Problem-posing: a look behind the scenes

Greg Oman*

March 25, 2018

Abstract

There is no shortage of papers and books which address the topic of mathematical problem-solving. The primary objective of this note is to model, via an explicit example, the activity of mathematical problem-*creating*.

1 Introduction

George Polya's classical text *How to Solve It* ([7]) is one of many excellent resources which gives the reader strategies for mathematical problem-solving. Indeed, there are many books, papers, and websites which address this topic; for a sampling, see [1]–[6] and [8]. Certainly the activity of problem-solving is ubiquitous both in the classroom and in the world of research mathematics. One could also argue that the process of problem-*creating* plays an equally fundamental role in the development of new mathematics (more on this below). Allow me to begin by giving some context in which to interpret the title of this paper. Several questions may come to your mind. Is this a paper about how to come up with recreational problems to pose in *The Monthly*? Will it give me a blueprint for devising undergraduate thesis topics? In part, the answer is "yes" to both questions.

Now, you might ask

1. "How will reading this paper benefit me?", or
2. "What useful things do you have to relate to me that haven't already been communicated in the literature?"

To answer question (1), let me start by stating that the intended audience of this note includes both students and faculty. For students with little to no research experience, my desire is that this paper will serve as a microcosm for how more advanced mathematical research is done. For students and faculty alike, I hope this note will encourage engagement in the very rewarding activity of problem-posing.

*University of Colorado, Colorado Springs

I will now comment on query (2). As stated in the abstract, there is no dearth of articles and websites which contain problem-solving and research advice. However, to my knowledge, there does not exist a book or paper which illustrates the process of creating *and* solving a mathematical problem. Now, it is true that mathematicians (as a whole) consistently solve open problems in the literature. However, much of the mathematical landscape is developed *laterally* instead of vertically; to develop it as such, one needs to be adept at the skill of inventing problems, not just solving them. Moreover, an important question I hear quite regularly from my advisees, from undergraduates to Ph.D. students, upon giving them problems on which to work is this: *how did you come up with that problem?* Though it may be difficult or impossible to give a fully satisfactory answer, the question is significant enough that it merits being addressed. The main objective of this article is to bring to light the informal self-talk in which one often engages when in search of that elusive "flash of insight". We will do this by modeling, via an explicit example, the process of coming up with and solving a mathematical problem.

Before digging in, kindly let me make one last point: just as musical talent is not imparted by merely watching a musician compose a symphony, so too is it unrealistic to expect that reading this note will immediately result in a newfound problem-posing ability. The goal of this paper is not so much to *teach* one how to problem-pose (if this is even possible), but to *inspire* one to try. So now, without further ado, let's roll up our sleeves and get to work!

2 Blood and Guts

Our first task is to choose a field in which to work. I would prefer to avoid analysis, combinatorics, geometry, and number theory. Of course, there are many beautiful problems in these areas, but they are already well-represented on The Putnam Exam as well as in the problem sections of various mathematical periodicals. I also would like to pick a field outside of my research specialty to show you that it is actually possible to discover new mathematical gems in an area you know little about. Moreover, it is possible to accomplish this while still an undergraduate. In fact, I devised a problem during my junior year of college which ultimately appeared in *Math Horizons*. It took me awhile to submit it for publication simply because I had no idea that my problem was publishable.

Group theory seems as good as any to fit the bill, so let's run with it and see what we can do. Let me assuage any concerns that the mathematics will be overly technical: if you know the definition of "group" and "homomorphism," then you are sufficiently equipped to digest the content of this paper.

Now that we have our area, we need to find a problem. If you are not a group theorist, possibly this seems like a fool's errand. It is actually quite a bit simpler than you may think! We will let the mantra *"think deeply of simple things"* be our guide (this quote, originally attributed to Gauss, was reinvigorated in the 20th century by Arnold Ross. He made it the motto of his famous Ross Program in Mathematics for Gifted High Schoolers).

