An Ideal Functional Equation with a Ring

Zoran Šunić

Department of Mathematics
Texas A&M University
College Station, TX 77843-3368
sunik@math.tamu.edu

Submitted: January 2002; Accepted: July, 2003
MR Subject Classifications: 13G05
Keywords: integral domain, ideal, subring, functional equation

There are many examples in mathematics and other sciences in which a single equation (or a relatively small system of equations) is capable of capturing the essence and complexity of an entire field. For example, the equation defining the zeros of the Riemann zeta function plays a central role in analytic number theory and related fields. Even a partial understanding of the solutions to this equation would provide keys to the answers to many far-reaching questions that are currently in the research focus of the mathematical community. In a somewhat opposite direction, several outstanding results from the theory of elliptic curves and modular forms, crowning the efforts of several generations of mathematicians, were needed to tackle the single equation that is the subject of Fermat's Last Theorem. While the equation we present in this note does not live up to the high standards set by these two examples, it still has the same flavor in the sense that it touches on some very subtle questions and provides unexpected connections.

The ideal functional equation we refer to in the title and solve in the sequel is given by

$$f(xz-y)f(x)f(y) + 3f(0) = 1 + 2f(0)f(0) + f(x)f(y). \tag{1}$$

As it is, the equation looks far from ideal and its ring cannot be detected. In addition, it is not clear what it means to solve the given equation, so let us provide some context.

For example, we may solve the ideal equation over $\mathbb{R}$, which means that we need to find all functions $f : \mathbb{R} \to \mathbb{R}$ such that (1) is satisfied for all x, y and z in $\mathbb{R}$.

Note that the ideal equation is equivalent to the following system of equations

$$f(xz-y)f(x)f(y) = f(x)f(y), \tag{2}$$

$$f(0) = 1. \tag{3}$$

Indeed, it is obvious that (2) and (3) together imply the ideal equation. On the other hand, setting $x = y = z = 0$ in the ideal equation yields $(f(0) - 1)^3 = 0$, which implies

$f(0) = 1$. Once we know that $f(0) = 1$ the equation (2) easily follows from the ideal equation.

Now we try to solve the system. Let f be a function that satisfies the equations (2) and (3).

Setting $z = 1$ and $y = 0$ in (2) yields $f(x)f(x) = f(x)$. Thus, for all x, $f(x) = 1$ or $f(x) = 0$. Let $S = \{x | f(x) = 1\}$. The function f is therefore given by

$$f(x) = \begin{cases} 1, & \text{if } x \in S \\ 0, & \text{if } x \notin S \end{cases}, \tag{4}$$

i.e., f is the characteristic function of the set S. However, not any set S would do. First, we know that $f(0) = 1$, which means 0 must be in S. Further, set $z = 1$ in (2). This gives

$$f(x - y)f(x)f(y) = f(x)f(y),$$

which implies that if both x and y are in S then so must be $x - y$. Now set $y = 0$ in (2). This gives

$$f(xz)f(x) = f(x)$$

and therefore if x is in S then so must be xz, for any z. Thus, S has the following three properties:

$$\begin{aligned} 0 &\in S, \\ x, y \in S \quad \text{implies} \quad x - y &\in S, \\ x \in S \quad \text{implies} \quad xz &\in S, \quad \text{for all } z. \end{aligned} \tag{5}$$

It is easy to see that the only two subsets S of $\mathbb{R}$ that satisfy the three conditions in (5) are $\mathbb{R}$ itself and $\{0\}$. The characteristic functions, given by (4), of either $S = \mathbb{R}$ or $S = \{0\}$ satisfy the system and therefore also our ideal equation (1).

As we see, the solutions of our ideal equation over $\mathbb{R}$ are not particularly exciting. In order to get spicier solutions we consider the ideal equation over the integers $\mathbb{Z}$. To be precise, this means that we need to find all functions $f : \mathbb{Z} \to \mathbb{Z}$ that satisfy the equation (1) for all x, y and z in $\mathbb{Z}$. For example, in addition to the characteristic functions of $\mathbb{Z}$ and $\{0\}$, the characteristic function of the set of even numbers

$$f(x) = \begin{cases} 1, & \text{if } x \text{ is even} \\ 0, & \text{if } x \text{ is odd} \end{cases}$$

satisfies the ideal equation. Indeed, if at least one of x or y is not even then both sides of (1) are equal to 3. If both x and y are even then both sides of (1) are equal to 4. Similarly, we can check that any set $S = n\mathbb{Z} = \{nm | m \in \mathbb{Z}\}$ that consists of all multiples of a fixed integer n has a characteristic function that satisfies the ideal equation. In fact, by following the exact same steps as we did above for $\mathbb{R}$, we conclude that any solution to the ideal equation over $\mathbb{Z}$ must be the characteristic function of a subset S that satisfies the three conditions in (5). A subset of $\mathbb{Z}$ satisfies these conditions exactly when it consists of all multiples of a fixed integer n, i.e., it is equal to $n\mathbb{Z}$, for some integer n.

