# CUBIC CONGRUENCES MODULO A PRIME, CARDANO, AND THE TI-89

Joseph Fadyn
Kennesaw State University
1100 South Marietta Parkway
Marietta, Georgia 30060
jfadyn@kennesaw.edu

## INTRODUCTION: Solving Cubic Congruences Modulo a Prime—A Classic Approach

In [3], I produced a TI-89 program called cunsolm() to solve cubic congruences modulo a prime mainly using the methods of Sun's paper [5]. The focus of Sun's paper is to express solutions of cubic congruences modulo a prime in terms of recursion sequences. I used his results in my paper [3] and his methods were adequate except in one special case. Although interesting, the results in Sun's paper are neither necessarily intuitive nor easily proven (Sun's paper is about 45 pages in length). For purposes of discussion in this paper, I will use the classical method of Cardano for solving cubic equations. The merit of this method is that it is much more easily understood. Although Cardano's method is intended for solving cubic equations over the field of complex numbers, I will illustrate here how the method of Cardano can be used when the field is the integers modulo a prime pr. In our solutions we will employ the TI-89 as an aid in making certain necessary computations. We will consider the problem (standard *congruence*):

$$Ax^3 + Bx^2 + Cx + D \equiv 0 \pmod{pr}, \text{ where pr is a prime number.}$$

Of course Cardano's method addresses the solution of the standard *equation*:

$$Ax^3 + Bx^2 + Cx + D = 0.$$

The following information about Cardano's cubic equation solution method is from Wikipedia [4]:

### Cardano's Method For Cubic Equations:

The solutions can be found with the following method due to Scipione del Ferro and Tartaglia, published by Gerolamo Cardano in 1545.

We first divide the standard equation by the leading coefficient to arrive at an equation of the form

$$x^3 + ax^2 + bx + c = 0 \qquad (1).$$

The substitution $x = t - a/3$ eliminates the quadratic term, giving the so-called *depressed cubic*

$$t^3 + pt + q = 0 \qquad (2)$$

where

$$p = b - \frac{a^2}{3} \qquad \text{and} \qquad q = c + \frac{2a^3 - 9ab}{27}.$$

We introduce two variables *u* and *v* linked by the condition

$$u + v = t$$

and substitute this in the depressed cubic (2), giving

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0 \qquad (3).$$

At this point Cardano imposed a second condition for the variables *u* and *v*

$$3uv + p = 0$$

which, combined with (3) (the first parenthesis vanishes, then multiply by $u^3$ and substitute *uv*) gives

$$u^6 + qu^3 - \frac{p^3}{27} = 0\,.$$

This can be seen as a quadratic equation in $u^3$. When we solve this equation, we find that

$$u^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

and thus

$$u = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \qquad (4)$$

Since $t = v + u$, $t = x + a/3$, and $v = -p/3u$, we find

$$x = -\frac{p}{3u} + u - \frac{a}{3}.$$

Note that there are six possibilities in computing *u* with (4), since there are two possibilities for the square root ($\pm$), and three for the cubic root (the principal root and the principal root multiplied by $(\frac{-1}{2} \pm \frac{\sqrt{3}}{2}i)$. The sign of the square root however does not affect the resulting *t* (a simple calculation shows that $-p/3u = v$), although care must be taken in three special cases to avoid divisions by zero:

First, if $p = q = 0$, then we have the triple real root
$t = 0.$
Second, if $p = 0$ and $q \neq 0$, then

$$u = 0 \text{ and } v = -\sqrt[3]{q}.$$

Third, if $p \neq 0$ and $q = 0$ then

$$u = \sqrt{\frac{p}{3}} \qquad \text{and} \qquad v = -\sqrt{\frac{p}{3}},$$

in which case the three roots are

$$t = u + v = 0, \qquad t = \omega_1 u - \frac{p}{3\omega_1 u} = \sqrt{-p}, \qquad t = \frac{u}{\omega_1} - \frac{\omega_1 p}{3u} = -\sqrt{-p},$$

where

$$\omega_1 = e^{i\frac{2\pi}{3}} = -\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i.$$

**Summary:**

In summary, for the cubic equation

$$x^3 + ax^2 + bx + c = 0$$

the solutions for *x* are given by

$$x = u - \frac{p}{3u} - \frac{a}{3}$$

where

$$p = b - \frac{a^2}{3}$$

$$q = c + \frac{2a^3 - 9ab}{27}$$

$$u = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

The expression above for *u* can generate up to three values (there are three cubic roots related by a factor which is one of the two non-real cubic roots of one, and two square roots of any sign ; but these 6 expressions can generate only 3 pairs). This also applies to the final solutions for *x*.

