MATH 175: 
INQUIRY-BASED INTRODUCTION TO CRYPTOLOGY

T. KYLE PETERSEN

"That student is taught the best who is told the least."
– R. L. Moore

1. Introduction

1.1. About the method. If you’re reading this, you’re probably a good teacher. (At the very least, you have a non-vanishing interest in teaching.) Did you ever have the sneaking suspicion that your students, even the “good” ones, who get the best grades on exams, don’t really know the material you’ve been trying to teach them? What percentage of your last calculus class would you say could recite that $\frac{d}{dx}[x^n] = nx^{n-1}$? What percentage could tell you why? My answers to these questions would be about 99 and about 15, respectively. If your numbers are higher, congratulations, but I’d wager anyone with an answer of more than 25 to the second question is an outlier.

Most students are led to believe mathematics consists of memorization of facts and simple algorithmic exercises. Inquiry-based learning (IBL, or the “modified Moore method”, after R. L. Moore) seeks to counteract this tendency. The pitfalls of the shallow view include the inability to assess the correctness of a written solution, the belief that there is one “right way” to solve a problem, and the idea that all problems can be addressed in just a few minutes. With an inquiry-based approach, students learn that many worthwhile questions have answers that can take hours, or even days (weeks!) to conquer, they see that a solution can often come from several different directions, and they develop a sharp eye for logical flaws in an argument. In short, IBL tries to makes students think like mathematicians. Once students have traced on their own all the steps and missteps leading to the claim $\frac{d}{dx}[x^n] = nx^{n-1}$, they understand the statement in a way that is simply not possible from memorization alone. The need for memorization of further facts falls by the wayside as students realize that so many

1And there are lots of steps! What is a limit? What is a derivative? The definitions of a function and of continuity probably also crop up...
ideas follow from true knowledge of the rules of the game and how to apply them.

But how do we get students to reach this point? R. L. Moore adopted a Socratic approach. There is no textbook, but rather the instructor gives students a list of problems and some statements of definitions and theorems, but with no exposition and no proofs. The course consists of students doing the problems and attempting to prove the theorems. During class meetings students present their findings at the board while the other students ask questions. The instructor largely lurks in the background, acting as moderator and cheerleader, but rarely, if ever, as judge. There are many variations on the theme, almost a spectrum, from “hard-core Moore”\(^2\) on one extreme to, at the other extreme, something much closer to a typical lecture-style course, with written homework, exams, and even textbooks. The specific structure of Math 175 is discussed in the next section.

There are several possible reasons why more courses are not taught in the IBL style. One reason is that this method requires different skills than lecturing does, and it can be easy for things to go very wrong—more about this in the “Difficulties and Advice” section. Even when done properly some still criticize the method; the main reason given is lack of coverage. It does seem to be generally true that the list of topics students see in a one-semester IBL course is shorter than the same list for a course taught in the lecture style. One counter-argument I have heard is that the learning curve for IBL students is exponential, whereas the curve for lecture style students is linear. So while after one semester the lecture class may be ahead, by the end of two semesters the IBL class will have overtaken them.

I prefer the following analogy. The main theorems and definitions from a course are like flowers. In a lecture course students pluck the flowers one by one and put them in a pretty vase to admire. In an IBL class, the students get down in the dirt to plant seeds, water them, and watch the flowers grow. A year later, the flowers in the vase will have wilted and died. With a little care, though, the IBL students will still have a flower garden.

1.2. About this document. My aim with this note is to give an idea of how this course has been run for the past couple of years, along with some general advice about my version of the IBL method. It is not an instruction manual. It is not a detailed syllabus. While it contains

\(^2\)One rumor—almost surely false—is that he once brought a revolver to class as extra motivation for a particularly recalcitrant group of students: “Today someone will prove Theorem X.”
information about the the structure of the course and the running of day-to-day operations, you will find little here that is specific to number theory or cryptography. (You can find that in the worksheets.) Difficulties in teaching this course are more likely to come from unfamiliarity with the method than from content.

For me, there is something paradoxical about trying to teach someone how to teach a course in which the guiding principle is that students teach themselves. Shouldn’t I just wish you luck and let you go figure it out for yourself? Maybe. But maybe you can learn something from my experience and opinions as well. (Really, the best thing I can recommend for someone interested in teaching an IBL course is to attend a workshop, or to sit in on a class taught by an experienced IBLer.) My point is that whatever I say, you need to make the material your own before you put it into practice. To be sure, I hope that the advice in this note saves you headaches and wasted time, but your own experiments and mistakes will teach you better than I ever could, and ultimately will make you a better teacher.

Good Luck!