How simple, you ask? Well, what is the objective of group theory? To study groups, of course. We may as well start with the very definition of a group. We recall that a group is a triple $(G, *, e)$ consisting of a set G, an operation $*$ on G, and an element e in G for which $*$ is associative, e is a two-sided identity with respect to $*$, and every member of G has a two-sided inverse with respect to e. Now what? As Hersh poetically states in [3], "Generalization is a much-traveled high road to publication." Let's venture down this road and see where it leads. In what ways might we generalize the definition of a group? Let's remove the inverse axiom. Do we have something new? Sadly, no. We have a monoid. What if we remove the identity axiom as well? We now have a semigroup. Since there are journals devoted solely to the theory of semigroups, we probably won't find anything new here. What if we remove only the associativity axiom? In this case, we get a loop. Even if you are not familiar with all these terms, a Google search will lead you to conclude rather quickly that we have reached a dead end. But remember that on the quest to uncover fruitful questions, eliminating dead ends is often part of the job. So let's not lose all hope just yet; we've only just begun...

Aside from groups, what other objects assume a central role in group theory? Special maps between groups called homomorphisms is a most reasonable answer to this question. Recall that if G and H are groups, and $f\colon G \to H$ is a function, then f is a *homomorphism* from G to H if $f(xy) = f(x)f(y)$ for all $x, y \in G$. Consider the formalization in first-order logic below:

$$\forall x \forall y \; f(xy) = f(x)f(y).$$

How might we generalize this definition? Possibly the most obvious way is to replace the universal quantifiers with existential quantifiers to get

$$\exists x \exists y \; f(xy) = f(x)f(y). \tag{1}$$

But one soon realizes that this generalization is actually much too broad to be of any interest. Indeed, *any* function $f\colon G \to H$ which satisfies $f(e) = e$ satisfies (1) (choose $x := y := e$). Moreover, if x and y are any distinct non-identity elements of G, then we may define $f(x)$ and $f(y)$ to be arbitrary elements of H and then set $f(xy) := f(x)f(y)$. Now extend f to G arbitrarily. Again, (1) holds. So it seems we've generalized so much that we have nothing interesting to say.

OK, so now let's try splitting the difference by only changing one of the universal quantifiers. But which quantifier do we change? We may as well just pick one and see what happens:

$$\forall x \exists y \; f(xy) = f(x)f(y). \tag{2}$$

But again, we see that this condition is too general to be of interest. I leave it to you to verify that a function $f\colon G \to H$ satisfies (2) above if and only if $f(e) = e$. Darn. Let's try the other option:

$$\exists x \forall y \; f(xy) = f(x)f(y).$$

Let us say that such an f is *homomorphic at x*. Have we finally uncovered something interesting? Before attempting to answer this, let's try to "feel out" this new definition. A natural starting point is to consider functions $f\colon G \to H$ which are homomorphic at e. Note that f is homomorphic at e if and only if $f(ey) = f(y) = f(e)f(y)$ for all $y \in G$ if and only if $f(e) = e$. Let's pause to record this observation.

$$f \text{ is homomorphic at } e \text{ if and only if } f(e) = e. \tag{3}$$

On one hand, it is mildly amusing that every function f which is homomorphic at e satisfies the familiar equation $f(e) = e$ (which holds for any homomorphism). On the other, *any* function $f\colon G \to H$ which satisfies $f(e) = e$ is homomorphic at e, so we haven't uncovered anything interesting just yet.

What do we do now? The canonical next step is to analyze functions which are homomorphic elsewhere. Thus, suppose that G and H are groups and $f\colon G \to H$ is a function which is homomorphic at g for some $g \in G$. The following (somewhat vague) open-ended question is now staring us directly in the face: what can we say about f?

We have now arrived at a make-or-break step in our investigation. You may ask, "What sorts of questions should we be asking about f?" I cannot overstate my response: *simple ones!* We already have a starting point. Recall from (3) that if f is homomorphic at e, then $f(e) = e$. Do we get the same conclusion if f is homomorphic at g for arbitrary $g \in G$? Let us check. If the answer is yes, then we are probably going to need to use e in our proof somewhere as well as the fact that f is homomorphic at g. So somewhere in our proof, we will probably need to see both "e" and "$f(g\cdot$ something)." Therefore, what is the natural choice for "something"? You guessed it... e! Now observe that $f(g) = f(ge) = f(g)f(e)$. So canceling $f(g)$, we see that $f(e) = e$. Combining this result with (3) above, we have the following:

$$\text{if } f \text{ is homomorphic at some } g \in G, \text{ then } f \text{ is homomorphic at } e. \tag{4}$$

