**Modular Multiplication and Encryption**

Author(s): John Quintanilla

Date/Time Lesson to be Taught: August 5, 2013

**Technology Lesson:** ~~Yes~~ No

Course Description:

Name: Summer Mathematical Enrichment Class 2013

Grade Level: Mostly 4th graders

Honors or Regular: Honors

Lesson Source: This lesson was inspired by *Cryptography As A Teaching Tool*, accessed at <http://www.math.washington.edu/~koblitz/crlogia.html>. In particular, note the second paragraph of this section:

**Kid-RSA.** The following cryptosystem can be introduced among secondary school students who have learned how to reduce numbers modulo a positive integer *n* and how to convert numbers from one base to another. In particular, they must know how to work with blocks of letters regarded as integers to the base 26, where each letter is a digit (that is, A=0, B=1,..., Z=25).

To set up the system, a student (Alice) chooses any two integers *a* and *b*, sets *M*=*ab*-1, then chooses two more integers *a*' and *b*', and finally sets *e*=*a'M+a*, *d*=*b'M+b*, *n*=(*ed*-1)/*M*= *a'b'M+ab'+a'b+*1. Her public key is (*n,e*), and her private key is *d*. (The letter ``e'' was chosen to signify ``encryption'' and ``d'' to signify ``decryption.'') To send Alice a plaintext *m*, one uses the map *c*=*em* (mod *n*); Alice deciphers the ciphertext by multiplying by *d* modulo *n*. Note that the decryption operation recovers the plaintext, because *dc*=*dem*=*m* (mod *n*).

As a side excursion, one can show how to make digital signatures. This works as follows. Suppose that Bob wants to sign a message to Alice with the letters ``BOB.'' Suppose that his public key is (*n',e'*), and his private key is *d'*. Let *s* be the integer corresponding to his signature: *s* = (BOB)26 = (1 26^2 + 14 26 + 1)10 = (1041)10. Bob first computes the least non-negative residue of *d's* modulo *n'*, then multiplies this number by *e* modulo *n*, and sends the result to Alice. Alice takes this number, multiplies it by *d* modulo *n* and then by *e'* modulo *n'*. It is not hard to see that she obtains *s* = (BOB)26. Alice then knows that no one other than Bob could have sent her this signature, because no one other than Bob knows the value *d'* that is ``undone'' by *e'* modulo *n'*.

An interesting question is whether the youngsters will be able to break Kid-RSA. If they can find an efficient way to compute an integer *d* such that *de*=1 (mod *n*) (not necessarily the same *d* that Alice has as her private key), then they can break the system, since multiplication by *d* modulo *n* inverts the encryption function, as we saw above. There is an efficient algorithm to find such a *d* that goes back to Euclid (see, for example, [7]), but students who have never studied number theory are not likely to know this algorithm.

Here is a question to which I do not know the answer: Can one prove that the ability to crack this cryptosystem (for any choice of *a,b,a',b'*) implies the ability to solve the equation *xr+ys*=1 for any two relatively prime integers *r* and *s*? Could there be a way to crack Kid-RSA without essentially rediscovering a version of the Euclidean algorithm?

In the current lesson plan, we use a pre-made table of age-appropriate 3-letter words, obviating the need for base-26 arithmetic. Also, to keep the numbers as small as possible (and to make one less complicating factor), we take *a’* = *b’* = 1.

Objectives:

* SWBAT perform modular multiplication via subtraction.
* SWBAT perform modular multiplication via quotient and remainder.
* SWBAT identify multiplicative inverses with modular multiplication.
* SWBAT apply multiplication inverses to encrypt and decrypt messages.

Texas Essential Knowledge and Skills:

§111.6. Grade 4.

(b)  Knowledge and skills

(4) Number and operations. The student applies mathematical process standards to develop and use strategies and methods for whole number computations and decimal sums and differences in order to solve problems with efficiency and accuracy. The student is expected to:Geometry and spatial reasoning. The student uses geometry to model and describe the physical world. The student is expected to:

(E) represent the quotient of up to a four-digit whole number divided by a one-digit whole number using arrays, area models, or equations

(H) solve with fluency one- and two- step problems involving multiplication and division, including interpreting remainders.

