M. Ram Murty

Department of Mathematics
Queen’s University, Kingston, Canada
murty@mast.queensu.ca

Trip to the Proof

How I discovered Euclidean proofs

Mathematicians carefully communicate the how of their results, but they hardly ever go into the why. In this new column ‘Trip to the Proof’ mathematicians describe the discovery process without going into the details of the proof. The first contribution is by Ram Murty, who holds a research chair in mathematics as well as an appointment in philosophy at Queen’s University, Canada.

It was the summer of 1975 when I was entering the final year of my undergraduate studies at Carleton University in Ottawa, Canada, that I wandered into the library in search of a topic to research for my Bachelor's thesis. Browsing through some old volumes of the American Mathematical Monthly, I chanced upon an interesting article written by Bateman and Low showing that there are infinitely many primes in every coprime arithmetic progression (mod 24) using only basic properties of polynomials and nothing deeper than the law of quadratic reciprocity. Of course, Dirichlet had proved in a series of papers written between 1837 and 1840 that there are infinitely many primes in any coprime arithmetic progression using analytic and arithmetic methods including his deep class number formula. By contrast, the Bateman and Low paper [1] followed the line of attack initiated by Euclid in 300 BCE and they seemed to suggest at the end of the paper that such ‘Euclidean proofs’ exist only when the residue class has order 1 or 2. I was intrigued by this and wrote to Professor Bateman to ask how one would prove such a statement. He responded by saying that he had no formal proof but that all the examples known satisfied this criterion. So I took this up for my Bachelor's thesis and tried to make the problem precise.

All of us are familiar with Euclid’s elementary proof of the infinitude of primes. It proceeds by contradiction. Assume that there are only finitely many, say $p_1, \ldots, p_r$. Then the number $P = p_1 \cdots p_r + 1$ is a number coprime to all of the primes $p_1, \ldots, p_r$. At the same time it is larger than 1 and so must be divisible by a prime which is not in our list, which is a contradiction. Many excellent books on elementary number theory often extend this argument to show infinitude of primes congruent to 1 or 3 (mod 4). For example, if there are only finitely many primes congruent to 3 (mod 4), say $p_1, \ldots, p_r$, then consider $P = 4p_1 \cdots p_r - 1$. This number being odd and being coprime to $p_1, \ldots, p_r$ must have prime divisors either congruent to 1 or 3 (mod 4). But not all its prime divisors can be 1 (mod 4) for otherwise, the number itself would be 1 (mod 4), which it is not. So it must have a prime divisor congruent to 3 (mod 4) not in our list. This contradiction shows there are infinitely many primes congruent to 3 (mod 4).

A small variation in this argument can show the infinitude of primes congruent to 1 (mod 4). Indeed, as before suppose there are only finitely many, say $p_1, \ldots, p_r$. Consider $N = 4(p_1 \cdots p_r)^2 + 1$ which is coprime to all of the primes $p_1, \ldots, p_r$. If $p$ is any prime divisor of $N$, then $p$ is different from $p_1, \ldots, p_r$ and $-1$ is a quadratic residue (mod p). But only primes congruent to 1 (mod 4) have $-1$ as a quadratic residue so that $p \equiv 1$ (mod 4).

Both of these proofs are in the spirit of Euclid and so my question was how far one could push this argument and give a ‘Euclidean proof’ of Dirichlet’s theorem. I was 22 years old at that time and I can vividly recall the great delight I felt when...
I asked the question. Bateman’s reply to my letter only encouraged me to make my question as precise as possible and to answer it the best I could. I believe that there are already several important features of the research experience evident in this narration. As I have taught my students in later years, research is really the art of asking ‘good questions’. What is a ‘good question’? This is difficult to define. However, the question should not be too easy or too difficult, but must be just right so as to stimulate some progress in the direction of the answer. Fortunately, this problem was just right and it took me to the frontiers of modern research.

There are other aspects of research that are underlined by my story. Browsing plays an important part in research. In my case, browsing old journals in the library was an exciting experience and I stumbled upon an article that I could dive deeper into. Moreover, there was some literature already in place that I could consult for a hint of how to proceed. For instance, Bateman seemed to imply that all the proofs known to him suggested such a proof can only be given if the residue class had order 1 or 2 but could not give a proof of this assertion.

In his paper, there was a reference to a 1912 paper of Schur [5] that showed using cyclotomic polynomials that if $k$ is a natural number and $a$ (mod $k$) is a residue class such that $a^2 \equiv 1$ (mod $k$), then one can construct a polynomial $f(x)$ with integer coefficients such that any prime divisor $p$ of $f(n)$ is congruent to either 1 or $a$ (mod $k$). Schur’s paper was written in German and was about ten pages long. Though I had a year long course in German in high school, I was not fluent in it. However, the paper was sufficiently short that I could sit with a dictionary and translate it well enough to reproduce Schur’s proof in my own words and make it the first chapter of my Bachelor’s thesis.

To give some idea to the reader of Schur’s argument, it may be instructive to proceed. For instance, Bateman seemed to say that he could not give a proof of this assertion. He did and finally published the generalization in a more accessible journal [4].

Perhaps the last chapter of this story is instructive. Often, we do not know the value of our own work. Without proper guidance, we may downplay the significance of our contribution. As advice to a young scientist, all I can say is that we should thoroughly investigate as best as we can and then publish our results, however modest they may be. This is the way science advances, not by giant leaps, but through small steps taken by many, many diligent people.

Acknowledgements
I thank Kumar Murty and Akshaa Vatwani for their helpful comments on an earlier version of this article.

References
1. P. Bateman and M. E. Low, Prime numbers in arithmetic progressions with difference 24, American Math. Monthly, 72 (1965), 139-143.