$) and been shocked to find that it equals that of $\mathbb{N}$ has undoubtedly stumbled across the enumeration of the $\mathbb{N}^2$ as depicted in Figure 10.1. Perhaps they have also noticed that this enumeration can be written down as a rational polynomial:

$$\ell(x, y) = \frac{(x + y - 2)(x + y - 1)}{2} + y.$$

This means that $2\ell : \mathbb{N}^2 \to \mathbb{N}$ is an injective integer polynomial! Having this fact in our repertoire, all we have to do now is find a way to replace $\mathbb{N}^2$ with $\mathbb{Z}^4$.

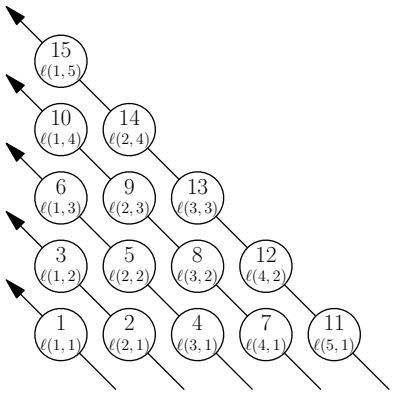

Figure 10.1: A proof that $|\mathbb{N}^2| = |\mathbb{N}|$ by enumerating $\mathbb{N}^2$ along diagonals.

Solution 1 by Nick Wage, '10. Use the notation $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. We construct the following polynomials in order:

$$\begin{aligned}
A &: \mathbb{N}_0^2 \to \mathbb{N}, & (x, y) &\mapsto 2\ell(x + 1, y + 1) \\
B &: \mathbb{N}_0^4 \to \mathbb{N}, & (w, x, y, z) &\mapsto A(A(w, x), A(y, z)) \\
C &: \mathbb{Z}^2 \to \mathbb{N}, & (x, y) &\mapsto B(x^2, (x + 1)^2, y^2, (y + 1)^2) \\
P_1 &: \mathbb{Z}^4 \to \mathbb{N}, & (w, x, y, z) &\mapsto C(C(w, x), C(y, z)).
\end{aligned}$$

It is clear from these definitions that A, B, C, and P_1 are integer-coefficient polynomials. We now show that each, in turn, is also injective, so that P_1 is the desired polynomial.

Polynomial $A(x, y) = 2\ell(x + 1, y + 1)$ is injective, as mentioned in the previous paragraph. This means there exists a pair of well-defined left inverses A_x and A_y (not necessarily polynomial) so that $A_x(A(x, y)) = x$ and $A_y(A(x, y))$. So for any $(w, x, y, z) \in \mathbb{N}_0^4$ we have

$$A_x(A_x(B(w,x,y,z))) = w, \qquad A_x(A_y(B(w,x,y,z))) = x,$$
$$A_y(A_x(B(w,x,y,z))) = y, \qquad A_y(A_y(B(w,x,y,z))) = z.$$

This means that we can decipher (w, x, y, z) from $B(w, x, y, z)$, whence B is injective. To see that C is injective, suppose we know the values of x^2 and $(x + 1)^2$ (which we will, by B's injectivity) for some integer x. If $(x+1)^2 < x^2$, x must be negative, i.e. $x = -\sqrt{x^2}$, and if $(x+1)^2 > x^2$ then x is non-negative, i.e. $x = \sqrt{x^2}$. So we may uniquely determine x from $C(x, y) = B(x^2, (x + 1)^2, y^2, (y + 1)^2)$, and likewise for y. So C is injective. Finally, P_1's injectivity follows from that of C by the same argument used for B. So this P_1 does indeed solve the problem. □

In order to turn 2ℓ into a full solution (i.e. to replace $\mathbb{N}$s with $\mathbb{Z}$s in the domain), this solver used the clever injective map $\mathbb{Z} \hookrightarrow \mathbb{N}^2,\ x \mapsto (x^2, (x + 1)^2)$. Other methods of injecting $\mathbb{Z}$ into $\mathbb{N}$ may be used for alternate solutions. For example, having encountered (during some dabbling in partition theory) **Euler's Pentagonal Number Theorem**, namely the result

$$\prod_{k=1}^{\infty}(1-x^k) = \sum_{i=-\infty}^{\infty}(-1)^k x^{k(3k+1)/2} = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \cdots,$$

(note that no power of x is hit twice by the sum), I recognized that $m(x) = \frac{x(3x+1)}{2}$ is such an injective polynomial $\mathbb{Z} \hookrightarrow \mathbb{N}_0$. This gives rise to the next solution.