Materials List and Advanced Preparations:

* Vocabulary sheet
* List of English 3-letter words (with some age-inappropriate 3-letter words omitted)
* Blank M-tables
* Modular multiplication handout (with two numbers that are multiplicative inverses)
* Kid RSA handout (Parts 1 and 2)
* Assessment (as time permits)
* List of RSA numbers
* Calculator
* Paper
* Pencil

**Accommodations for Learners with Special Needs (ELL, Special Ed, 504, GT, learning styles, etc.):** None provided below, though this could be added.

**5Es**

|  |  |  |
| --- | --- | --- |
| **ENGAGEMENT 1 Time: 5 Minutes** | | |
| **What the Teacher Will Do** | **Probing/Eliciting Questions** | **Student Responses and Misconceptions** |
| Take a look at the paper with the hundreds and hundreds of three-letter words.  This is an example of a **code**, where every word has been changed into a number. Please write **code** on your vocabulary sheet.  That really wasn’t much of a secret code. Today, we’re going learn some of the math that goes into making a really secret code. | 45. What word did I say?  130. What word did I say?  420. What word did I say?  Can I have a volunteer? (Picks a student.)  You’re going to be the **sender**. I’m going to be the **receiver**. Pick a word off the list, and tell me the number that goes with your word.  Was your word (fill in the word)?  (Repeat this a few times with other senders.)  Do you think this is a good code?  OK, here’s a different question. Suppose someone else was giving me a number. Did you understand which word it was?  How did you do that?  So was that secret message much of a secret? | Bat.  Eat.  Raw.  Writes **code** on vocabulary sheet.  Sender tells me a number.  Sender answers.  Yes, this is fun!  Yes, of course.  We just looked at the paper.  No, not really. |
| **Evaluation/Decision Point Assessment** | | **Student Outcomes** |
| Students can use the given code for three-letter words. | | Students are engaged with the day’s lesson. |

|  |  |  |
| --- | --- | --- |
| **EXPLORATION 1A Time: 10 Minutes** | | |
| **What the Teacher Will Do** | **Probing/Eliciting Questions** | **Student Responses and Misconceptions** |
| Today, we’re going to learn about a special kind of multiplication table. (Hands out M5 table.)  We’re going to call this an M5 table. We’re still going to multiply, but we’re only going to permit answers that are less than 5.  OK, so 1 times 2 is 2. Let’s put that in the table.  Of course. So we’ll put that in the table too.  OK, we’re done. Now let me tell you the rule we’re going to use when we hit a number bigger than 5. We’re just going to subtract 5 until we get a number less than 5.  For example, 2 times 3 is 6.  So what I’m going to do is subtract 5.  So, where I would ordinarily write 6, I’m going to write 1. (Writes 1 twice in the table, for 2 times 3 and 3 times 2.) Remember, this is not a multiplication table, but an M table. So the rules are a little bit different.  We only have a few more left before the table Is done. | Can somebody pick two numbers that, when you multiply them, you get an answer less than 5?  Any others?  Any others?  (Keep going until 0 and 1 columns are filled, as well as 2 times 2.)  Any others?  Is that bigger than 5?  What’s 6 – 5?  What should we try next?  I can’t write 8 in the table, since that’s bigger than 5. So what should I write instead?  What next?  What should go in the table?  What next?  What should go in the table?  What next?  What should go in the table? | (Maybe) 1 and 2!  2 times 1!  I don’t think so.  Yes.  1.  2 times 4 is 8.  8 minus 5, or 3.  3 times 3 is 9.  9 minus 5, or 4.  3 times 4 is 12.  12 minus 5, or 7.  Wait, we can only put down an answer less than 5.  So 7 minus 5, or 2.  4 times 4, or 16.  16 minus 5 is 11.  11 minus 5 is 6.  6 minus 5 is 1. |
| **Evaluation/Decision Point Assessment** | | **Student Outcomes** |
| Students have completed the table of multiplication modulo 5:   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **M5** | **0** | **1** | **2** | **3** | **4** | | **0** | 0 | 0 | 0 | 0 | 0 | | **1** | 0 | 1 | 2 | 3 | 4 | | **2** | 0 | 2 | 4 | 1 | 3 | | **3** | 0 | 3 | 1 | 4 | 2 | | **4** | 0 | 4 | 3 | 2 | 1 | | | Students understand what’s expected to construct an M table… multiplication followed by subtraction as necessary. |

