SOLVING QUARTIC CONGRUENCES MODULO A PRIME ON THE TI-89

Joseph Fadyn
Southern Polytechnic State University
1100 South Marietta Parkway
Marietta, Georgia 30060
jfadyn@spsu.edu

INTRODUCTION

We consider the problem of solving the quartic congruence:

$$Ax^4 + Bx^3 + Cx^2 + Dx + E \equiv 0 \pmod p \qquad (1)$$

where p is a prime greater than 3 using the TI-89. We assume that p does not divide A, for otherwise the congruence reduces to $Bx^3 + Cx^2 + Dx + E \equiv 0 \pmod p$, which is cubic. Cubic congrences are discussed in my paper "Solving Cubic Congruences Modulo a Prime On The TI-89" [2] which appears in the Proceedings of the ICTCM 2011. To solve the quartic congruence, we will follow the method of Zhi-Hong Sun as discussed in his paper "Cubic and Quartic Congruences Modulo a Prime" [3] (Journal of Number Theory, 2003). First, we observe that the quartic congruence has 0, 1, 2 or 4 solutions (unless roots are repeated). To begin, by multiplying (1) by the inverse of A mod p, we may assume that the quartic is monic, of the form: $f(x) = x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 \equiv 0 \pmod p$. Quoting from Sun [3] (p. 37) we have:

For the general quartic polynomial $x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$ let

$$a = a_2 - \frac{3a_1^2}{8}, \quad b = a_3 - \frac{a_1a_2}{2} + \frac{a_1^3}{8}, \quad c = a_4 - \frac{a_1a_3}{4} + \frac{a_1^2a_2}{16} - \frac{3a_1^4}{256}$$

and $y = x + a_1/4$. Then we find

$$x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = y^4 + ay^2 + by + c.$$

So we only need to study the congruence $x^4 + ax^2 + bx + c \equiv 0 \pmod p$.

We will refer to the congruence $y^4 + ay^2 + by + c \equiv 0 \pmod p$ as the "depressed quartic." We now begin the coding of our main TI-89 program quarsom(_) which will solve a quartic congruence modulo a prime p:

```
quarsom(bot,bit,b2t,b3t,b4t,p)
Prgm
modinv(bot,p)->bin: mod(bin*b1t,p)->b1: mod(bin*b2t,p)->b2: mod(bin*b3t,p)->b3
mod(bin*b4t,p)->b4: quarta(b1,b2,p)->aq: quartb(b1,b2,b3,p)->b1
quartc(b1,b2,b3,b4,p)->cq :
```

In this code, In this code, modinv(a,m) finds the inverse of a modulo m (see [1]), and quarta, quartb and quartc are functions which find the coefficients a, b, and c in the depressed quartic $y^4 + ay^2 + by + c \equiv 0 \pmod p$ and are defined as follows:

```
quarta(b1,b2,p): mod(b2-3*modinv(8,p)*b1^2,p)
quartb((b1,b2,b3,p): mod(b3-modinv(2,p)*b1*b2+modinv(8,p)*b1^3,p)
quartc(b1,b2,b3,b4,p):mod(b4-modinv(4,p)*b1*b3+modinv(16,p)*b1^2*b2-
3*modinv(256,p)*b1^4,p)
```

Next, Sun defines:

$$D(a,b,c) = -(4a^3 + 27b^2)b^2 + 16c(a^4 + 9ab^2 - 8a^2c + 16c^2).$$

Then we have from [3]:

Lemma 5.1. *Let p be an odd prime, and $a,b,c \in \mathbb{Z}$ with $p \nmid b$. Then the congruence $x^4 + ax^2 + bx + c \equiv 0 \pmod p$ has one multiple solution if and only if $D(a,b,c) \equiv 0 \pmod p$.*

There follows from [3]:

Remark 5.1. If $p > 3$ is a prime, $a,b,c \in \mathbb{Z}$, $p \nmid b$ and $p \mid D(a,b,c)$, one can verify that the congruence $x^4 + ax^2 + bx + c \equiv 0 \pmod p$ has the following multiple solution:

$$x \equiv \begin{cases} -\frac{3b}{4a} \pmod p & \text{if } 2a^3 - 8ac + 9b^2 \equiv 0 \pmod p, \\ -\frac{(a^2+12c)b}{2a^3-8ac+9b^2} \pmod p & \text{if } 2a^3 - 8ac + 9b^2 \not\equiv 0 \pmod p. \end{cases}$$

So if $D(a,b,c) \equiv 0 \pmod p$, we have a multiple root, say x^*. Then we are assured that: $(x-x^*)^2 = x^2 + 2xx^* + (x^*)^2$ is a factor of $x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 \pmod p$. So we may obtain the other (quadratic) factor by division modulo p. We continue our coding of quarsom() as follows:

```
modinv(4,p)->tin: If qdisc(aq,bq,cq,p)=0 and mod(bq,p) ≠0 Then:
mod(2*aq^3-8*aq*cq+9*bq^2,p)->kp: If kp = 0 Then mod(-3*bq*tin*modinb(aq,p),p)
mod(-3*bq*tin*modinv(aq,p),p)-> tmp: Else :
mod(-(aq^2+12*cq)*ba*modinv(kp,p),p)-> tmp : EndIf: Disp "A Repeated Root
Exists": Pause: pdivmdp([[1,0,aq,bq,cq]],[[1, mod(-2*tmp,p),mod(tmp^2,p]],p):
x^2+q[1,2]*x+q[1,3]->f(x): qucon(p): If norots=0 Then mod(tmp-tin*b1,p)->rt[1]: Disp
"Roots Are:" Disp rt[1],rt[1]: Go to stpe: EndIf: If norots=1 Then:
mod(rt[1]-tin*b1,p)->rt[2] : Disp "Roots Are:" : Disp rt[1],rt[1],rt[2],rt[2]: Go to stpe:
EndIf: If norots=2 Then: mod(rt[1]-tin*b1,p)->rt[1]: mod(rt[2]-tin*b1,p)->rt[2]:
mod(tmp-tin*b1,p)-> rt[3]: Disp "Roots Are:" : Disp rt[3], rt[3], rt[1], rt[2] : Go to stpe:
EndIf: EndIf:
```

In this code, qucon(p) is a quadratic congruence solver (see [1]), pdivmdp() does polynomial division modulo p (see [2]), and TI-89 function qdisc() finds D(a,b,c) and is defined as follows:

```
qdisc(aq,bq,cq,p):mod((-4*aq^3+27*bq^2)*bq^2+16*ca*(aq^4+9*aq*bq^2-
8*aq^2*cq+16*cq^2),p)
```