Solution 2 by the author. Define $n(x) = 2m(x) + 1 = x(3x + 1) + 1$, which has integer coefficients and strictly positive values. Note that $n(x) = n(y)$ for any integers x and y implies that $x = y$ or $x + y = -\frac{1}{3}$, i.e. $x = y$. Thus, $n : \mathbb{Z} \hookrightarrow \mathbb{N}$ is injective. So we may define the injective polynomial $D : \mathbb{Z}^2 \hookrightarrow \mathbb{N}$ by $(x, y) \mapsto 2\ell(n(x), n(y))$, and the final solution $P_2(w, x, y, z) = D(D(w, x), D(y, z))$ is found as above. □

10.3 Draw from Intuition

Consider the simple **floor** (or **greatest integer**) **function** $\lfloor\cdot\rfloor$. Given any number r, this function tells us two important pieces of information: macroscopically, the unit interval in which r lies, namely the half-open interval $[\lfloor r\rfloor, \lfloor r\rfloor + 1)$; and microscopically, how far away we landed from that integer, $r - \lfloor r\rfloor$. Intuitively, we have a number of larger targets equipped with small, disjoint regions for error. This separation into primary and error terms comes most directly from analysis, by approximating a function locally with its linear derivative and quadratic error. But the method has certainly been put to good use in other ways: for example, Hamming's "error correcting codes" tightly pack disjoint balls in $\mathbb{F}_2^n$ in order to (1) identify a code word even if there were a few errors in the transcription, and (2) locate those errors.

This disjoint wiggle-room intuition can be very beneficial for the problem at hand by dividing the given output into a primary, large value with a relatively tiny error term added on, both of which are thus uniquely determined. The fuzzy idea of exploiting big and small terms (perhaps by throwing in huge exponents and coefficients!) that comes from the above intuition is certainly enough to solve the problem, especially when one leans on the intuitive notions of big and small as elucidated by the infamous "Big 'O' Notation." A rather nice way of combining these ideas is explained below.

Solution 3 by the author. Suppose we have two positive integers a and b with $a < b$. I claim that the value $b^2 + a$ uniquely identifies both a and b. Indeed, since $b^2 + 1 \le b^2 + a \le b^2 + b - 1$, and the intervals $[c^2 + 1, c^2 + c - 1]$ and $[(c + 1)^2 + 1, (c + 1)^2 + (c + 1) - 1]$ are disjoint for

all positive integers c (since $c^2 + c - 1 < (c+1)^2 + 1$), the value $b^2 + a$ falls into at most one such interval, which uniquely determines b. The value of a follows. We thus obtain an injection $E : \mathbb{Z}^2 \hookrightarrow \mathbb{N},\ (x, y) \mapsto n(x) + (n(x) + n(y))^2$ (where n is the injection $\mathbb{Z} \hookrightarrow \mathbb{N}$ from above), and as usual the final solution $P_3(w, x, y, z) = E(E(w, x), E(y, z))$ is immediate. □

In fact, the lemma used above may be strengthened:

Lemma 1. *For fixed n and k, the equation $k = a_n^n + a_{n-1}^{n-1} + \cdots + a_1$ has at most one solution in positive integers $a_1, \ldots, a_n$ subject to the condition $0 < a_1 < a_2 < \cdots < a_n$.*

Proof. We have the inequality

$$\begin{aligned} a_n^n + 1 < a_n^n + \cdots + a_1 &< a_n^n + a_n^{n-1} + \cdots + a_n \\ &< a_n^n + \tbinom{n}{n-1} a_n^{n-1} + \cdots + \tbinom{n}{1} a_n + 2 = (a_n + 1)^n + 1, \end{aligned}$$

so the value of $a_n^n + \cdots + a_1$ falls into at most one interval of the form $[c^n + 1, (c+1)^n]$, which uniquely defines the value of a_n. The result then follows by induction. □

We therefore obtain a slightly more elegant(?) solution.