Let's keep digging, using (4) as our guide. We have shown that if f is homomorphic at some $g \in G$, then f is homomorphic at e. Said another way, setting $K := \{g \in G\colon f \text{ is homomorphic at } g\}$: if K is nonempty, then $e \in K$. It is not hard to see that K may be empty. Indeed, if $f\colon G \to H$ and $f(e) \neq e$, then by (3) and (4), f is not homomorphic at any $g \in G$. But we have shown that if K is nonempty, then $e \in K$. What well-studied subsets of G have this property? Well, subgroups certainly do. So maybe if K is nonempty, then K is a subgroup of G. Let's see if this is true. Assume that f is homomorphic at a and at b. Then for any $g \in G$, $f((ab)g) = f(a(bg)) = f(a)f(bg) = f(a)(f(b)f(g)) = (f(a)f(b))f(g) = f(ab)f(g)$, and hence f is homomorphic at ab. It remains to check if f is homomorphic at a^{-1}. We want to see if $f(a^{-1}g) = f(a^{-1})f(g)$ for all $g \in G$. If this is true, we will probably need to use the fact that f is homomorphic at a. In this case, we expect to need to use f, a, a^{-1}, and g in our argument. As above, we may just string them together (strategically) and then see where we end up: $f(g) = f(aa^{-1}g) = f(a)f(a^{-1}g)$. Therefore, $f(a^{-1}g) = (f(a))^{-1}f(g)$. What we would like now is for $(f(a))^{-1} = f(a^{-1})$. This is clearly equivalent to $f(a)f(a^{-1}) = e$. Since f is homomorphic at a, this reduces to $f(aa^{-1}) = f(e) = e$. The final equation is true by (3) and (4). So we have shown that

$$\text{if } K \text{ is nonempty, then } K \text{ is a subgroup of } G. \tag{5}$$

OK, so now we have a result that is slightly less trivial than our previous observations. What can we use it for? Can we *specialize* this result to a "simple" (no pun intended) class of groups to obtain something interesting? Where do we start? Well, since every group is the union of its cyclic subgroups, there is a sense in which the cyclic groups form the building blocks of the class of all groups. Can you think of a nifty way to apply (5) to a cyclic group $G := \langle g \rangle$? Suppose that $f\colon G \to H$ is homomorphic at g. Then the set of all elements x of G for which f is homomorphic at x is a subgroup of G which contains g. Therefore,

$$\text{if } f\colon \langle g \rangle \to H \text{ is homomorphic at } g, \text{ then } f \text{ is a homomorphism.} \tag{6}$$

Where are we now? We seem to have uncovered an interesting property in (6) above. Let's translate (6) into a less formal statement: every cyclic group G has an element $g \in G$ (namely, a generator) for which every function $f\colon G \to H$ which is "locally homomorphic" at g is "globally homomorphic." Keeping with this theme, can you think of a canonical direction in which to continue our investigation? How about this:

Question. Which groups G possess the following property (P): there exists $g \in G$ such that every $f\colon G \to G$ which is homomorphic at g is a group homomorphism?

Note that we are now considering only functions f for which the domain and codomain coincide. The reason for this is that the question has a simpler logical structure than if we consider functions $f\colon G \to H$, and since we are exploring uncharted territory, we may as well make life easy on ourselves (are you keeping track of how many times I have used the word "simple"?).