**Cardano's Method For Cubic Congruences Modulo a Prime**

To begin our discussion of how to apply Cardano's method to solve cubic congruences modulo a prime pr, we first observe that the equation:

$$x^3 + ax^2 + bx + c = 0 \qquad (1).$$

is assumed to be monic. This is not a difficulty, since if we begin with:
$Ax^3 + Bx^2 + Cx + D \equiv 0 \pmod{pr}$, we may simply multiply this equation by the inverse of A modulo pr to obtain equation (1). Since pr is a prime and $A \neq 0$, (A,pr) = 1 so such an inverse always exists. In the substitution: $x = t - a/3$, we will interpret the division by 3 as multiplication by the inverse of 3 modulo pr and so the depressed cubic (2) is easily obtained (where we interpret the equality as a congruence modulo pr and pr is larger than 3). To be brief, the method of Cardano proceeds directly to the solution:

$$u = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \qquad (4)$$

and then: $x = -\frac{p}{3u} + u - \frac{a}{3}$. We simply need to interpret these expressions as congruences modulo pr. To reduce the amount of computation that needs to be done by hand, I have written two TI-89 programs which I list below. The first program cubdep() yields the monic cubic and the depressed cubic, and the second program carducub() finds $u^3$ :

$$u^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

```
cubdep(a0,a1,a2,a3,pr)
Prgm
ClrIO: modinv(a0,pr)->inv: mod(inv*a1,pr)->a1: mod(inv*a2,pr)->a2
mod(inv*a3,pr)->a3 :DelVar x: Display “Monic Cubic Is:”
Disp x^3+a1*x^2+a2*x+a3 = 0: Pause: Disp “Equation Stored In Variable MONIC” :
x^3+a1*x^2+a2*x+a3=0->monic: Pause: modinv(3,pr)->tin: DelVar p,q,t:
mod(a2-a1^2*tin,pr)->p:modinv(27,pr)->tsvnin:mod(a3+2*a1^3*tsvnin-a1*a2*tin,pr)-
>q
Disp “p=”: Disp p: Pause: Disp “q=:” Disp q: Pause: Disp “Depressed Cubic Is:”
Disp t^3+p*t+q = 0: Disp “Depressed Cubic Stored as DEP”: t^3+p*t+q=0->DEP
EndPrgm
```

This program calls the program modinv() which finds inverses modulo n and whose listing appears in [2].

```
carducub(p,q,pr)
Prgm
DelVar ucubed
If mod(p,pr)=0 Then: 0->ucubed: Goto stp2: EndIf
If mod(p,pr) ≠ 0 and mod(q,pr)=0 Then: √(mod(p*modinv(3,pr),pr))->u: Disp “u=”:
Disp u: Stop: EndIf
mod(-q*modinv(2,pr),pr)+√(mod(q^2*modinv(4,pr)+p^3*modinv(27,pr),pr))->ucubed
Lbl stp2
Disp “u cubed is:” : Disp ucubed
EndPrgm
```

We also see that it will be necessary to extract square roots and cube roots modulo a prime pr. The TI-89 programs sqrtmdp() and curtmdp() which are listed in my paper [3] can be used for this purpose. Let’s begin with a simple example:

Example 1: $x^3 - 72x^2 + 54x + 14 \equiv 0 \pmod{89}$.

First we find the depressed cubic: cubdep(1,-72,54,14,89) yields:

$t^3 + 17t + 6 \equiv 0 \pmod{89}$.

Next we employ: carducub(17,6,89) which yields:

$u^3 \equiv 86 + \sqrt{(69)} \pmod{89}$

Now sqrtmdp(69,89) yields the two square roots of 69 mod 89, which are 43 and 46. Using either root will produce the same results. Therefore:

$u^3 \equiv 86 + 43 \equiv 40 \pmod{89}$.

