ASEE 2022 ANNUAL CONFERENCE
Excellence Through Diversity
MINNEAPOLIS, MINNESOTA, JUNE 26TH-29TH, 2022 ASEE
Paper ID #36947

Constructing Quadratic Equations modulo N to emphasize the differences between real and modular arithmetic operations

Carlos Salazar

Visiting Professor at the United State Coast Guard Academy

Constantine Macris

Constructing Quadratic Equations modulo N to emphasize the differences between real and modular arithmetic operations

By

Carlos Salazar and Constantine Macris
U.S. Coast Guard Academy

Abstract – Cadets majoring in Cybersecurity at the United States Coast Guard Academy are typically enrolled in the department's Introductory Cryptography course during the Fall of their Junior year. Many of these students struggled to understand the need to use modular operations to solve quadratic equations modulo N. This was because homework assignments requiring the solution of these equations typically employed equations for which regular real operations were perfectly satisfactory. Quadratic equations modulo N are assigned to help the students recognize the similarities between modular and real arithmetic while also helping them see the differences. These equations are also introduced to prepare the students for the study of elliptic curves. Three specific differences between modular quadratic equations and real arithmetic quadratic equations were identified. Modular arithmetic equations can fail to have any solutions if the modulus for an otherwise acceptable equation does not permit a multiplicative inverse required for solution. Modular quadratic equations can also have solutions where real quadratic equations would fail to have any solutions (complex solutions). And finally, modular quadratic equations with composite moduli can have many more than two solutions. All three of these differences can be exploited to prevent the students from solving a quadratic equation using real arithmetic methods and thus compel them to use modular techniques. It was observed on the homework assignments that a significant fraction of the students failed to use modular techniques to solve the quadratic equations that were assigned and it was suspected that many of those that did were unsure of why they needed to employ them. After constructing quadratic equations that took advantage of the peculiar properties of modular arithmetic the students were unable to use real arithmetic techniques and had to resort to modular methods thus reinforcing the need to use those methods to solve the modular equations.

Introduction

Modular arithmetic is a staple of modern cryptography[1][4]. While Discrete Mathematics is a prerequisite for the Introduction to Cryptography course at the USCGA, students still struggle to appreciate the similarities and differences between real arithmetic and modular arithmetic. In order to help the students gain familiarity with the cryptographic applications of modular arithmetic they are given 1^{st} and 2^{nd} order congruences mod n to solve for their homework. This also readies them for introduction to elliptic curves which use 3^{rd} order congruences[3]. Unfortunately, they often eschew modular methods of solving the 2^{nd} order congruences preferring to fall back on other methods of solving quadratic equations with which they have greater familiarity. This can lead them to miss solutions or not appreciate the modular nature of the 2^{nd} order congruences. In order to encourage the students to use modular methods to solve these types of equations we assign congruences that cannot be solved using the standard real techniques. Then when confronted with a problem where these techniques break down they must of necessity turn to modular methods to get the correct results. This paper describes techniques

for constructing 2nd order polynomial congruences mod n of the form $ax^2 + bx + c \equiv 0$ that cannot be easily solved using the standard real techniques such as graphing, factoring, completing the square, or the familiar quadratic formula $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$.

Traditional ways of solving quadratic equations

There are four typical methods for solving real quadratic equations of the form $ax^2 + bx + c \equiv 0$ [2]. These include factoring, completing the square, the quadratic formula, and graphing.

Example 1: if $x^2 + 2x + 1 = 0$, the student can factor the equation into $(x+1)(x+1) = 0$. This would result in a double root at -1.

Example 2: if $x^2 + 4x + 3 = 0$, the student can complete the square by adding 1 to both sides of the equation resulting in $x^2 + 4x + 4 = 1$. This then leads to $(x+2)^2 = 1$. Taking the square root of both sides results in $x + 2 = \pm 1$. Solving for x gives the roots -3 and -1.

Example 3: if $x^2 - x - 2 = 0$, the student can use the quadratic formula $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$ to get $x = \frac{1 \pm \sqrt{1^2-4(-2)}}{2} = (1 \pm 3)/2$. This results in roots at 2 and -1.

Figure 1 contains graphs of examples 1 and 2 showing the zero crossings (roots) of each.