2. History and Structure of Math 175

Math 175 was originally conceived by Phil Hanlon in the late 1980s as a “problems course” for honors freshmen. He gave students a list of fifty or so problems, usually discrete, but with no obvious unifying theme. He would lecture on various topics, and every few days a student would present a solution to a problem from the list. Grades were based purely on the number of solutions presented. This was classic Moore method.

While some students relished the open-ended nature of the course, many of their classmates disliked the fact there was no specific content for the course. With this in mind, Hanlon tried to tie the problems to some specific content. First he tried graph theory, then cryptology, which stuck. Prodded by student interest, he and several collaborators later developed an entire “coursepack” with some historical motivation and exposition on cryptographic methods and related mathematical topics.

Hanlon taught the course each year through the late 1990s and intermittently thereafter. (He took a job in the Provost’s office.) From 1999–2005 several people taught the course, in several different formats. At one point a hardcover textbook, *Invitation to Cryptology,* was added to the required course materials. In general, the course lost almost all connection to the Moore method.
When I was hired in 2006, it was with the understanding that I would help revive the IBL character of Math 175. In the fall of that year, Kirsten Eisenträger and I designed and co-taught the course. We still had the textbook and coursepack that fall, but in 2007 and 2008 those materials were dropped in favor of the materials contained in this folder. Otherwise, the structure, grading procedures, and content is largely unchanged from 2006, including, notably, the co-teaching model. In 2007 undergraduate teaching assistant Thomas Fai attended class meetings and helped to answer student questions. In 2008, François Dorais and I co-taught the course.

Math 175 is a “freshman honors seminar,” which means that it is a small class intended for first-year students in the honors program. Each section is capped at 20 students. I have had between 15 and 19 students in the four sections I’ve taught. The students are generally from the LSA honors program, though there are usually a few from Engineering and from general LSA. Very few students have a desire to major or minor in mathematics before taking the course. Part of the aim of the course is to get students excited about mathematics. Hopefully some of them will go on to take further math courses.

Students not in the honors program are required to have instructor approval to enroll in Math 175. I never turned away an interested freshman, but I always declined requests from upperclassmen. I think it is important that the class be fairly homogeneous. Students should feel as equals with their classmates and thus be unafraid to express their opinions. With this in mind, I think it is also important to identify and gently nudge out students who are too good. For example, in fall 2008 there were three students in one section of Math 175 who were also taking math 295 (“super honors” calculus). They were good students but they upset the egalitarian dynamic of the classroom.

The course meets four days a week for fifty minutes. Monday, Tuesday, and Wednesday class is held in a seminar room with individual desks and several chalkboards. Thursday meetings are held in a computer lab. Attendance is absolutely mandatory. I’ve used a very effective carrot-and-stick approach. As reward for coming to class, participation makes up a full 20% of their final grade. The punishment for missing class is severe. Each student gets three “free” absences. Each subsequent absence results in the final grade dropping by a full letter, e.g., an A student with five unexcused absences receives a C.

2.1. Group work. On a typical class day, we randomly arrange students in groups of two or three, and hand out one of the worksheets.
Students stay with their group until completion of the worksheet; often three or four class meetings. These worksheets are meant to be done (only) in class. The pace of the course overall is dictated by student progress through the worksheets. When one worksheet is finished, there is usually some sort of “wrap up” discussion and new groups are formed to begin a new worksheet. It is a real luxury that Math 175 is not a prerequisite for any subsequent course. This means you can really wallow in a topic if it seems to be the right thing for the students.

As students dig into the worksheets, we circulate to listen to student ideas, and to ask and answer questions. Students are periodically invited to the board to present solutions to the problems on the worksheets. Usually one or two students will be selected to present in the second half of the class period. Be sure to allow at least ten minutes for a presentation; fifteen or twenty is better. Too often in my first year I found myself rushing students through their presentations. This is frustrating for everybody. Keeping an eye on the clock is any easy solution to this problem. More on answering student questions, motivating students when stuck, and managing student presentations is discussed in the “Difficulties and Advice” section.

The design of the worksheets is as follows. Like a section of a textbook, a given worksheet usually has one main idea. A “goal theorem”, say. The worksheet builds gradually toward this goal theorem, introducing definitions as necessary. There is a mix of numerical and abstract problems, all of which are meant to guide students to the idea of the goal theorem.

My approach for designing such a worksheet is straightforward. Beginning with the goal theorem, I first write my own proof. Then I ask, “what would a student need to know to understand and construct this proof?” First off, they probably need a lemma or two. Now, what would they need to be able to prove these lemmas? Is it possible to guide students (with examples) to the idea of the lemma before they’ve seen its statement? There are also some definitions that should probably appear along the way, and they too should be motivated with examples. In the end, a typical goal theorem will come at the end of a sequence of fifteen or more problems. Along the way there is no such thing as a problem that’s “too small” for the students.