|  |  |  |
| --- | --- | --- |
| **EXPLORATION 1B Time: 30 Minutes** | | |
| **What the Teacher Will Do** | **Probing/Eliciting Questions** | **Student Responses and Misconceptions** |
| We just did an M5 table.  Now I want you to work with a partner to make an M4 table.  Good. So the 0 row, 0 column, 1 row, and 1 column will be easy for you. Work with your partner to complete the rest of the table. And remember that this is an M4 table, not an M5 table.  Good. Next, I want you to work on the M3 table. | What was the significance of the 5?  And what numbers appeared on the top row and left column?  Two of these numbers will be really, really easy to multiply. Which two numbers are the easiest? | That’s the number we subtracted.  0 through 4.  0 and 1!  Students work until they get the full M4 table:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | M | 0 | 1 | 2 | 3 | | 0 | 0 | 0 | 0 | 0 | | 1 | 0 | 1 | 2 | 3 | | 2 | 0 | 2 | 0 | 2 | | 3 | 0 | 3 | 2 | 1 | |
| *Continue as time permits for M2 and M6 through M10 tables. Teacher perambulates to answer questions as they arise. The pace will slow down once M6 is reached. Teacher may suggest for students to try the M10 table after M2, as that will be the fastest “big” table to complete. Students may volunteer patterns that they see in the M-tables.*  *M11 and M12 tables are provided for quicker students to do as the others finish through M9.*  *Some students might volunteer a shortcut: the Explanation about multiplying, dividing, and writing down the remainder might arise here. So roll with the punches and see what happens… it may prove best to discuss the Explanation earlier than expected.* | | |
| **Evaluation/Decision Point Assessment** | | **Student Outcomes** |
| Students have completed as many modular multiplication tables as time permits. | | Students understand the process of modular multiplication. |

|  |  |  |
| --- | --- | --- |
| **EXPLANATION 1 Time: 15 Minutes** | | |
| **What the Teacher Will Do** | **Probing/Eliciting Questions** | **Student Responses and Misconceptions** |
| Let’s take a look at the M6 table.  Good. Let’s take a closer look at what you just described. You started with 4 times 5. That’s 20. Let me write that on the board like this:  X X X X X  X X X X X  X X X X X  X X X X X  Then you started taking them away 6 at a time.  Let me draw another 20 X’s, except using rows of 6:  X X X X X X  X X X X X X  X X X X X X  X X  Good. Let’s do it again.  Let’s review. In the first example, we chose the M6 table, and we had 4 times 5. Of course, 4 times 5 is 20. We drew 20 X’s in 3 rows of 6, leaving 2 X’s left over. So the M6-product of 4 and 5 was 2.  In the second example… (*repeat, except with the numbers chosen by class*).  That’s right. In the first example, 20 divided by 6 is 3 with 2 left over.  Please write **quotient** and **remainder** on your vocabulary sheets. (Writes on board.)  Let’s look at the second example. (Repeats.)  Good. Let’s try it again.  The M number that we’re dividing by has a special name. It is called the **modulus**. Please write **modulus** on your vocabulary sheets. (Writes on board.) | What was the M-product of 4 and 5? (Writes on board.)  Can you tell me how you got that?  Can I draw 20 X’s into rows of 6?  So what happens when we start taking away 6 at a time?  So, using the M6 table, what was the M-product of 4 and 5?  And what does that mean in this picture?  Did I care about how many rows I took away?  Somebody pick a different M-table and two numbers bigger than 1 from that table.  Does this procedure remind you of anything?  Do you remember what the 3 is called?  And what is the 2 called?  Somebody pick a different M-table and two numbers bigger than 1 from that table. | I got 2.  4 times 5 is 20.  20 minus 6 is 14.  14 minus 6 is 8.  8 minus 6 is 2.  2 is less than 6, so I stopped.  No, 6 doesn’t go evenly into 20.  Yes, but you’ll have some left over.  The first row goes away, then the second row goes away, and then the third row goes away.  2.  The two Xs on the last row.  Not really. What’s important is the number of X’s on the last row.  *(Repeat the above argument with the numbers chosen by the students.)*  No, not really.  Oh… division!  The quotient.  The remainder.  Students write **quotient** and **remainder** on their vocabulary sheets.  *(Repeat the above argument --- multiply the numbers, divide by the modulus, and find the remainder. This should match the number in the M-table.)*  Students write **modulus** on their vocabulary sheets. |
| **Evaluation/Decision Point Assessment** | | **Student Outcomes** |
| Students have confirmed several M-table values match the remainder when the regular product is divided by the modulus. | | Students understand the connection between modular multiplication and finding a remainder. |