Next, we require $\sqrt[3]{40} \pmod{89}$. For this we use: curtmdp(40,89) which yields one cube root: 42 (mod 89). Therefore, u ≡ 42 (mod 89). Next, we use:

$$x = u - \frac{p}{3u} - \frac{a}{3}$$

$$x \equiv -\frac{17}{(3 \cdot 42)} + 42 - \frac{(-72)}{3} \pmod{89}$$

Using the TI-89 we have: modinv(3,89) =30 and modinv(42,89) =53 so that:
x ≡ -17*30*53 + 42 + 24 ≡ 3 (mod 89). It is easily verified that this solution is correct by substitution into the original congruence. As an option, we may use my TI-89 program cunsolm() from [3] to verify: cunsolm(1, -72, 54, 14, 89) , which produces the output: "One Solution. It Is:" 3.

Example 2: $2x^3 - 30x^2 + 162x - 350 \equiv 0 \pmod{1237}$.

We employ: cubdep(2, -30, 162, -350, 1237) to obtain the monic cubic:
$x^3 + 1222x^2 + 81x + 1062 \equiv 0 \pmod{1237}$. Observe, therefore that a = 1222. The depressed cubic is: $t^3 + 6t + 1217 \equiv 0 \pmod{1237}$. Next, carducub(6, 1217, 1237) yields: $u^3 \equiv 10 + 6\sqrt{(3)} \pmod{1237}$. Now, sqrtmdp(3, 1237) produces the two square roots of 3 mod 1237, which are 341 and 896. We use 341 to obtain:
$u^3 \equiv 10 + 6(341) \equiv 819 \pmod{1237}$. Now, curtmdp(819, 1237) gives three cube roots: 1166, 342, and 966. Therefore u = 1161, 342, or 966 (mod 1237). Now we employ:

$$x = u - \frac{p}{3u} - \frac{a}{3}$$

Using the TI-89, this corresponds to:
x ≡ -p*modinv(3u,pr) + u – a*modinv(3,pr). Using each value of u in turn, we get:

If u = 1166, x ≡ -6*modinv(3*1166,1237) + 1166 -1222*modinv(3,1237), or
x ≡ -6*1086 + 1166 -1222*825 (mod 1237) ≡ 840 (mod 1237).

If u = 342, then x ≡ -6*modinv(3*342,1237) + 342 -1222*modinv(3,1237), or
x ≡ -6*469 + 342 -1222*825 (mod 1237) ≡ 7 (mod 1237).

If u = 966, then x ≡ -6*modinv(3*966,1237) + 966 -1222*modinv(3,1237), or
x ≡ -6*919 + 966 -1222*825 (mod 1237) ≡ 405 (mod 1237).

So our solutions modulo 1237 are: x ≡ 840, 7, 405 (mod 1237). A direct check in the original congruence is simple. As an alternative, consider:
cunsolm(2, -30, 162, -350, 1237) , which produces: “The Three Roots Are:” 840, 405, 7 as expected.

Example 3: $x^3 - 15697x^2 + 13412x + 23995 \equiv 0 \pmod{764587}$.

We have: cubdep(1, -15697, 13412, 23995, 764587) which produces the depressed cubic:
$t^3 + 711734t + 295907 \equiv 0 \pmod{764587}$. Next, carducub(711734, 295907, 764587) yields: $u^3 \equiv 234340 + \sqrt{(262114)} \pmod{764587}$. Now, sqrtmdp(262114,764587) gives the two square roots of 262114 modulo 764587, which are 732754 and 31833. Therefore: $u^3 \equiv 234340 + 31833 \pmod{764587} \equiv 266173 \pmod{764587}$. Finally, curtmdp(266173, 764587) gives: “No Cube Root Exists”. Therefore, this congruence has no solution. We may verify by using: cunsolm(1, -15697, 13412, 23995, 764587), which yields: “NO SOLUTION”.

A difficulty which can arise in solving cubic congruences by Cardano’s method is that in the expression for $u^3$ :

$$u^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

The square root may not exist modulo the prime pr. In our three examples above, this did not occcur, but it is certainly possible. When the square root does not exist modulo pr, we may still attempt to find u by extracting cube roots in the field $Z/(pr^2Z)$. For this we use the algorithm referred to in my paper [3] for finding roots in finite fields. The program we need from [3] is rrotinfg(c,d,e,r,pr) which finds (with r=3) the cube roots of $c+e\sqrt{(d)}$ in the field $GF(pr^2)$, the Galois field of order $pr^2$ , if they exist.

Example 4: $x^3 + 56342x^2 – 123456x – 234515 \equiv 0 \pmod{345769}$.