Next we consider the case when b ≡ 0 (mod p). In this case our quartic is biquadratic: $x^4 + ax^2 + c \equiv 0 \pmod{p}$, which we may solve for x^2 using qucon(p) and then solutions are the square roots of x^2 modulo p (if they exist). We continue coding quarsom():

```
aq->aqh: cq->cqh: If mod(bq,p)=0 Then: DelVar x,f: x^2+aqh*x+cqh->f(x):
modinv(4,p)->fin: qcon(p): If norots=0 Then: Disp "Quartic Has No Solution":
0->norots: Goto stpe: EndIf: If norots=1 Then: sqrtmdp(rt[1],p) : If numrots=0 Then:
sqrtmdp(rt[1],p): If numrots =0 Then: Disp "Quartic Has No Solution": 0->norots:
Goto stpe: EndIf: If numrots=1 Then: Disp "Quartic Has One Solution":
mod(rot[1]-fin*b1,p)->rt[1]: Disp rt[1]: Disp "Root is 4-fold": 1->norots: Goto stpe:
EndIf: If numrots = 2 Then: Disp "Quartic Has Two Solutions":
mod(rot[1]-fin*b1,p)->rt[1] : mod(rot[2]-fin*b1,p)->rt[2]: Disp rt[1]: Disp rt[2]: Disp
"Roots are 2-fold": 2->norots: Goto stpe: EndIf: EndIf: If norots=2 Then:
sqrtmdp(rt[1],p): If numrots=0 Then: sqrtmdp(rt[2],p): If numrots =0 Then: Disp
"Quartic Has No Solution": 0->norots: Goto stpe: EndIf: If numrots=1 Then: Disp
"Quartic Has One Solution: mod(rot[1]-tin*b1,p)->rt[1]: Disp rt[1]: Disp "Root is 2-
fold": 1->norots: Goto stpe: EndIf: If numrots=2 Then: Disp "Quartic Has 2 Solutions":
mod(rot[1}-fin*b1,p)->rt[1]: mod(rot[2]-fin*b1,p)->rt[2]: Disp rt[1]: Disp rt[2]: 2-
>norots: Goto stpe: EndIf: EndIf: If numrots = 1 Then: mod(rot[1]-fin*b1,p)->rt[1]:
sqrtmdp(rt[2],p): If numrots=0 Then: Disp "Quartic Has One Solution": Disp rt[1]: Disp
"Root is 2-fold": 1->norots: Goto stpe: EndIf: If numrots=1 Then: Disp "Quartic Has
Two Solutions": mod(rot[1]-fin*b1,p)->rt[2]: Disp rt[1]: Disp rt[2]: Disp "Roots are 2-
fold" : 2->norots: Goto stpe: EndIf: If numrots=2 Then: Disp "Quartic Has Three
Solutions": mod(rot[1]-fin*b1,p)->rt[2]: mod(rot[2]-fin*b1,p)->rt[3]: Disp "A 2-fold
Root Is:" : Disp rt[1]: Pause: Disp "Other Roots Are:" : Disp rt[2]: Disp rt[3]: 3-
>norots: Goto stpe: EndIf: EndIf: If numrots=2 Then: mod(rot[1]-fin*b1,p)->rut[1]:
mod(rot[2]-fin*b1,p)->rut[2]: sqrtmdp(rt[2],p): If numrots=0 Then: Disp "Quartic Has
Two Solutions": Disp rut[1]: Disp rut[2]: rut[1]->rt[1]: rut[2]->rt[2]: 2->norots: Goto
stpe: EndIf If numrots=1 Then : Disp "Quartic Has Three Solutions": Disp rut[1]: disp
rut[2]: rut[1]->rt[1]: rut[2]->rt[2]: mod(rot[1]-fin*b1,p)->rt[3]: Disp "And A 2-fold
Root:" Disp rt[3]: Pause: 3->norots: Goto stpe: EndIf: If numrots=2 Then: Disp
"Quartic Has Four Solutions": Disp rut[1]: Disp rut[2]: rut[1]->rt[1]: rut[2]->rt[2]:
mod(rot[1]-fin*b1,p)->rt[3]: mod(rot[2]-fin*b1,p)->rt[4]: Disp rt[3]: Disp rt[4]:
 4->norots:Goto stpe: EndIf: EndIf: EndIf: EndIf: DelVar f:
```

In this block of code, sqrtmdp(a,p) extracts the square roots of a modulo p and is listed in [1]. Next we will deal with the one solution case. As stated in Sun [3], we have:

Theorem 5.2. *Let $p > 3$ be a prime, and $a, b, c \in \mathbb{Z}$. Then the congruence $(*) x^4 + ax^2 + bx + c \equiv 0 \pmod p$ has one and only one solution if and only if the congruence $(**)$ $y^3 + 2ay^2 + (a^2 - 4c)y - b^2 \equiv 0 \pmod p$ is unsolvable. Moreover, if $(**)$ is unsolvable, then the unique solution of $(*)$ is given by*

$$x \equiv \frac{1}{4b}(a^2 - 4c - S^2_{\frac{p+1}{2}}) \pmod p,$$

where $\{S_n\}$ is defined by

$$S_0 = 3, \quad S_1 = -2a, \quad S_2 = 2a^2 + 8c,$$

$$S_{n+3} = -2aS_{n+2} + (4c - a^2)S_{n+1} + b^2 S_n \quad (n = 0, 1, 2, \ldots). \qquad (5.6)$$