Solution 4 by Scott Kominers '09 and the author. The polynomial $P_4 : \mathbb{Z}^4 \to \mathbb{N}$ defined by

$$\begin{aligned} P_4(w, x, y, z) = n(w) &+ \big(n(w) + n(x)\big)^2 + \big(n(w) + n(x) + n(y)\big)^3 \\ &+ \big(n(w) + n(x) + n(y) + n(z)\big)^4 \end{aligned} \tag{10.1}$$

is injective by Lemma 1. □

Note that not only is the error-term intuition useful for solving the problem, but the proof itself—even simply line (10.1) alone—clearly elucidates the idea that the solver had in mind.

10.4 Draw from Idea

Speaking of ideas, here are two more, very ill-formed ideas toward different solutions, both derived from number theory (as a healthy break from the analysis and algebra influences above). We are told to extract multiple pieces of information from a single integer, so we can probably do something with the **representations** of this integer: indeed, the (decimal or binary) **digits** of a number give lots of distinct pieces of information, as do the (prime) **divisors**.

It is often the case that one can store valuable polynomial information in the digits of a number. For example, it is known that if $a_n \ldots a_1 a_0$ is the base-10 expansion of a prime q, then the polynomial $p(x) = a_n x^n + \cdots + a_1 x + a_0$ is irreducible [BFO], and the proof relies heavily on the fact that $p(10) = q$. For this problem, though, I found it difficult to directly apply this digit-storing idea, as most of the potential solutions I found along these lines ended up being exponential, not polynomial. However, a slight generalization of the idea of **digit** leads perhaps to base Fibonacci,[1] base factorial,[2] or base -4 representations,[3] none of which I could get to work here. Another slight generalization of the digit notion—never fully giving up on this idea, but instead running as far as necessary with it—perhaps leads to quadratic form representation theory and representation as sums of (two or more) squares, which, unfortunately, is not usually unique (except for primes $p \equiv 1$ or $2 \bmod 4$ in the two squares case). This in turn recalls Waring's problem and representations as sums of higher powers. Finally, perhaps, one considers sums of *different* powers, and is thus lead to a solution similar to Solution 4. As the increasing powers a_i^i recall the increasing

[1] e.g. IMO 1993 #5
[2] e.g. AIME-II 2000 #14
[3] e.g. USAMO 1996 #4

exponents of the base in usual base-number representation, we are really not too far away from the initial base-digit idea.

The other idea was that of (prime) factors. Suppose we had an injective polynomial $p(x)$ that only output primes. Then knowing the value of $n = p(x) \cdot p(y)$ would uniquely tell you the (unordered) set $\{x, y\}$ by simply factoring n. Unfortunately, such a polynomial does not exist,[4] but the idea may still be useful, and prime factors and polynomials can mix well together in other ways. For example, given any $x \in \mathbb{Z}$, all prime divisors of $x^2 + 1$ must be of the form $p \equiv 1$ or $2 \bmod 4$; cyclotomic polynomials Φ_m directly generalize this fact by only allowing prime divisors of $\Phi_m(x)$ to be congruent to $1 \bmod m$ with finitely many exceptions.[5] However, as I have not yet found a solution down this road, let us move back to the original *divisors* idea, this time throwing out the *prime* part.

Divisors always come in pairs, but how can we distinguish a particular pair? Can we distinguish between pairs of divisors if there is only one nontrivial pair? (Yes, but then $n = pq$ is a product of two primes, and we are back to primes.) What if both elements in the divisor pair are equal? Then $n = a^2$, and we do not get multiple values. But what if the divisors are *almost* equal? I.e., what if we pick the *closest* pair of divisors? In this case, the pair is certainly uniquely defined.

Along these lines, we would like to be able to say that if $m \gg r$, and if a and b with $a < b$ have $ab = m(m + r)$, then $a \leq m < m + r \leq b$, i.e. the closest pair of divisors of $m(m + r)$ is in fact $(m, m + r)$. Indeed, a lemma of this form is not difficult to prove:

Lemma 2 (1998 St. Petersburg City Mathematical Olympiad)**.** *Let n be a positive integer. Show that any number greater than $n^4/16$ can be written in at most one way as the product of two of its divisors having difference not exceeding n.*