|  |  |  |
| --- | --- | --- |
| **ELABORATION 1 (time permitting) Time: 15 Minutes** | | |
| **What the Teacher Will Do** | **Probing/Eliciting Questions** | **Student Responses and Misconceptions** |
| Let’s now take a look at your M tables.  Please write **prime** on your vocabulary sheet.  Good. If the M number has factors, then the M product of those factors is 0.  Excellent. In college math, each one of these M-tables is called a **ring**.  The prime ones --- which don’t have any M-products of 0 --- are called **fields**.  Please circle the upper-left hand corners of M2, M3, M5, M7, and M11, since they’re the special ones.  Let’s now look at just the M5 table.   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **M** | **0** | **1** | **2** | **3** | **4** | | **0** | 0 | 0 | 0 | 0 | 0 | | **1** | 0 | 1 | 2 | 3 | 4 | | **2** | 0 | 2 | 4 | 1 | 3 | | **3** | 0 | 3 | 1 | 4 | 2 | | **4** | 0 | 4 | 3 | 2 | 1 |   That’s OK. This is why the M tables are special for primes. For M2, M3, M5, M7, and M11, we can define division. But for the others, we could get more than one answer, or we could get no answer. That’s the big difference between a ring and a field. | Which M tables have no zeroes?  Why not?  OK, let’s ignore the 0 row and 0 column. Which M tables have no other zeroes besides those?  So which tables have a 0 somewhere else besides the 0 row and 0 column?  So let’s list all the times that we get an M-product of 0 somewhere else besides the 0 row and 0 column.  So let’s think about this. M2, M3, M5, M7, and M11. What’s special about 2, 3, 5, 7, and 11?  And what’s about the others?  So 6 is not prime. Can anyone explain how this would cause an M-product of 0?  Can anyone explain any of the other cases when we get an M product of zero?  What is 1 divided by 2?  Yes, with ordinary numbers, 1 divided by 2 is one-half. But with M5, 1 divided by 2 is actually an ordinary number.  Sure. Take a look at the table. 2 times what number gives you an M5-product of 1?  That’s right... using the M5 table, 2 times 3 is 1. Also, what is 3 times 2?  So these are part of the same fact family. (Writes 2×3 = 1 and 3×2 = 1 on the board.) Let’s now write the other two parts of this fact family. 2 times 3 is 1. So, if we’re using the M5-table, what is 1 divided by 2? (Writes 1÷2 = on board.)  And what’s 1 divided by 3? (Writes 1÷3 = on board.)  Good. We get some funny rules when we use the M-tables, right?  Let’s try the M6 table. What’s 2 divided by 2?  Actually, it’s not so easy. What’s 2 times 4 on the M6 table?  So, if 2 times 4 is 2, then what’s 2 divided by 2?  But you said that 2 divided by 2 is 1. What happened? | None of them.  They all have zeroes in the 0 row and 0 column.  M2, M3, M5, M7, and M11.  M4, M6, M8, M9, M10, and M12.  In M4, 2 times 2 is 0  In M6, 2 times 3 is 0  In M6, 4 times 3 is 0  In M8, 2 times 4 is 0  In M8, 4 times 4 is 0  In M8, 6 times 4 is 0  In M9, 3 times 3 is 0  In M9, 3 times 6 is 0  In M10, 2 times 5 is 0.  In M10, 4 times 5 is 0.  In M10, 6 times 5 is 0.  In M10, 8 times 5 is 0.  In M12, there are lots.  They’re prime numbers!  They’re not prime!  Students write **prime** on their vocabulary sheets.  Sure. 2 times 3 is 6. Then we subtract 6 to get 0.  Sure. 3 times 3 is 9. Then we subtract 9 to get 0.  (Answers vary.)  Students write **ring** and **field** on their vocabulary sheets.  Students circle these five corners.  One-half.  What?!?!  Ohh.. 2 times 3 is 1.  3 times 2 is also 1.  1 divided by 2 is 3.  1 divided by 3 is 2. (Nervous laughter.)  YES!  That’s easy: 1.  2 times 4 is 2.  4.  Uh, er, um… |
| **Evaluation/Decision Point Assessment** | | **Student Outcomes** |
| Students understand that zero products are impossible only for a prime modulus. | | Students understand how the concepts of prime and composite are related to the M tables. |