We have shown that cyclic groups have property (P). Are these the only ones? Space restrictions preclude me from going into details, but let me say that you are going to get stuck if you try to prove that the answer is "yes" (you may want to try proving it now and see what difficulties you encounter). So let's look for noncyclic groups with property (P). We may as well start by checking the smallest non-cyclic group $H := \mathbb{Z}/\langle 2 \rangle \times \mathbb{Z}/\langle 2 \rangle$ (we now switch to additive notation). Let $a \in H \backslash \{0\}$ be arbitrary, and suppose $f\colon H \to H$ is homomorphic at a. We will verify that f is a homomorphism. First, choose any nonzero $b \neq a$. Now let $x, y \in H$ be arbitrary. We will prove that $f(x+y) = f(x) + f(y)$. If $x = y$, then $f(x+y) = f(x+x) = f(0) =$ (by (3) and (4)) $0 = f(x) + f(x) = f(x) + f(y)$. Assume now that $x \neq y$. If $x = 0$ or $y = 0$, then we are done since

$f(0) = 0$. If $x = a$ or $y = a$, then we are also done since f is homomorphic at a (and because the group operation is commutative). Finally, we may assume that x and y are distinct, nonzero, and different from a. The only pair of elements of H with this property are $a + b$ and b. Thus we may assume that $x = a + b$ and $y = b$. Then $f(x+y) = f(a) = f(a)+f(b)+f(b) = f(a+b)+f(b) = f(x)+f(y)$.

The plot has now thickened a bit. What would be *really* interesting is if $\mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$ turned out to be the only non-cyclic group with property (P). Of course, we hardly have enough data to confidently make such a conjecture. So let's take a moment to analyze the proof given above that $\mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$ has property (P). There are two properties of $\mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$ which played essential roles in our argument, namely,

(i) $\mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$ has 4 elements, and

(ii) every non-identity element of $\mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$ has order two.

Our goal is to figure out if there are any other non-cyclic groups which possess property (P). How might we proceed? Observe that if G is any *other* non-cyclic group with property (P), then G has at least six elements, so G cannot possess property (i). However, since property (ii) played an important role in our argument above, it is natural to wonder if the converse also holds. In other words, a canonical question is whether G non-cyclic with property (P) implies that every nonidentity element of G has order 2. Supposing for the moment that this is the case, how might we go about proving it?

Let G be a non-cyclic group with property (P) and let $a \in G$. We wish to prove that $a^2 = e$. Clearly, we may suppose that $a \neq e$. By definition of property (P), there exists some $g \in G$ such that every $f\colon G \to G$ which is homomorphic at g is a homomorphism. If we can construct a map $f\colon G \to G$ which is homomorphic at g and is such that $f(G) = \{e, a\}$, then since f is a homomorphism, $\{e, a\}$ would be a subgroup of G. But then $a^2 = e$, as desired. So now we turn our attention to constructing a map $f\colon G \to G$ which is homomorphic at g such that $f(G) = \{e, a\}$. We need $f(gx) = f(g)f(x)$ for all $x \in G$. To simplify matters (there's that word again!), we might try to find such an f with the property that $f(g) = e$. Then we need only check that

$$f(gx) = f(x) \text{ for all } x \in G. \tag{7}$$

If f is homomorphic at g and $f(g) = e$, then necessarily $f(g^m) = e$ for every integer m. Since we also want a to be in the range of f, the most natural definition to try is the following:

$$f(x) = \begin{cases} e & \text{if } x \in \langle g\rangle, \\ a & \text{otherwise.} \end{cases}$$

But does it work? Let $x \in G$ be arbitrary. Then note that $f(x) = e$ iff $x \in \langle g\rangle$ iff $gx \in \langle g\rangle$ iff $f(gx) = e$. Because the codomain of f contains exactly two elements, it is clear that $f(gx) = f(x)$ for all $x \in G$, and hence f satisfies (7).

Since G is not cyclic, there is some $x \in G \backslash \langle g \rangle$. Thus $f(G) = \{e, a\}$, as required. Again, let's pause to take stock of what we have.

$$\text{A non-cyclic group } G \text{ with property (P) satisfies } x^2 = e \text{ for all } x \in G. \qquad (8)$$