If you plan to teach this course you should go through the worksheets and modify them to suit your own tastes. If you prefer a different path

---

3Don’t give them any free answers! I like to use the psychiatrist’s old trick of answering a question with a question. Student: “There are infinitely many primes, right?” Instructor: “Do you think there are infinitely many primes?”
to a particular goal theorem, map it out! If there is a topic omitted that you really like (Pollard’s \( \rho \) method for instance), make a new worksheet!

The students should keep notes on the worksheet problems in a separate folder, or in a composition notebook. This will be their “textbook” for the course and helpful when it is time to do homework or study for exams.

2.2. **Computer lab.** The computer lab is generally fun for everyone. Students get into groups of two or three to complete a day’s task. Sometimes the goal is very narrow (“decode this message”), other times it is wide open (“find the largest integer you can with the following properties...”). Often the lab activities are phrased in terms of a competition, with bonus points for the winning team. Whereas the homeworks and in-class worksheets encourage students to think deeply and methodically, the lab activities often reward speed and following hunches—different kinds of problem solving skills.

Sometimes the lab topics are closely related to the worksheets from earlier in the week, e.g., implementing the Euclidean algorithm. Other times the lab has little to do with the classwork. In either case the topic should be engaging and most students should be able to finish within an hour. Students find the labs a nice respite from the hard work they are putting in on the class worksheets.

Maple is the default program for most of these activities, though there are some web-based activities as well. An added benefit of using software like Maple is that students can begin to use it when working on homework problems.

The computer lab activities have changed much more from year to year when compared with the worksheets. Dorais is working to redesign the computer labs (making them more cohesive) for fall 2009.

2.3. **Homework and exams.** In some IBL courses there is no homework and there are no exams. Grades are based solely the number and quality of solutions presented, for example. In other IBL courses, there is written homework, but no exams, and presentations make up a large part of a student’s grade. Math 175 has both written homework and exams, and we don’t grade presentations. One advantage of this approach is that it makes grading straightforward for the instructor. No different from a typical lecture course, really. Also, it feels more “normal” for the students. The class is different enough for them already, and if they were to be graded on presentations, that would only add anxiety to a situation they already find stressful. I have considered
dropping the final exam in favor of some sort of final project, but for now this is a vague idea.

During the semester the students have nine homework assignments, two midterms, and a final exam. Students are encouraged to work together on the homework, though they must acknowledge their collaborators and write up their own solutions. The way the homeworks and exams are currently written reflects the timing of the most recent semester’s students. If you find your class moving faster or slower, you may need to move some problems accordingly or change due dates to match the pace of the worksheets.

The homeworks have two parts. The first contains problems and exercises based on material presented in the worksheets. The second, called “outside the box” (OTB) questions, are often quite challenging. The exams are meant to be fairly straightforward, with problems drawn from worksheet material and of difficulty comparable to the first part of the homework.

The purpose of the OTB questions is to help students develop their problem solving skills. These problems may or may not (more often not) be related to the worksheets. Often they have many layers so that students can see progress without necessarily reaching the final answer. Usually a student can receive half credit or more on these problems for some carefully worked out examples and a nice conjecture. Rarely will a student be able to tackle all the OTB questions on a homework (and they are not required to do so).

Apart from developing good problem solving skills, the homework can help students develop their skill at communicating complex ideas. Thus the standard for written homework is very high. As is to be expected, their writing is generally horrible at the beginning of the semester. But they do improve! Early and often, you can show them what good mathematics writing looks like, and cheerfully encourage them to achieve that goal. They need to be told that yes, complete sentences in proper English are required, and no, three examples do not prove a universal statement. Then they need to be told again. And again. But if you are patient, and encourage them to talk about it with one another, they get it eventually.

Each year I am struck by the quality of written work at the end of the semester compared to that of the beginning. While still not perfect, I would compare it favorably to the writing found in a junior-level linear algebra class.
3. Difficulties and Advice

Run well, this course can be the most fun you’ve ever had in a classroom. (Certainly that has been my experience.) However, there are many places where it can go off the rails if you’re not careful. The results can be painful for everyone involved.

3.1. Marketing the method. One of the best ways to ensure a successful semester has nothing to do with mathematics. Here is a terrific quote from a former student, when asked what he would tell future students taking the class:

You may think that Professor Petersen does not lecture because he does not know what he’s doing, or is a bad teacher. This is false. I learned some of the best critical, logical thinking skills from him because of the specific way in which this class is taught.