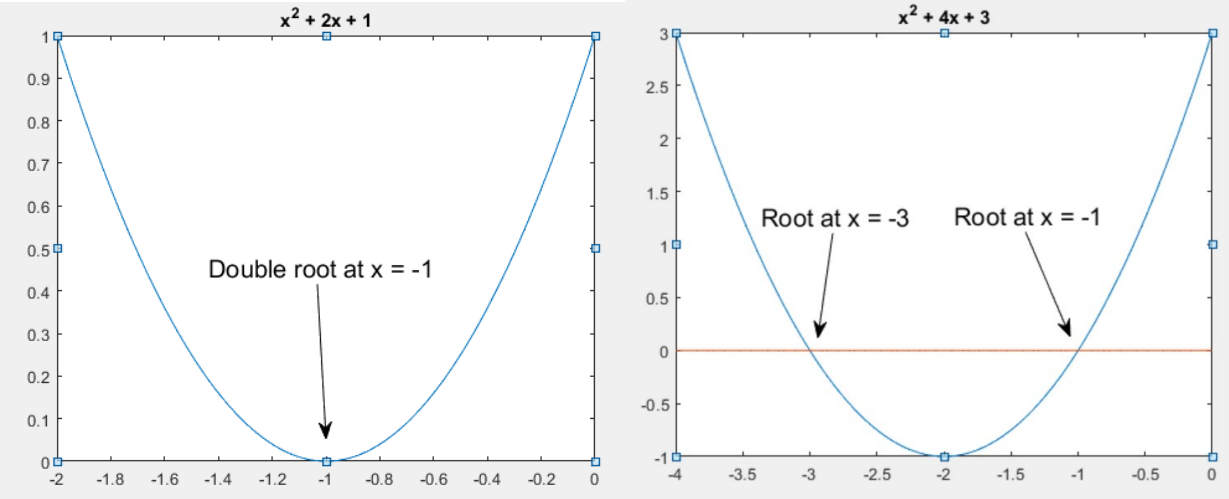

Figure 1 graphs of example quadratic equations

Using the quadratic formula to solve quadratic congruences

A popular approach to deriving the quadratic formula is to complete the square as in example 2 but using the variables a, b, and c rather than specific numbers from a particular example. The quadratic formula can in many cases be used to solve quadratic congruences as long as we use modular versions of the operations used to compute square roots, handle negative numbers by reduction modulo n and perform divisions by using multiplicative inverses. It should be noted

that congruences mod a composite n are not subject to the Fundamental Theorem of Algebra and by proper choice of n many more than 2 roots can be obtained. These additional roots will be obtained when solving for the square roots of the discriminant. This is because the procedure for solving for square roots involves factoring the modulus n, solving for the square roots mod each of the factors, and then recombining the results using the Chinese Remainder Theorem [4]. Alternatively, when n is small an exhaustive search can yield all the possible square roots mod n. This can, and often does, result in many more solutions to a given quadratic congruence. Let us revisit the first example with a mod of 9 using the quadratic formula.

Example 1 mod 9 using the quadratic formula and replacing the operations with their modular counterparts.

$x^2 + 2x + 1 \equiv 0 \bmod 9$

Step 1 write out the quadratic formula

$x = \frac{-2 \pm \sqrt{2^2 - 4(1)}}{2} = x = \frac{-2 \pm \sqrt{0}}{2}$

Step 2 solve the equation $d^2 \equiv 0 \bmod 9$. An exhaustive search of the 9 possibilities results in $d \equiv 0, 3, 6$. Which is two more solutions than the single real solution of 0.

Step 3 identify the multiplicative inverse of 2 mod 9. This can be accomplished in a variety of ways by the student who has been introduced to these techniques by this point in the course[1][4][6]. The multiplicative inverse of 2 mod 9 is 5 (i.e., $2*5 = 10 \equiv 1 \bmod 9$). The resulting formula is $5(-2 \pm d) \bmod 9$.

Step 4 substitute the different values of d into the above equation and reduce them mod 9.

$5(-2+0) \equiv -10 \equiv 8 \bmod 9$

$5(-2+3) \equiv 5 \bmod 9$

$5(-2+6) \equiv 20 \equiv 2 \bmod 9$

Note that by choosing a composite n (in this case n = 9) we were able to create a congruence with three solutions vice the single (or rather double) root of the real quadratic equation!