Recall that the task at hand is to figure out whether there are any non-cyclic groups aside from $\mathbb{Z}/\langle 2 \rangle \times \mathbb{Z}/\langle 2 \rangle$ which have property (P). Maybe at this stage, you don't know what the answer is; possibly you don't even have a gut instinct about what the answer is. So what to do? A strategy (not necessarily the *only* reasonable strategy) is the following: simply pick "yes" or "no" and try to prove it. If you are successful, then you're done. If not, analyze what the roadblock is and then reassess your assertion. Recall the properties (i) and (ii) of $\mathbb{Z}/\langle 2 \rangle \times \mathbb{Z}/\langle 2 \rangle$ which played an integral role in showing that $\mathbb{Z}/\langle 2 \rangle \times \mathbb{Z}/\langle 2 \rangle$ has property (P). Property (i) was that $\mathbb{Z}/\langle 2 \rangle \times \mathbb{Z}/\langle 2 \rangle$ has 4 elements. Since every non-cyclic group not isomorphic to $\mathbb{Z}/\langle 2 \rangle \times \mathbb{Z}/\langle 2 \rangle$ has more than 4 elements, one could argue that our best guess at this juncture is that $\mathbb{Z}/\langle 2 \rangle \times \mathbb{Z}/\langle 2 \rangle$ is the only non-cyclic group with property (P) (let me stress that this is still just a *guess* based on almost no information). For now, let's assume this is the case and see what we can uncover.

So let us suppose that H is a non-cyclic group with property (P) not isomorphic to $\mathbb{Z}/\langle 2 \rangle \times \mathbb{Z}/\langle 2 \rangle$ and see if we can find a contradiction. By definition, there is some $h \in H$ such that every $f \colon H \to H$ which is homomorphic at h is a homomorphism. Our proof of (8) entailed constructing a function with range of size two. Can we modify this construction to obtain a contradiction? Note that if we can show that there is function $f \colon H \to H$, homomorphic at h with range of size three, then we certainly could obtain a contradiction: the range would be a subgroup of H of size three. But then the range would contain an element of order three, contradicting (8). Following the strategy used in establishing (7), let us see if we can find such an f with $f(h) = 0$ (again, we use additive notation; by (8) above, H is abelian). Then as before, we need only check that $f(h + x) = f(x)$ for all $x \in H$.

To summarize, here is what we want to do:

Strategy. Find a function $f \colon H \to H$ which satisfies the following conditions:

1. $f(h) = 0$,
2. $f(h + x) = f(x)$ for all $x \in H$, and
3. the range of f has cardinality three.

Is this an onerous task? Well, (1) is easy: we simply define $f(h) = 0$. As for (2), suppose $x \in H$ and we have defined f such that $f(h + x) = f(x)$. Now suppose $y \in H$ and we want to define $f(y)$ and $f(h + y)$ so that $f(h + y) = f(y)$. The issue is that if y (respectively, $h + y$) happens to be a member of $\{h + x, x\}$, then $f(y)$ (respectively, $f(h + y)$) is *forced* on us. This makes the task of defining f

a bit more challenging. But observe that this issue goes away if $\{h+x, x\}$ and $\{h+y, y\}$ are either equal or disjoint. Hence we ask: if $x, y \in H$ are such that $\{h+x, x\}$ and $\{h+y, y\}$ are not disjoint, then does $\{h+x, x\} = \{h+y, y\}$? Note that if $x = y$ or $h+x = h+y$, then it is easy to see that equality holds. Therefore, we may assume without loss of generality that $h+x = y$. Adding h to both sides and using the fact that $h+h = 0$, we obtain $x = h+y$. Then again, the two sets coincide. Let us pause to record this fact.

$$\mathcal{P} := \{\{h+x, x\} \colon x \in H\} \text{ is a partition of } H. \tag{9}$$

Next, observe that $\{0, h\}$ is a member of the partition above. Now pick partition sets $\{h+x, x\}$ and $\{h+y, y\}$ so that all three partition sets $\{0, h\}$, $\{h+x, x\}$, and $\{h+y, y\}$ are distinct (observe that this is possible since H, being noncyclic and not isomorphic to $\mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$, has at least six elements). Finally, choose distinct nonzero elements $a, b \in H$. Map the set $\{0, h\}$ to 0 (that is, map 0 and h to 0), then map $\{h+x, x\}$ to a and $\{h+y, y\}$ to b. Lastly, extend the map to the entire set of partitions arbitrarily, subject to the restriction that each partition set be mapped to either 0, a, or b. We now have a map f which satisfies items 1.–3. Success!