We use cubdep(1, 56342, -123456, -234515, 345769) to obtain the depressed cubic:
$t^3 + 250388t + 144338 \equiv 0 \pmod{345769}$. Next, carducub(250388, 144338, 345769) gives: $u^3 \equiv 273600 + 13\sqrt{(537)}$ We employ: sqrtmdp(537, 345769) which yields “No Root Exists”, so that $\sqrt{(537)}$ does not exist modulo 345769. Next we have:
rrotinfg(273600, 537, 13, 3 , 345769). This gives three cube roots:
$u_1$ = [105585, 89228], which represents $105585 + 89228\sqrt{(537)} \pmod{345769}$
$u_2$ = [329697, 192923], which represents $329697 + 192923\sqrt{(537)} \pmod{345769}$
$u_3$ = [256256, 63618], which represents $256256 + 63618\sqrt{(537)} \pmod{345769}$.
To check that these are the cube roots we desire, we can use the program
mdexpi(a, b, c, e, n) which finds $(a + c\sqrt{(b)})^e \pmod{n}$ using a form of modular exponentiation. We have:
mdexpi(105585,537,89228,3,345769) = [273600, 13] ,
mdexpi(329697, 537, 192923, 3, 345769) = [273600, 13] ,

mdexpi(256256, 537, 63618, 3, 345769) = [273600, 13] .
So all of $u_1$ , $u_2$ , and $u_3$ represent correct cube roots of 273600 + 13√(537) (mod 345769).
Now, x ≡ -p/(3u) + u – a/3 (mod pr). For $u_1$ = 105585 + 89228√(537) , we obtain for x:

$$x \equiv -\frac{250388}{3\cdot\left(105585+89228\sqrt{537}\right)} + 105585 + 89228\sqrt{537} - \frac{56342}{3} \pmod{345769}$$

$$x \equiv \frac{\left(-250388\cdot\left(89228\sqrt{537}-105585\right)\right)}{12792750993549} + 105585 + 89228\sqrt{537} - (56342)\cdot modinv(3, 345769)$$

$$x \equiv \frac{\left(243471\cdot\sqrt{537}+65009\right)}{250388} + 105585 + 89228\sqrt{537} - (56342)\cdot(230513)$$

$$x \equiv \left(243471\sqrt{537}\right) + 65009\right)\cdot 221561 + 105585 + 89228\sqrt{537} + 317317$$

$$x \equiv 256541\sqrt{537} + 105585 + 89228\sqrt{537} + 317317$$

$$x \equiv 0\cdot\sqrt{537} + 77133 \equiv 77133 \pmod{345769}.$$

So a solution is x ≡ 77133 (mod 345769) .

As we can see, the amount of computation required to find x once u is known is substantial. Here is a short TI-89 program which will aid in this computation. If u = c + d√(e), and a and p are as before, we have:

```
cubicx(p,a,c,d,e,pr)
Prgm
modinv(3,pr)->tin
mddiv(mod(-p*tin,pr),0,c,d,e,pr)
Disp "x="
Disp mod(c+did[1,1]+mod(-a*tin,pr),pr)+mod(d+did[1,2],pr)* √(e)
EndPrgm
```

For example, for $u_1$, we have cubicx(250388,56342,105585,89228,537,345769) which gives $x_1$ ≡ 77133 (mod 345769).
For $u_2$ we have cubicx(250388,56342,329697,192923,537,345769) which gives
$x_2$ ≡ 129305 √(537) + 106147 (mod 345769).
For $u_3$ we have cubicx(250388,56342,256256,63618,537,345769) which gives
$x_3$ ≡ 216467 √(537) + 106147 (mod 345769).
Of course the values of x produced by $u_2$ and $u_3$ do not correspond to values in Z/(345769Z). So the congruence has only one solution, x ≡ 77133 (mod 345769). It is interesting to note, however, that on the TI-89 if we define:
$x^3 + 56342x^2 – 123456x – 234515$ -> f(x) , then:

$f(x_2) \equiv f(129305\ \sqrt{(537)} + 106147) \equiv 0 \pmod{345769}$, and
$f(x_3) \equiv f(216467\ \sqrt{(537)} + 106147) \equiv 0 \pmod{345769}$ .
Therefore $x_2$ and $x_3$ represent solutions of the cubic congruence over the field $GF(345769^2)$.
We may verify that only one solution exists in Z/(345769Z) by using:
cunsolm(1, 56342, -123456, -234515, 345769) which produces:
"ONE SOLUTION. IT IS:" 77133.