Consider the first sentence. If you don’t convince the students otherwise, this is their most common assumption. You’re lazy, a bad teacher, you don’t know what you’re doing. Before you have even given them the first handout they are skeptical of the method or worse.

First impressions matter. On the first day of class try to tackle the “perception problem” head-on. Explain to them why you think the class is taught as it is: that they will learn the material better, that they will have ownership of the ideas, that they will experience the joy of discovery of new ideas, and so forth.

Analogies can also help. Ask the students what their hobbies and extracurricular interests are. Any basketball players? Any cellists? Ask them how they became proficient. Did you become a good basketball player by watching your coach dribble around and do lay-up drills? by watching Michael Jordan? No. Did you learn to play the cello by watching your teacher do scales? by listening to Yo-Yo Ma? Of course not.

To become good at something you need to do it yourself. This makes sense to students. In this class you, the instructor, will play the role of coach.

If you hit the students early and often with these ideas—I probably bring it up in one way or another at least once a week for the first month—you can convince them that at least there is a good philosophy behind the structure of the course. This gets you as far as the second sentence in the student quote above. Bringing each student all the way to the final sentence is subtler, and, perhaps, not always possible.
The problem is that unlike playing basketball or playing music, most students don’t inherently derive joy from “playing” mathematics. Therefore the hard work involved in getting better and learning will tend to feel like work for them. It is good to remember this point of view throughout the semester so that, whenever possible, you show students what a great game this math stuff can be!

3.2. Developing a positive culture. One of the simplest ways to get students to enjoy themselves while working hard is to get them to enjoy coming to class. It is easy for students to be excited about the days in the computer lab. On days spent in the classroom with the worksheet it takes more effort. In general the time spent in class should be friendly and open so that students feel comfortable offering their opinions without fear of looking foolish. Students need to make mistakes and discuss the dead ends to get the most out of class time. If they are too shy or embarrassed to speak openly everyone loses out.

A certain passiveness or apathy in the mathematics classroom is something that, for many students, has been reinforced for years. The standard model has them sit quietly at desks listening to a lecture and passively taking notes. Few are engaged mentally. They are rarely, if ever, challenged to think in the moment. Part of the difficulty early in the semester is to overcome their habits.

In a similar vein, consider Schoenfeld’s observation [?] that U.S. high school students average about two minutes of thinking per homework problem. Two minutes! You either get it immediately or it’s hopeless. To the average student, working on the same problem for fifteen minutes is an eternity. This is probably tied to the notion that mathematical ability is something innate, rather than something attained through hard work. They are shocked when I tell them that I, as a research mathematician, am stuck more than 95% of the time. I have no idea what the answer is or how to get there. What do I do then? Work more examples. Ask a narrower question. Ask a broader question. Change the parameters and do even more examples. These ideas don’t occur naturally to most students. So tell them. They need to learn that it is the struggle that matters, and that the struggle is often a necessary precursor to that five percent of insight and progress.

What is rewarded in the classroom is the struggle, not only the solution. Every attempt is to be applauded. Most of the students are likely to be unsure of themselves in the beginning. For these students the first few experiences should always end on a positive note, even if what the student says is nonsense mathematically. Thank the student for speaking up. Smile. Locate the kernel of truth in what the student
said and point out its brilliance to the rest of their group or to the class.

It’s also fun to point out that while some approaches are “incorrect solutions”, they are theorems themselves, and the students are still creating mathematics! Say students analyze a certain function and find $f(1) = 2, f(2) = 4, f(3) = 8, f(4) = 16$. At this point the conjecture $f(n) = 2^n$ emerges and students spend a good deal time and effort to proving the conjecture, to no avail. Finally, someone, for lack of any better ideas, works out the case $n = 5$ and finds $f(5) = 31$. Most students will despair—they don’t even have a good conjecture now! Suppose class is ending and you want to end on a positive note. You can take the chalk and write the following on the board (the group of students is Sarah, Jimmy, and Eva):

**Theorem 1** (Sarah, Jimmy, Eva). We have $f(n) = 2^n$ for $n = 1, 2, 3, 4,$ and $f(5) = 31$.

**Corollary 1.** The function $f(n)$ is not generally equal to $2^n$.

This is progress! Make them believe it!

### 3.3. Presentations at the board.

Over the course of the semester all the students should spend roughly the same amount of time presenting at the board. While walking around the classroom, identify which groups “get it” and which groups are having more trouble. Anywhere from ten to thirty minutes from the end of class ask a particular student to go to the board and present a solution to a particular problem. In the beginning especially, I like to pick students who seem to have a good handle on the problem. For students who seem more shy or less confident, I pick an easier problem to help their chances for a positive experience.