3 Now What?

Here is a synopsis of the mathematical results of the previous section: let G be a group. Then there exists some $g \in G$ such that every map $f\colon G \to G$ which is (locally) homomorphic at g is a (global) homomorphism if and only if G is cyclic or $G \cong \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$. Where do we go from here? Clearly this result does not qualify as a research paper, so that option is out. But there are two directions in which we may proceed. The first is to pose the following problem (with solution) and submit it for publication in a mathematical periodical with a problem section (*Math Magazine*, *The College Math Journal*, *The Monthly*, *Pi Mu Epsilon*, etc.). Here is one way to phrase the problem:

Problem. Let G be a group, and let $g \in G$. Say that a function $f\colon G \to G$ is *homomorphic at* g provided $f(gx) = f(g)f(x)$ for all $x \in G$. Find all groups G with the following property: there exists some $g \in G$ such that if $f\colon G \to G$ is any function which is homomorphic at g, then f is a homomorphism.

As our work demonstrates, the problem is accessible in that it does not require any deep theorems of group theory to solve. Second, it is enticing in the following sense: it is fairly easy to make initial progress on the problem as it is not too difficult to see that cyclic groups satisfy the above condition. However, it is much less obvious that there is exactly one noncyclic group with this property. Given the length of this paper, it may be difficult to assess how much space a concise solution would take up. One can give it in less than a page. Combining all of these attributes makes the problem a strong candidate for publication.

Now, one might be curious if the above problem is new. Given that there are so many venues in which recreational problems appear (periodicals, journals, textbooks, etc.), it is quite difficult to know for sure if a given problem proposal is new. That said, I have published over 40 problems myself, and only once did a referee find my proposed problem in the literature. So this may not be as big of a barrier to publication as you might anticipate.

Next, you may wonder, "Why would I care to publish such a problem?" The answer depends on your lot in life. If you are on the Princeton faculty, it is not likely that a problem posed in The Monthly will count for much when you come up for promotion (though it is interesting that John Conway lists one of the problems he posed in *The Monthly* on his c.v.; this can be found online at `http : //web.math.princeton.edu/WebCV/ConwayBIB.pdf`, item 138). On the other hand, if you are an undergraduate applying to graduate schools, having a published problem under your belt is evidence of mathematical imagination; it may help you be more competitive when applying to graduate programs. For faculty, there are many institutions in which such a publication counts as scholarship; Kenyon College is such an example (I thank Associate Provost Brad Hartlaub for confirming this assertion).

Last but not least, let me remark that the fun isn't over yet! We haven't quite squeezed all the juice out of the problem presented in this paper. As a sequel, I cordially invite you to try your hand at Problem #??? in this issue of Pi Mu Epsilon Journal.

References

[1] P. Etingof, http://web.mit.edu/primes/succeed.shtml (2017).

[2] R. Hamming, http://www.csee.umbc.edu/~finin/YouAndYourResearch.html (2016) (transcription of the Bell Communications Research Colloquium Seminar, March 7, 1986).

[3] R. Hersh, *How to do and write math research*, Math. Intelligencer **19** (1997), no. 2, 58–60.

[4] http://mathoverflow.net/questions/451/advice-on-doing-mathematical-research (2017).

[5] S. Krantz, *How to write your first paper*, Notices Amer. Math. Soc. **54** (2007), no. 11, 1507–1511.

[6] E. Lady, http://www.math.hawaii.edu/~lee/how-to.html (2017).

[7] G. Polya, *How to solve it. A new aspect of mathematical method.* Expanded version of the 1988 edition, with a new foreword by John H. Conway. Princeton Science Library. Princeton University Press, Princeton, NJ, 2004.

[8] T. Tao, http://terrytao.wordpress.com/career-advice/does-one-have-to-be-a-genius-to-do-maths/ (2017).

About the author

Greg Oman is an assistant professor at UCCS. He works primarily in algebra and logic. One of the most enjoyable aspects of his job, however, is posing recreational problems in various mathematical periodicals.

Greg Oman

University of Colorado, Colorado Springs
1420 Austin Bluffs Parkway
Colorado Springs, CO 80918
goman@uccs.edu