Constructing congruences to impede the traditional solution techniques

Case 1 – factoring. If we restrict the leading coefficient a to be equal to 1 in the quadratic congruences that we construct we can make use of the Integral Root Theorem (a special case of the Rational Root Theorem) [5] which states that the rational roots p/q of a given polynomial

$$a_n x^n + a_{n-1} x^{n-1} + \ldots a_1 x + a_0 = 0$$

with leading coefficient a_n and constant coefficient a_0 must satisfy the conditions that $q \mid a_n$ and $p \mid a_0$. Here the expression $q \mid a$ signifies that q can be divided evenly into a with no remainder. With $a_n = 1$ the only integer that divides 1 is 1 and hence the only integer roots that satisfy the real solution of the given quadratic equation/congruence will be the factors of a_0 (i.e. c in the equation $x^2 + bx + c$). It will suffice therefor to factor the term c and check each of these factors to see if they are a solution to the quadratic equation. If they are not, then factoring the equation will not work. It should be noted that if the equations are constructed to produce a negative discriminant it will also be impossible to factor the equation since no real roots exist.

Case 2 – Completing the square. In order to complete the square an integer value must result from computing the term $(b/2a)^2$. If we are restricting a to be equal to 1, this means that b must be odd. If it is desired to have an a that is not equal to 1, then this expression must be computed and must result in a non-integer value. Again if the discriminant of the equation is negative, completing the square will not result in an expression with real roots.

	A	B	C	D	E	F	G	H	I	J
1	n	21	2			a	1			
2	0	13				b	7			
3	1	0				c	13			
4	2	10				d	-3		negative	
5	3	1				d mod n	18		not a perfect square	
6	4	15				(b/2a)^2	12.25		non integer	
7	5	10								
8	6	7								
9	7	6								
10	8	7								
11	9	10								
12	10	15								
13	11	1								
14	12	10								
15	13	0								
16	14	13								
17	15	7								
18	16	3								
19	17	1								
20	18	1								
21	19	3								
22	20	7								
23	21	13								
24										

Figure 2 Spreadsheet used to help satisfy conditions for impeding traditional solution techniques

Case 3 – Graphing. In order to prevent a student from graphing solutions to the given quadratic congruence it suffices to make the discriminant negative. This will result in two complex roots which cannot be graphed (i.e., the resulting graph of the equation will not intersect the x axis).

Case 4 – Quadratic Formula using real operations. Given that the discriminant of our quadratic congruences is negative we need to ensure that the modular reduction of the discriminant is not a perfect square. Otherwise the student will be able to execute a single modular reduction and take the positive and negative square roots of the perfect square and continue on with real operations to solve the given congruence.

Case 5 – Real methods produce at most two distinct real roots. Use of a composite n can produce multiple integer roots/solutions to a given quadratic equation. In fact, congruences can be found

that satisfy the first four cases and then different moduli can be chosen that will result in completely different sets of roots (both number and content).

To assist in generating suitable equations a spreadsheet can be used. See Figure 2. Note that cell G4 in the spreadsheet contains the computation of the discriminant. Cells G1 through G3 contain the coefficients a, b, and c, respectively of the equation/congruence $ax^2 + bx + c \equiv 0$. Cell G5 holds the modular reduction of the discriminant. It should be verified that this is not a perfect square. Cell G6 holds the result of the computation of the term $(b/2a)^2$. This should be a non-integer to ensure that the completion of the square cannot be carried out.

Results

Students were assigned the following quadratic congruence for their homework and asked to solve it modulo 769 using only modular arithmetic operations.

$$3x^2 + 21x + 36 \equiv 0 \bmod 769$$

769 is a prime number so there are at most 2 roots. The discriminant is positive and a perfect square. The term $(b/2a)^2$ is a non-integer. A graph of the equation is in Figure 3 below.