The cubic congruence: $y^3 + 2ay^2 + (a^2 - 4c)y - b^2 \equiv 0$ (mod p) is sometimes called the "resolvent cubic". Our coding of quarsom() continues as follows:

```
DelVar f: mod(2*aq,p)->aqq: mod(aq^2-4*cq,p)->bqq: mod(-bq^2,p)->cqq:
x^3+aqq*x^2+bqq*x+cqq->f(x): cunsolm(1,aqq,bqq,cqq,p): If norots=0 Then:
Disp "Quartic Has One Solution": quartons(aq,bq,cq,p): mod(tsol-modinv(4,p)*b1,p
->rt[1]: Disp "Quartic Root Is:" Disp rt[1]: 1->norots: Goto stpe: EndIf: EndIf:
```

The program cunsolm() appears in [2]. As in [2] we use matrix methods as suggested in [4] to compute $S_{(p+1)/2}$. The program quartons() which is called in the code above is for this purpose.

```
quartons(a1,a2,a3,p): Prgm: csponmat(a1,a2,a3,p,(p+1)/2): mod(temp[1,1],p)->sponem:
mod(te[1,1],p)->sphalfm:mod(modinv(4*a2,p)*(a1^2-4*a3-sphalfm^2),p)->sol:
EndPrgm
```

The program quartons() calls csponmat() whose listing appears below:

```
csponmat(a1,a2,a3,n,e): Prgm: DelVar b: randMat(3,3)->b: -2*a1->b[1,1]:
4*a3-a1^2->b[1,2]: a2^2->b[1,3]: 1->b[2,1]: 0->b[2,2]: 0._b[2,3]: 0->b[3,1]:
1->b[3,2]: 0->b[3,3]: matsp(b,e-2,n): pone*[[2*a1^2+8*a3][2*a1][3]]->temp:
tmp*[[2*a1^2+8*a3][2*a1][3]]->te: EndPrgm
```

The listing for matsp() appears in [2]. Having disposed of the one solution case we now consider the no solution case. Following Sun, we denote the number of solutions as $N_p(f(x))$. Let (a/p) be the Legendre symbol. Theorem 5.8 from Sun [3] follows:

Theorem 5.8. *Let $p > 3$ be a prime, $a, b, c \in \mathbb{Z}$ and $p \nmid bD(a, b, c)$. Then $N_p(x^4 + ax^2 + bx + c) = 0$ if and only if there exists an integer y such that $y^3 + 2ay^2 + (a^2 - 4c)y - b^2 \equiv 0 \pmod p$ and $(\frac{y}{p}) = -1$. When $N_p(x^4 + ax^2 + bx + c) > 0$ we have $N_p(x^4 + ax^2 + bx + c) = N_p(y^3 + 2ay^2 + (a^2 - 4c)y - b^2) + 1$.*

We continue our coding of quarsom():

If norots=1 Then: mdexp(rt[1],(p-1)/2,p): If z = p-1 Then: Disp "Quartic Has No Solutions": 0->norots: Goto stpe: Else: Disp "Quartic Has Two Solutions":

We are now in the two solution case for our quartic. We may employ Sun's theorem:

Theorem 5.4. *Let $p>3$ be a prime, $a,b,c\in\mathbb{Z}$ and $p\nmid bD(a,b,c)$. Then congruence $(*)$ $x^4+ax^2+bx+c\equiv 0 \pmod p$ has exactly two solutions if and only if congruence $(**)$ $y^3+2ay^2+(a^2-4c)y-b^2\equiv 0 \pmod p$ has one and only one solution and the unique solution of $(**)$ is a quadratic residue modulo p. Furthermore, if $y\equiv u^2 \pmod p$ is the unique solution of $(**)$ and $v^2\equiv -u^4-2au^2-2bu \pmod p$, then the two solutions of $(*)$ are given by $x\equiv \frac{1}{2}(u\pm\frac{v}{u}) \pmod p$.*

Our coding of quarsom() now continues as follows:

1->co: DelVar ruut: sqrtmdp(rt[1],p): rot[1]->ruut[1]: rot[2]->ruut[2]: Lbl stp4: mod(ruut[co],p)->rotu:mod(-rotu^4-2*aq*rotu^2-2*bq*rotu,p)->vtmp: sqrtmdp(vtmp,p): If numrots=2 Then: Goto stp3: Else: 1+co->co: Goto stp4: EndIf: Lbl stp3: mod(rot[1],p)->rotv: modinv(2,p)->tin: modinv(rotu,p)->rin: modinv(4,p)->fin : mod(mod(tin*(rotu+rotv*rin),p)-fin*b1,p)->rt[1] : mod(mod(tin*(rotu-rotv*rin),p)-fin*b1,p)->rt[2]: Disp "Quartic Roots Are:"Disp rt[1]: Disp rt[2]: 2->norots: Pause: Goto stpe: EndIf: EndIf: EndIf: If norots=3 Then: For I,1,3: mdexp(rt[I],(p-1)/2,p): If z=p-1 Then: Disp "Quartic Has No Solution": 0->norots: Goto stpe: EndIf: EndFor:

Finally we deal with the four solution case of the quartic. From Sun [3], we have:

Theorem 5.6. *Let $p>3$ be a prime, $a,b,c\in\mathbb{Z}$ and $p\nmid bD(a,b,c)$. Then congruence $(*)$ $x^4+ax^2+bx+c\equiv 0 \pmod p$ has four solutions if and only if congruence $(**)$ $y^3+2ay^2+(a^2-4c)y-b^2\equiv 0 \pmod p$ has three solutions and all the three solutions are quadratic residues modulo p. Furthermore, if $y\equiv u_1^2, u_2^2, u_3^2 \pmod p$ $(u_1,u_2,u_3\in\mathbb{Z})$ are the solutions of $(**)$ such that $u_1u_2u_3\equiv -b \pmod p$, then the four solutions of $(*)$ are given by*

$$x\equiv \frac{u_1+u_2+u_3}{2},\ \frac{u_1-u_2-u_3}{2},\ \frac{-u_1+u_2-u_3}{2},\ \frac{-u_1-u_2+u_3}{2} \pmod p.$$

We continue our coding of quarsom( ):

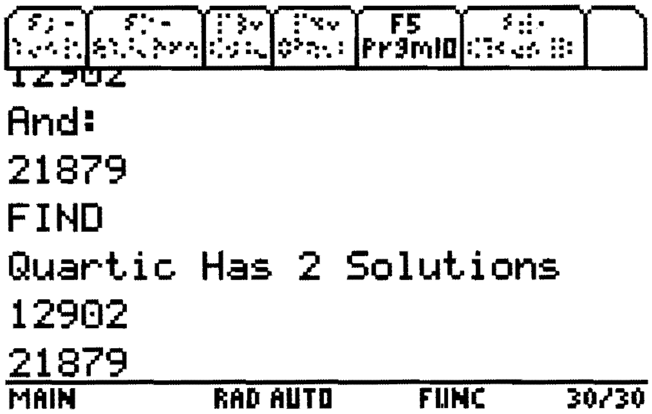
Disp "Quartic Has Four Solutions": DelVar rta, rtb, rtc, uk: sqrtmdp(rt[1],p): Mod(rot[1],p)->rta[1]: mod(rot[2],p)->rta[2]: sqrtmdp(rt[2,],p): mod(rot[1],p)-> rtb[1]: mod(rot[2],p)->rtb[2]: sqrtmdp(rt[3],p): mod(rot[1],p)->rtc[1]:mod(rot[2],p) ->rtc[2] : For ii, 1,2: For jj, 1,2: For kk,1,2: If mod(rta[ii]*rtb[jj]*rtc[kk],p)=mod(-bq,p) Then: rta[ii]->uk[1]: rtb[jj]->uk[2]: rtc[kk]->uk[3]: Goto stp2: EndIf: EndFor: EndFor: EndFor: Lbl stp2: modinv(2,p)->tin: modinv(4,p)->fin: mod(mod((uk[1]*uk[2]+uk[3])* tin,p)-fin*b1,p)->rt[1]: mod(mod((uk[1]-uk[2]-uk[3])*tin,p)-fin*b1,p)->rt[2]:

mod(mod((uk[2]-uk[1]-uk[3])*tin,p)-fin*b1,p)->rt[3]: mod(mod((uk[3]-uk[1]-uk[2])* tin,p)-fin*b1,p)->rt[4]: Disp "Quartic Roots Are:" Disp rt[1]: Disp rt[2]: Disp rt[3]: Disp rt[4]: 4->norots: Pause: EndIf: EndIf: Lbl stpe: EndPrgm