|  |  |
| --- | --- |
| **EVALUATION 1 / ENGAGEMENT 2 Time: 15 Minutes** | |
| **Evaluation/Decision Point Assessment** | **Student Outcomes** |
| I’m now going to hand out a blank M9 table. I want you to complete it. You can either use the original subtraction method or else use division; it’s your choice.  Fill out as much of the M9 table as you can in the time that we have. | Students remember how to make an M table, perhaps using division to speed things up. |

|  |  |  |
| --- | --- | --- |
| **EXPLORATION 2 Time: 15 Minutes** | | |
| **What the Teacher Will Do** | **Probing/Eliciting Questions** | **Student Responses and Misconceptions** |
| I want you to get a liitle more practice with using the M tables. So please pick an M table larger than M6. | (Walks students through the steps of the Modular Multiplication Lesson handout. Students either work individually or in pairs.)  (Picks a student.) Please tell the class which M-table you chose, and which two numbers you chose.  (Asks two or three more students to share their choices.)  So did most everyone have different choices of the M-table and the two different numbers from that M-table?  OK, most everyone had different numbers. Now, what final answers did we get? | Answers vary.  Yes.  We all got 1 through 6! |
| **Evaluation/Decision Point Assessment** | | **Student Outcomes** |
| Students get extra practice with modular multiplication. | | Students are engaged and want to know how everyone got the same six answers. |