Example 5: $x^3 - 187x^2 + 6412x - 2395 \equiv 0 \pmod{13001}$.

We use cubdep(1,-187,6412,-2395,13001) to obtain the depressed cubic:
$t^3 + 3423t + 5834 \equiv 0 \pmod{13001}$. Next, carducub(3423,5834,13001) yields:
$u^3 \equiv 10084 + 10\ \sqrt{(102)} \pmod{13001}$. We use sqrtmdp(102,13001) to see that "No Root Exists", so $\sqrt{(102)}$ does not exist mod 13001. We use rrotinfg(10084,102,10,3,13001) to obtain the outputs:
$u_1$ = [56, 12963], which represents $56 + 12963\ \sqrt{(102)} \pmod{13001}$,
$u_2$ = [12386, 5354], which represents $12386 + 5354\ \sqrt{(102)} \pmod{13001}$, and
$u_3$ = [559, 7685], which represents $559 + 7685\ \sqrt{(102)} \pmod{13001}$.
To check these cube roots we employ:
mdexpi(56,102,12963,3,13001) = [10084,10]
mdexpi(12386,102,5354,3,13001) = [10084,10]
mdexpi(559,102,7685,3,13001) = [10084,10].
To find the solutions x, we observe that a = -187 and p = 3423 and we use:
$x_1$ = cubicx(3423, -187, 56, 12963, 102, 13001) $\equiv$ 4508 (mod 13001)
$x_2$ = cubicx(3423, -187, 12386, 5354, 102, 13001) $\equiv$ 3166 (mod 13001)
$x_3$ = cubicx(3423, -187, 559, 7685, 102, 13001) $\equiv$ 5514 (mod 13001).
It is easily verified that these solutions check in the original congruence. We may also verify by running: cunsolm(1, -187, 6412, -2395, 13001) to obtain the output: "Three Solutions", "One Solution Is" 3166. "Other Solutions Are:" 4508 , 5514.

Example 6: $x^3 + 5894x^2 + 98234x - 48594 \equiv 0 \pmod{2785649}$.

We use cubdep(1, 5894, 98234, -48594, 2785649) to get the depressed cubic:
$t^3 + 1518184t + 2325314 \equiv 0 \pmod{2785649}$.
Next, carducub(1518184, 2325314, 2785649) yields:
$u^3 \equiv 1622992 + 5\ \sqrt{(6842)} \pmod{2785649}$. Next, sqrtmdp(6842, 2785649) produces "No Root Exists", so that $\sqrt{(6842)}$ does not exist mod 2785649. To continue, we employ:
rrotinfg(1622992, 6842, 5, 3, 2785649) which indicates that "No Root Exists". Therefore, since there is no cube root of $u^3 \equiv 1622992 + 5\ \sqrt{(6842)}$ in the field $GF(2785649^2)$, u does not exist and so the original congruence has no solution. This is verified by cunsolm(1, 5894, 98234, -48594, 2785649) which yields "NO SOLUTION".

Next we will consider an example of each of the three special cases mentioned in the article.

Special Case #1: First, if $p = q = 0$, then we have the triple real root: t=0

Example 7: $x^3 + 1544x^2 + 2266x + 8 \equiv 0 \pmod{2683}$.
We have cubdep(1, 1544, 2266, 8, 2683) which yields: p =0, q = 0, so the depressed cubic is: $t^3 \equiv 0 \pmod{2683}$, and so $t \equiv 0 \pmod{2683}$. To obtain x, we use:
$x \equiv t - a/3 \pmod{pr}$, so that $x \equiv 0 - 1544*\text{modinv}(3,2638) \equiv -1544*1789 \pmod{2683}$.
Therefore, $x \equiv -2762216 \equiv 1274 \pmod{2683}$. Note that this value of x is a root of multiplicity three. This is verified by using cunsolm(1, 1544, 2266, 8, 2683), which yields: "There is a Triple Root. It Is:" 1274 .

Special Case #2: Second, if $p = 0$ and $q \neq 0$, then

$$u = 0 \text{ and } v = -\sqrt[3]{q}.$$

Example 8: $x^3 + 119x^2 + 597x + 1132 \equiv 0 \pmod{1237}$.