When the student has written their solution on the board, call the class to attention, “All right, now we have Eva presenting her solution to problem 3,” and take a seat at the back of the classroom. (Physically moving to the back of the room and sitting down removes you from a position of authority and places Eva, at the chalkboard, in that position.) When Eva has finished her explanation, there will be silence. Probably the class will turn in their seats to look to you for approval/disapproval. Smile. Say nothing yet of your thoughts of the solution. Ask if there are questions for the speaker. Once any questions are answered, if you think the presentation was complete and correct, say so—“Great job, Eva! I especially like the part where...”—and give the speaker a round of applause.
What if a student presents a solution and there is an obvious flaw in the argument? You ask, “Does anyone have a question for Eva?” and you wait. Don’t...say...anything. Wait! Don’t say anything. Wait longer! Two minutes of silence is not unusual. It is very likely that someone in class sees the error but is too shy or too polite to point it out. Eventually someone will speak up, and then it is your job to facilitate discussion. It is not your job to point out the mistake, and it is certainly not your job to show them how to fix it. This is where the cool stuff happens, because, believe it or not, they will figure things out for themselves. You “helping” here just steals the thunder from someone who could have thought of the idea for themselves. The confidence that students gain at this time is invaluable.

3.4. When students are stuck. It is possible there will be times that nobody but you sees the fatal flaw in an argument. You’ve asked for questions, waited two full minutes, and still nothing but blank stares. What to do? Hint at it. The more oblique the suggestion, the better. I like starting this approach by having the presenter read their solution aloud again. Then I ask for questions and wait again. Still nothing? I focus in a bit more. “Could you please read the second paragraph once more?” Still nothing? “Could you please read that paragraph one more time? There’s still something that I don’t quite understand.” You can also ask someone in the audience to describe their approach. “Anna, could you tell us how this compares to your group’s solution?” Still nothing? (I can’t actually think of time when I got this far and there were still no fruitful comments from the audience.) Well, have them read it again: “Okay, one more time, from the top...” It’s sort of like the shampoo algorithm: Lather. Rinse. Repeat as necessary.

But of course you don’t have unlimited time and students don’t have unlimited patience and determination. Sometimes you really are beating a dead horse, or it’s nearly the end of the hour and you want to end on an upbeat note. This is a very delicate situation. I would argue that it’s okay to leave a problem on the board unresolved, provided that you can cast off any air of defeat before dismissing the class. “Okay, Jimmy, unfortunately we’re near the end of the hour, so we’ll have to pause here and begin again tomorrow. I think we made some real progress today, though! This must just be a real tough nut to crack...We’ll all sleep on it and see what we can come up with tomorrow. Remember it took two hundred years to prove Fermat’s last theorem!”

Managing situations like this require the most skill on the part of the instructor. First you need to realize that time is running away and
nobody is going to have answer. Then you need to disengage everyone in a way that doesn’t feel like giving up. It’s not easy.

Students can also use help before getting to the chalkboard. When stuck during group work the “Read it. Read it again.” approach isn’t usually appropriate. There are many other suggestions that you can give students to get them past a hurdle though. Prompt them without giving away too much. “Which examples have you tried? Hmm... what about an example where n is prime?” Sometimes students throw up their hands and ask a question that in essence says “Can you tell us the answer please?” These include gems like “I don’t get it,” and “I don’t know what I’m supposed to do.” My favorite approach to these questions is to answer with my own question: “What part of the problem don’t you get?” or “What do you think you should do here? Did you try an example?” Also, “Do you understand all the words in the statement of the problem?” (This can be a legitimate concern!)

In general, just remember that the goal is to have the students identify and correct mistakes without your help. The less you say to get them to do that, the better. Once they’ve done it, go bananas! “That is so awesome! That’s the most incredible thing I’ve ever seen!” It really is exciting to watch when it works well, so chances are your praise will be genuine. If not, fake it.

4. Some Reading

The Legacy of R. L. Moore Project website [?] is a good resource for all things inquiry-based, and can put you in touch with a large network of practitioners and proponents of the method. They have an annual meeting in Austin, Texas. Paul Halmos’ article [?] is great reading and makes a compelling argument for teaching what he calls a “problems course”. For convenience it is included in this folder. Alan Schoenfeld is a leading math education researcher and proponent of inquiry-based methods. The article cited below [?], and included in this folder, points out several problems arising in lecture-based courses that he feels are corrected in an inquiry-based environment.

References