|  |  |  |
| --- | --- | --- |
| **EXPLANATION 2 Time: 10 Minutes** | | |
| **What the Teacher Will Do** | **Probing/Eliciting Questions** | **Student Responses and Misconceptions** |
| Wait a minute. You’re telling me that nearly everyone used different numbers, but everyone got 1 through 6.  Good. Somebody pick another M table, and give me two other numbers that have an M-product of 1.  OK, let me give you one. Let’s do an M19 table.  I know, I know. But it’ll be OK. My first number is going to be 13.  Good. We’re going to use the M19 table, and our two numbers are 13 and 3. Now, we don’t have a completed M19 table, so we’re going to have to figure these out together.  I’m going to call 19 my **public key**. The first number, 13, is called the **encryption key**. And the second number is called the **decryption key**. Please write these on your vocabulary sheets.  Good. What I just did was take the original number 2 and **encrypt** it. Please write **encrypt** on your vocabulary sheets.  Good. To get the original 2 back, we’re going to **decrypt** this 7. Please write **decrypt** on your vocabulary sheets. | How did that happen?  How did you pick your two numbers from the table?  Let’s start with 2. What’s the M-product of 2 with the first number?  And what’s the M-product of that with the second number?  Good. (Repeat for 3 and 4.)  I need to figure out the number so that 13 times \_\_\_\_ is equal to 1 using the M19 table. Any ideas?  OK, let’s find it. What’s 13 times 2?  On the M19 table?  Well, that didn’t work. Let’s keep going. What’s 13 times 3?  On the M19 table?  Let’s start with 2. What’s 2 times 13?  On the M19 table?  How are we going to get the original 2 back?  OK, 7. What’s 7 times 3?  On the M19 table?  Good. Does someone else want to volunteer a starting number? | I don’t know.  Ohh… we chose the numbers to have an M-product of 1. So multiplying the two numbers separately was just like multiplying by 1.  Answer depends on the numbers selected.  Hey, it’s 2!  Nervous laughter.  But we haven’t made an M19 table!  Uh, um, er….  26.  Oh, 26 minus 19 is 7.  39.  Oh, 39 minus 19 is 20.  20 minus 19 is 1.  *Or: 39 divided by 19 is 2 with remainder 1.*  Students write the words **public key**, **encryption** and **decryption key** on their vocabulary sheets.  26.  26 minus 19 is 7.  Students write **encrypt** on their vocabulary sheets.  We’re going to multiply by 3!  Students write **decrypt** on their vocabulary sheets.  21.  21 minus 19 is 2. We got 2 again!  Answers vary… numbers could get large! |
| **Evaluation/Decision Point Assessment** | | **Student Outcomes** |
| Students are more comfortable with M-multiplication, including M19 multiplication, for which they do not have pre-made table. | | Students will see that the original number is returned by M-multiplying by two different numbers. |

|  |  |  |
| --- | --- | --- |
| **ELABORATION 2A Time: 20 Minutes** | | |
| **What the Teacher Will Do** | **Probing/Eliciting Questions** | **Student Responses and Misconceptions** |
| *Hands out Make Your Keys worksheet: Part 1.*  This process --- encrypting a message and then decrypting it --- is called an algorithm. Please write algorithm on your vocabulary sheet.  In the handout that I’ve given you, you will use the M tables to encrypt and decrypt a message.  (Walks students through Steps A-V.)  So that’s the first problem… the M table is too small to permit a lot of messages.  Here’s the second problem. Suppose the sender sends a message to the receiver… but I want to capture the message and figure it out for myself.  So that’s another problem. Because the M-table is so small, it’s easy for someone to break the code. | Why not? You’ve got the same list of words that we do.  There are a couple of small problems with the code we just used. First, what kind of number could you start with?  And why couldn’t you choose a number like 15 or 123?  What do I need to do that?  And if you’re using an M11 table, how many possible descriptive keys are there?  Is that a lot of possible decryption keys, or is that only a few? | Students write **algorithm** on their vocabulary sheets.  No!  A number between 1 and 8.  Because those were off the table!    The decryption key.  I don’t know… 10?  Only a few. |
| **Evaluation/Decision Point Assessment** | | **Student Outcomes** |
|  | |  |

|  |  |  |
| --- | --- | --- |
| **ELABORATION 2B Time: 25 Minutes** | | |
| **What the Teacher Will Do** | **Probing/Eliciting Questions** | **Student Responses and Misconceptions** |
| *Hands out Make Your Keys worksheet: Part 2.*  Let’s do another encryption, except using bigger numbers.  (Walks students through Steps A-W. Also, pick someone’s work and use a calculator to confirm that the M-product of Step F and Step G is 1 when using modulo Step E.)  That’s right. This is the basis behind the **RSA algorithm**, which is used all over the world. Every time your parents use a credit card, RSA encryption is used to keep their information safe and secure.  The RSA algorithm was invented in 1977. It’s younger than me! And it uses a lot of math.  What we’ve done isn’t quite the RSA algorithm. But I’ll tell you a few things about it:  1. It relies on modular multiplication.  2. It has a public key, an encryption key, and a decryption key.  3. It uses really, really, *really* big numbers! Take a look at some of the numbers that have been used for RSA encryption for the past 20 years! Each number is the product of two really, really big prime numbers. Once the number is factored, then it can no longer be used for encryption. |  |  |
| **Evaluation/Decision Point Assessment** | | **Student Outcomes** |
|  | |  |