Now, cubdep(1, 119, 597, 1132, 1237) yields: p = 0, q = 248 with depressed cubic:
$t^3 + 248 \equiv 0 \pmod{1237}$. At this point it is instructive to use: carducub(0, 248, 1237) which yields $u^3 \equiv 0 \pmod{1237}$ so that $u \equiv 0 \pmod{1237}$. This means of course that we cannot recover x by using:

$$x = -\frac{p}{3u} + u - \frac{a}{3}.$$

because of division by zero. The article asserts that $v = -\sqrt[3]{q}$
and so since t = u + v we infer that $t = v = -\sqrt[3]{q}$ .
And indeed, we see that from our equation: $t^3 + 248 \equiv 0 \pmod{1237}$, we have:
$t^3 \equiv -248 \pmod{1237}$, so that $t \equiv -\sqrt[3]{q} \pmod{pr} \equiv \sqrt[3]{-248} \equiv \sqrt[3]{989} \pmod{1237}$.
We use curtmdp(989, 1237) which indicates that "No Cube Root Exists", so the original congruence has no solution. This is verified by cunsolm(1, 119, 597, 1132, 1237), which gives "NO SOLUTION".

Special Case #3: Third, if $p \neq 0$ and $q = 0$ then

$$u = \sqrt{\frac{p}{3}} \qquad \text{and} \qquad v = -\sqrt{\frac{p}{3}},$$

in which case the three roots are

$$t = u + v = 0, \qquad t = \omega_1 u - \frac{p}{3\omega_1 u} = \sqrt{-p}, \qquad t = \frac{u}{\omega_1} - \frac{\omega_1 p}{3u} = -\sqrt{-p},$$

where

$$\omega_1 = e^{i\frac{2\pi}{3}} = -\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i.$$

Example 9: $x^3 + 236x^2 + 1463x + 3758 \equiv 0 \pmod{4567}$.

We use cubdep(1, 236, 1463, 3758, 4567) to obtain p = 2688, q = 0 so the depressed cubic is: $t^3 + 2688t \equiv 0 \pmod{4567}$. The simplest way to proceed is to factor the left hand side of this congruence to obtain: $t*(t^2 + 2688) \equiv 0 \pmod{4567}$, which results in: $t \equiv 0 \pmod{4567}$ or $t^2 \equiv -2688 \pmod{4567}$. At this point we observe that the three solutions predicted by the article are t = 0, t = √(-p) and t = -√(-p), and we can see above that this is indeed the case. To continue, we note that –2688 ≡ 1879 (mod 4567), and that sqrtmdp(1879, 4567) gives 1415 and 3152 as the two square roots of 1879 mod 4567. Therefore we obtain: t ≡ 0 , t ≡ 1414, and t ≡ 3152 (mod 4567). To recover x, we use
x = t – a/3 where a = 236 and $3^{-1} \equiv$ modinv(3, 4567) ≡ 3045 (mod 4567).
For t = 0, x ≡ 0 – (3045)*(236) ≡ 2966 (mod 4567).
For t = 1415, x ≡ 1415 – (3045)*(236) ≡ 4381 (mod 4567).
For t = 3152, x ≡ 3152 – (3045)*(236) ≡ 1551 (mod 4567).
These three solutions check in the original congruence. In addition, these results are verified by cunsolm(1, 236, 1463, 3758, 4567), which produces: “THREE SOLUTIONS. One Solution Is:” 4381. “Other Solutions Are:” 1551, 2966.

It is interesting to note in the final example above that the alternate solutions for t,

$$t = \omega_1 u - \frac{1}{3}\frac{p}{\omega_1 u} \qquad t = \frac{u}{\omega_1} - \frac{1}{3}\frac{\omega_1 p}{u}$$

where

$$\omega_1 = e^{i\frac{2\pi}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i.$$

can also be used to produce values of t, t ≡ 1414, and t ≡ 3152 (mod 4567), but with considerably more computational effort than using t = √(-p) and t = -√(-p) as we did in Example 9 above.

*References*


1. E. Bach and J. Shallit, *Algebraic Number Theory*, *Volume 1*, The MIT Press, 1996.
2. J.N. Fadyn, *Solving Quadratic Congruences Modulo a Prime on The TI-89*, Proceedings of the ICTCM 2010.
3. J. N. Fadyn, *Solving Cubic Congruences Modulo a Prime on the TI-89*, Proceedings of the ICTCM 2011.
4. Wikipedia: http://en.wikipedia.org/wiki/Cubic_function#Cardano.27s_method
5. Z.H. Sun, *Cubic and Quartic Congruences Modulo A Prime*, Journal of Number Theory, 102, No. 1, 41-89 (2003).