The discussion we had up to now should "ring" a bell already. The conditions in (5) that describe the sets S providing the characteristic functions (4) that satisfy our "ideal" equation (1) are actually the conditions that define the notion of an ideal in a ring (for a definition of a ring and ideal see, for example, [**1**, p. 194, p. 216]). It is easy to check that the relevant parts of the discussion above remain valid for arbitrary integral domains [**1**, p. 200]. Thus, we make the following conclusion.

Conclusion. A function $f : D \to D$ is a solution to the ideal equation (1) over an integral domain D exactly when it is the characteristic function, given by (4), of an ideal S of D.

The ideal structure in integral domains is very important and difficult question that lies in the heart of several mathematical areas such as commutative algebra and algebraic geometry. It is quite interesting that we could capture all ideals in a single functional equation.

A few further modestly illuminating comments are in order.

We see now the reason why our ideal equation does not have particularly exciting solutions over $\mathbb{R}$. The reason is that $\mathbb{R}$ is a field [**1**, p. 204] and every field has only two ideals, namely the field itself and the zero ideal $\{0\}$.

If instead of the ideal equation we consider the more aesthetically appealing equation (2) alone, we note that the its only solutions over an integral domain D are the characteristic functions of the ideals of D and the constant zero function. The fact that the zero function is a solution to (2) could be thought of as a nuisance, since this function is the characteristic function of the empty set, which is not an ideal of D. This is precisely why our ideal equation (1) had to be slightly more messy and include the part that served as a filter for the zero function.

Next, we note that we can use a similar functional equation to describe, say, the subrings [**1**, p. 196] of an integral domain D. One such equation is

$$f(x-y)f(xy)f(x) + 3f(0) = 1 + 2f(0)f(0) + f(x)f(y).$$

Once again, the messy part of the equation just serves to filter out the zero function and the interesting part is the equation

$$f(x-y)f(xy)f(x) = f(x)f(y),$$

which is satisfied by the characteristic functions of the subrings of the integral domain D as well as by the zero function.

If we do not insist on having a single equation describing the type of subsets we are interested in, and quite often there is no reason to do so, we can easily push our idea(l)s further. For example, the only solutions to the system of equations

$$\begin{aligned} f(0) &= 1, \\ f(1) &= 0, \\ f(x-y)f(x)f(y) &= f(x)f(y), \\ 1 - f(xy) &= (1-f(x))(1-f(y)), \end{aligned}$$

over an integral domain D are the characteristic functions of the prime ideals of D [**1**, p. 200]. We recall that a prime ideal S in a ring R is an ideal, different from R, that satisfies the condition

$$xy \in S \quad \text{implies} \quad x \in S \text{ or } y \in S.$$

In case, for aesthetic or some deeper reasons, we do insist on a single functional equation we may try the following. Assume that D is an integral domain for which there exists a polynomial $p(x_1, x_2)$ with coefficients in D such that

$$p(x_1, x_2) = 0 \quad \text{if and only if} \quad x_1 = x_2 = 0. \tag{6}$$

Then

$$\begin{aligned} p(x_1, p(x_2, x_3)) = 0 &\quad \text{if and only if} \quad x_1 = x_2 = x_3 = 0, \\ p(x_1, p(x_2, p(x_3, x_4))) = 0 &\quad \text{if and only if} \quad x_1 = x_2 = x_3 = x_4 = 0, \end{aligned}$$

and so on. Thus we can rewrite any system of n equations over D as a single equation over D. For example, the system

$$\begin{aligned} f_1 &= 0, \\ f_2 &= 0, \\ f_3 &= 0, \end{aligned}$$

could be rewritten as the single equation

$$p(f_1, p(f_2, f_3)) = 0.$$

A polynomial $p(x_1, x_2)$ with the property (6) exists in many cases. A precise description of all such cases would lead us considerably deeper in the subject than we are willing to go at this moment. As an easy example, we note that such a polynomial over $\mathbb{Z}$ is $p(x_1, x_2) = x_1^2 + x_2^2$. Thus, we may write a single functional equation that describes all prime ideals of $\mathbb{Z}$. Since the prime ideals of $\mathbb{Z}$ are the zero ideal $\{0\}$ and the ideals of the form $p\mathbb{Z} = \{pm | m \in \mathbb{Z}\}$, for p a prime number, such a functional equation, rather implicitly, describes the prime numbers. With the last observation, we just made a quick peek into number theory.

Finally, we conclude our little interplay of ring theory, functional equations and logic with an invitation to try and find functional equations leading to other types of subsets in integral domains and, more generally, to various substructures in other algebraic settings.

A particularly easy example is the case of Boolean algebras [**1**, p. 511]. If B is a Boolean algebra, the only functions $f : B \to B$ that satisfy the equation

$$f(0) \;\wedge\; [f(x) \Rightarrow f(\bar{x})] \;\wedge\; [(f(x) \wedge f(y)) \Rightarrow f(x \wedge y)] \;=\; 1, \tag{7}$$

for all x and y in B, are exactly the characteristic functions of the boolean subalgebras of B (an expression of the form $A \Rightarrow B$ used in (7) is just a shorthand for $\bar{A} \vee B$).

References

1. Aigli Papantonopoulou, *Algebra, Pure and Applied*, Prentice Hall, New Jersey, 2002, xx+550.