Proof (method by Titu Andreescu and Dorin Andrica). Suppose $a < c \leq d < b$ with $ab = cd = t$ and $b - a \leq n$. Note that

$$(a + b)^2 - n^2 \leq (a + b)^2 - (b - a)^2 = 4ab = 4cd = (c + d)^2 - (d - c)^2 \leq (c + d)^2,$$

so that $(a + b)^2 - (c + d)^2 \leq n^2$. But as $a + b > c + d$ (since the function $f : x \mapsto x + t/x$ decreases for $t < \sqrt{x}$, which means $f(a) > f(c)$), we find

$$n^2 \geq (c + d + 1)^2 - (c + d)^2 = 2c + 2d + 1.$$

Finally, the AM-GM inequality gives

$$t = cd \leq \left(\frac{c + d}{2}\right)^2 \leq \frac{(n^2 - 1)^2}{16} < \frac{n^4}{16},$$

proving the claim. □

Thus armed, we arrive at our last solution to the Bert and Ernie problem:

Solution 5 by the author. Consider the polynomial $F : \mathbb{Z}^2 \to \mathbb{N}$ defined by

$$F(x, y) = (n(x) + n(y))^2 \cdot \left((n(x) + n(y))^2 + n(x)\right).$$

As $F(x, y) > n(x)^4 > n(x)^4/16$, and as the difference of the two factors is exactly $n(x)$, Lemma 2 proves that, for fixed x and y, the factorization $F(x, y) = ab$ with $a \leq b$ and $b - a \leq n(x)$ is unique. Taking (a, b) to be the pair of divisors of $F(x, y)$ that are closest together, we must obtain

$$a = (n(x) + n(y))^2, \qquad b = (n(x) + n(y))^2 + n(x).$$

[4] Indeed, if an integer polynomial f has only prime outputs, then since the prime $q = f(1)$ divides all numbers $f(1 + kq)$ for $k \in \mathbb{Z}$, all of these prime values must be $\pm q$. But then f takes one of those values infinitely many times, so f is constant.

[5] Specifically, if $p \mid \Phi_m(x)$, then either $p \equiv 1 \bmod m$ or $p \mid m$, a result apparently proved by Legendre [Ga].

From here, x and y can be reconstructed, whence F is injective. Then

$$P_5(w, x, y, z) = F(F(w, x), F(y, z))$$

solves the problem. □

The preceding solution is an attempt to illustrate some of my thinking while engaging the two ideas mentioned above. It follows a depth-first-like traversal through the directed graph of free idea association, moving to a related node if the current ideas become exhausted or seem unfruitful. Whether or not my brain actually thinks in depth-first terms (or perhaps it is performing greedy best-first, or even A^* search), exploring these associations can certainly be a useful exercise. Almost certainly, the resulting graph traversal will differ greatly from person to person.

10.5 A Parting Challenge: The Bert and Ernie Contest

Now that you have seen my thoughts and approaches for this problem, I would love to see yours! I hereby present the following challenge:

The Bert and Ernie Contest. *Show us how* you *would solve my favorite problem.*

You are invited to submit a different solution based on ideas or premises not discussed here, along with a short description of the methods and approaches used. Successful submissions will be acknowledged both on The HCMR's website and in future issues; the most novel and illuminating will be published. Submissions for this Bert and Ernie Contest should be directed to me (Zachary Abel), either at `hcmr-problems@hcs.harvard.edu` or at the address on the inside front cover.

10.6 Acknowledgments

I am very grateful to, among others and in no particular order, Menyoung Lee, Daniel Litt, Brett Harrison, Scott Kominers, Eleanor Birrell, Brian Basham, Eddie Keefe, Zachary Galant, Ernie Fontes, Alex Zhai, Professor Noam D. Elkies, Dr. Grant Mindle, and Dr. Barbara Currier, for stimulating discussion relating to the Bert and Ernie problem, and of course to Scott Kominers and Nick Wage for sharing their solutions. I would also like to thank my father, Dr. Bruce J. Abel who inspired me to invent this problem. I am once again indebted to Daniel Litt, Scott Kominers, and Eleanor Birrell for their helpful comments on earlier drafts of this article. Finally, I thank you in advance for your future submissions to The Bert and Ernie Contest.

References

[BFO] J. Brillhart, M. Filaseta, and A. Odlyzko: On an irreducibility theorem of Cohn, A., *Canadian Journal of Mathematics* **33** #5 (1981), 1055–1059.

[Ga] Yves Gallot: Cyclotomic polynomials and prime numbers (2000, Revised 2001), `http://pagesperso-orange.fr/yves.gallot/`