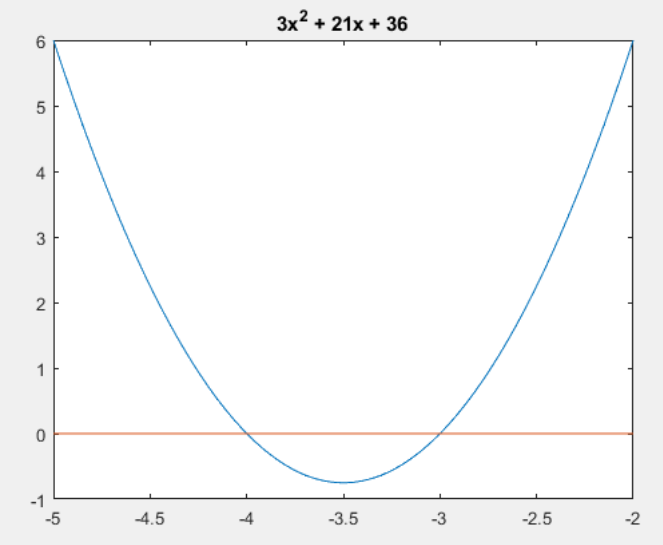

Figure 3 Graph of the homework problem initially assigned

Due to the nature of this congruence the students had factoring, graphing, and the quadratic formula (without the need for modular operations) available to solve it. Of the 21 students in the class, 14 correctly solved the congruence using modular methods to compute the square root, modular reduction of negative numbers, and the multiplicative inverse of 6 mod 769 (i.e., 641) to perform the division. The other students took various shortcuts or failed to complete the problem. One student solved the problem by factoring first and then reducing the resulting negative integers to the correct solution. Many of the students asserted incorrectly that there were only

two roots for the square root expression (which was true in this case with a prime modulus but not true in general for a composite modulus).
Homework feedback was provided to the students highlighting the need to use modular methods, and stressing that a composite modulus could result in more than 2 solutions to a given quadratic congruence. The role of the CRT in solving the square root problem mod a composite modulus was also emphasized.
For the final exam, the students were assigned the following congruence mod 51, a composite modulus that resulted in four solutions $x \equiv 5, 22, 26, 43$.

$$x^2 + 3x + 11 \equiv 0 \bmod 51$$

Of the 15 students who took the final exam, 8 did the problem correctly using modular methods, and found all 4 roots. Previously seven of these eight had correctly completed the homework but one had not used the multiplicative inverse. Four did not finish the problem. Of these four, one had previously done the homework correctly, one had failed to finish the first time also, the other two had not used the multiplicative inverse to solve the homework. The final three all got at least one root but less than all four. Two of them had used real methods on their previous homework and one had completed the homework correctly. It appears that two of the students had not understood the assignment completely when they did the homework and were unable to properly solve the congruence using modular methods on the exam. One of the students had failed to do the homework assignment correctly but learned from the given feedback and completed the exam problem properly. Five of the students did not complete the homework correctly and also failed to complete the problem on the final exam. See Table 1 below for a summary.

Number	Homework	Final Exam
8	7 correct, 1 DNU Mult Inv	8 correct
4	1 correct, 2 DNU Mult Inv, 1 DNF	4 DNF
3	1 correct, 2 real methods	3 missed several roots

Table 1 Results of quadratic congruence harder solve using real methods & adding solutions

Conclusions and further work

We have shown how to construct 2nd order polynomials equations mod n that are harder to solve using real methods and that have an arbitrary number of solutions. When compared to naively constructed quadratic congruences that can be solved using a variety of real methods these congruences can identify deficiencies in students' understanding of the modular methods needed to solve quadratic congruences. These methods include reducing integers mod n, using multiplicative inverses in place of division, and properly solving for all the solutions to the square root mod composite n problem. Prior to this pedagogical innovation students often struggled to use modular methods when computing the solution to 2nd order polynomials blindly using the quadratic formula, completing the square, or factoring while not considering or using modular methods. After assigning equations that had been constructed to not allow this, more students were able to correctly solve these types of problems on the final exam and we were able

to identify those students who still failed to grasp the required modular techniques. Going forward we will be assigning these especially constructed equations in the homework from the beginning in order to prevent students using real methods and getting the correct answers for the wrong reasons. The need to find more than two roots is especially important as it highlights an important distinction between real quadratic equations and quadratic congruences mod a composite n.

References

1. W. Trappe, L. Washington, “Introduction to Cryptography with Coding Theory,” Pearson, 2003.
2. B. Rich, P. Schmidt, “Shaum’s Outline of Theory and Problems of Elementary Algebra” The McGraw-Hill Companies, 2004
3. H. Cohen, “A Course on Computational Number Theory,” Springer-Verlag, 1993.
4. A. Menezes, P. van Oorschot, and S. Vanstone,”Handbook of Applied Cryptography”, CRC Press, 1996.
5. D. Arnold, G. Arnold,”Cambridge 4 Unit Mathematics Year 12”, Cambridge University Press, 2000.
6. O. Levin, “Discrete Mathematics An Open Introduction”, Ind Published, 2018

.