A METHOD TO TEACH NUMBER THEORY USING A COMPUTER

Chris K. Caldwell

1. Introduction

Much of elementary number theory was discovered through computation, yet computation and discovery are almost nonexistent in the traditional number theory course. As a result this course often becomes stale and theoretical.

To allow discovery in our number theory course we have used muMATH by SoftwareHouse (augmented with our own number theoretical routines) as an unlimited precision calculator, making otherwise tedious computations trivial. Using carefully selected homework assignments, the students were led by to discover number theory for themselves. In class we developed *the student's* results and laid the groundwork for *their* future discoveries.

The homework problems not only set the pace of the course, but were chosen to teach the students how to experiment and conjecture. By using a text only as a reference we avoided the student's usual proof algorithm: (1) reread the techniques in the section containing the problem, (2) apply only those techniques.

In this paper we give examples of the homework problems and explain the philosophy behind their choice. We end with a brief discussion of the program and the text.

2. The Homework

To emphasize discovery, homework problems were chosen to be open ended. To make student discoveries central to the course, the lectures usually centered on the previous night's homework. Lectures also introduced definitions and concepts necessary for following problem sets. Consider the following homework problems:

1. Choose several primes p. For each evaluate (p-1)! modulo p. Make a conjecture. Prove your conjecture.

2. Choose a prime p and an integer a. Evaluate a^{p-1} modulo p. Repeat with several different a's and p's, be sure to try a = 0. Make a conjecture. Prove your conjecture.

While doing these problems the student quickly conjectures Wilson's theorem and Fermat's little theorem respectively, though they can not yet prove them. The proofs are given the next class day. Because we were proving results the student had discovered herself, the student was more interested, and remembered the results longer.

In real life we rarely know ahead of time if we can prove our conjectures, though we often have a gut feeling. To help develop this instinct in our students we did not indicate if they could succeed in their assigned proofs. The following problem, for example, leads to the unproven Goldbach's conjecture.

3. Choose any even integer larger than two. Can it be written as the sum of two primes? Make a conjecture. Prove your conjecture.

In the class meeting following this problem, we would discuss the progress that has been made towards a proof. More importantly, we would discuss why this result is harder to prove than the previous results.

Very little of undergraduate mathematics was done this century, so students rarely encounter unsolved problems. Number theory is an ideal place to correct this shortcoming. Here is one example:

4. Let F(n) = 3n+1 if n is odd, n/2 if n is even. Starting with any positive integer iterate this function until you reach one. For example starting with 13 we get the following sequence of numbers 13,40,20,10,5,16,8,4,2,1. Prove or disprove that the sequence always terminates (always reaches one).

(The function F is included as part of our computer software.) Shank's book [8] is an excellent source for this type of problem.

In the above examples the student could not have completed the proof herself. To avoid the danger that the student would not even try to prove her results, many of the problems had trivial proofs:

5. Take any three digit number and write it down twice. For example, 451 becomes 451451. Divide the resulting six digit number by 77. Make a conjecture. Prove your conjecture.

(Note abcabc = abc·1001 = abc·77·13.) It is surprising how many students can not tell whether proving a result will be easy or difficult. Hopefully students develop the necessary intuition as they see both easy and difficult problems side by side.

Two more pitfalls to avoid are the law of small numbers [5], and the student's desire to do only the minimum work required. We attack these problem with the following.

6. For n = 1,2,...,20 factor n^2+n+41. Make a conjecture. Prove your conjecture.

7. Use PRIMETEST to test the primality of the following numbers: 31, 331, 3331, 33331, 333331, 3333331. Make a conjecture. Prove your conjecture.

(PRIMETEST is part of our computer package.) Here the suggested numbers are all prime, so many students fell into the trap and conjectured that the results are always prime. Only about one half of the students looked look at unlisted terms in the second sequence. 33333331 is prime, but 17 divides 333333331.

Problems six and seven could be used to lead into a classroom discussion about Fermat and Mersenne primes, or about formulas for the n-th prime, or functions which take on only prime values... The student should be shown that there are vast unexplored frontiers.

We close this section with a follow up to problems six and seven.

8. We have seen several sequences whose first few terms are prime. Construct an interesting sequence of your own which begins with at least five primes.

This problem exemplifies our goals: it requires student discovery, it is open ended, and it can be used to lead into many classroom discussions.

3. The Program

All of the examples above are computationally intensive. Few students enjoy calculating 13^{72} modulo 73 by hand, or factoring $20^2+20+41$ by hand. So the computer was introduced as a calculator, making the calculation trivial - but leaving the student to interpret the results. We used muMATH by SoftwareHouse because it was cheap and ran on the IBM-PCs we had available. Any software package that had unlimited precision rational arithmetic could have been used. To this package we added the basic functions of number theory (phi, sigma, Jacobi symbol,...) along with routines to factor numbers (Pollard's rho and p-1 methods, ... [see references 2 and 7]). We also included the primality proving theorems of [1].

The computer was used as a discovery tool only, it was not the object of study and few students bothered to even list the subroutines. Less than fifteen minutes was necessary for most students to begin using the program. Many students enjoyed having the machine factor their phone numbers, social security numbers, even their names (viewed as integers base 36). The program greatly encouraged mathematical play.

As an example of the surprising power of this little system, consider the numbers in problem seven, $a_n = (10^n-7)/3$. It was known that these are prime for n =1,2,3,4,5,6, 7,17,39,49,59,77 and 100. Using the muMATH routines (and factorizations from [2]) we proved the primality of two of the next three probable-primes: a_{150} and a_{381}. Harvey Dubner showed a_{318} is prime.

4. The Text and Students

This course could have been taught without a text, or with a text like Shank's book [8], however, we chose to use a traditional text as a reference (Burton[3]). Next time we will probably use Eyden [4] or Rosen [6] because of their treatment of primality testing and RSA codes. Whatever text is chosen, do not follow it closely. Otherwise the students will look up the results rather than discover the results. Not all students thrived under these conditions (a few were frightened by the problems sets and dropped the course immediately), but most students did very well, and a few even learned to love

number theory. The students' confidence increased. Many made mathematical discoveries for the first time in their lives. Several now regularly use the computer as a tool in mathematics.

Our small school has two number theorists and a biannual number theory course. So I have only been able to teach number theory once. I will definitely use this approach again.

REFERENCES

1. John Brillhart, D. H. Lehmer and J. L. Selfridge, "New Primality Criteria and Factorizations of $2^m \pm 1$", Math. Comp. 29 (1975), 620-647.
2. Brillhart, Lehmer, Selfridge, Tuckerman, Wagstaff, Factorization of $b^n \pm 1$, $b = 2,3,5,6,7,10,11,12$ Up To High Powers, Contemporary Mathematics 22, American Mathematical Society, 1988.
3. David Burton, Elementary Number Theory, Allyn and Bacon, 1975.
4. Charles Eyden, Elementary Number Theory, Random House, 1987.
5. Richard Guy, "The Strong Law of Small Numbers," Amer Math Monthly, 95 #8 (1988), 697-711.
6. Kenneth H. Rosen, Elementary Number Theory, 2ed, Addison-Wesley, 1988.
7. Hans Reisel, Prime Numbers and Computer Methods for Factorization, Birkhauser, 1985.
8. Daniel Shanks, Solved and Unsolved Problems in Number Theory, Chelsea, New York, 1978.

Department of Mathematics and Computer Science
University of Tennessee at Martin
Martin, TN 38238