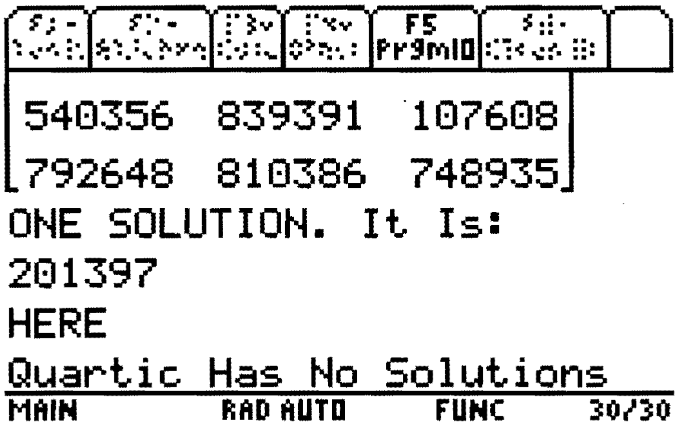
This completes the coding of our main program quarsom(). Let's consider some examples:

Example 1: $x^4 + 7174x^3 + 5596x^2 + 9497x + 13112 \equiv 0$ (mod 18773).
Using the functions quarta(7174,5596,18773), quartb(7174,5596,9497,18773) and quartc(7174,5596,9497,13112,18773), we find that a ≡ 13773, b ≡ 0, c ≡ 17364 (mod 18773). So the depressed quartic is $y^4 + 13773y^2 +17364 \equiv 0$ (mod 18773). Now, qdisc(13773,0,17364,18773) produces 0 so that at least one multiple root is indicated. Our depressed quartic is biquadratic (quadratic in y^2) and we use qucon(_) to solve, obtaining $y^2 \equiv 2500$ (mod 18773). Finally sqrtmdp(2500,18773) yields two square roots, which are 50 and 18723 (mod 18773). Thus the factorization of the depressed quartic is: (y-50)*(y-50)*(y-18723)*(y-18723) (mod 1773). So y ≡ 50 and y ≡ 18723 are both 2-fold roots mod 18773. Converting back to x we get:
x ≡ 50 – 7174*modinv(4,18773) ≡ 7643 as a two-fold root, and
x ≡ 50 – 18723*modinv(4,18773) ≡ 7543 as another two-fold root. The result of running quarsom(1, 7174,5596,9497,13112,18773) follows:

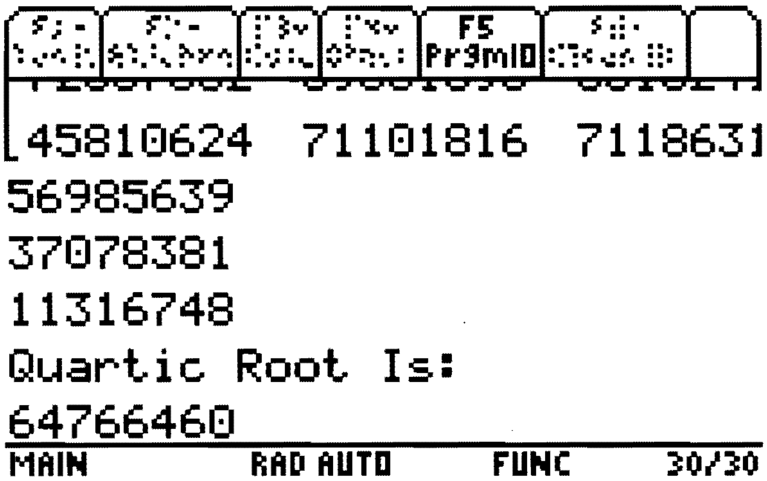
Example 2: $576x^4 + 7654 \cdot x^2 - 4897 \equiv 0$ (mod 34781).
We obtain the monic quartic by multiplying by modinv(576,34781) ≡ 19987 (mod 34781). This produces: $x^4 + 13660x^2 +32176 \equiv 0$ (mod 34781). This is biquadratic, so the depressed quartic is $y^4 + 13660y^2 + 32176 \equiv 0$ (mod 34781). Now, qdisc(13660,0,32176,34781) ≡ 34691 ≢ 0 mod(34781), and b ≡ 0 mod (34781), so no multiple root is indicated. We use qucon() to solve $y^2 + 13660\ y + 32176 \equiv 0$ (mod 34781), obtaining $y^2 \equiv 21387$ and $y^2 \equiv 34519$ (mod 34781). Then: sqrtmdp(21387, 34781) yields "No Root Exists" and sqrtmdp(34519, 34781) yields the values of y, y ≡ 12902 and y ≡ 21879 (mod 34781). Since in this problem x = y, we have our two solutions to the original congruence. Employing quarsom(576, 0, 7654 , 0 , -4897 , 34781) yields the output:



Example 3: $5748 \cdot x^4 - 8907 \cdot x^3 + 69034 \cdot x^2 + 38765 \cdot x - 821345 \equiv 0 \pmod{983243}$. Mulitplying by modinv(5748,983243) ≡ 519504 gives the monic quartic: $x^4 + 902673\ x^3 + 633954\ x^2 + 772677\ x + 52372 \equiv 0 \pmod{983243}$. Then functions quarta, quartb and quartc yield: a ≡ 330163, b ≡ 664929, and c ≡ 819722 (mod 983243). So the depressed quartic is: $y^4 + 330163y^2 + 664929y + 819722 \equiv 0 \pmod{983243}$. Employing qdisc(330163,664929,819722,983243) gives $486750 \not\equiv 0$ (mod 983243). The coefficients of the resolvent cubic are obtained via: mod(2*330163,983243), mod(330163^2-4*819772,983243) and mod(-664929^2,983243). We then obtain the resolvent cubic: $z^3 + 660326z^2 + 42215z + 718411 \equiv 0 \pmod{983243}$. We solve this using: cunsolm(1,660326,42215,718411,983243) to obtain one solution: z ≡ 201397 (mod 9832431). But 201397 is not a quadratic residue modulo 983243, since using Euler's criterion we compute: mdexp(201397, (983243-1)/2, 983243) ≡ $983242 \not\equiv 1$ (mod 983243). So by Theorem 5.8 in Sun, the original quartic has no solution. Using quarsom(5748, -8907, 69034, 38765, -821345, 983242) gives the output below. The "One Solution" here refers to the one solution of the associated cubic. The bottom line in the output indicates that the "Quartic Has No Solutions".

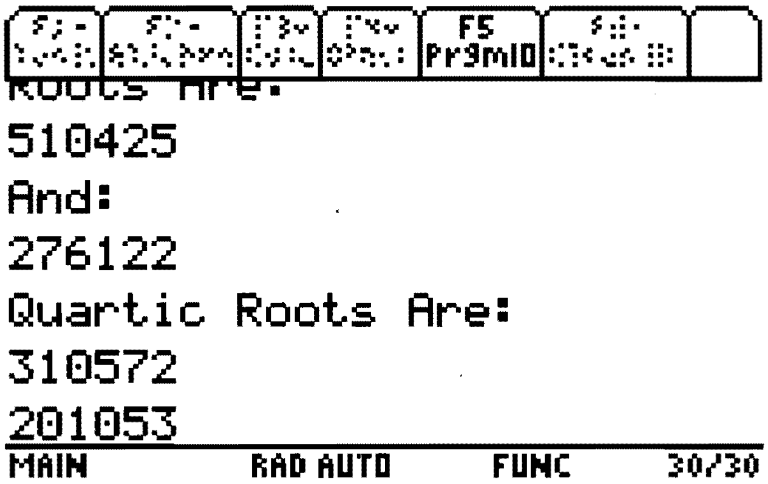


Example 4: $883957 \cdot x^4 + 920987 \cdot x^3 - 23765 \cdot x^2 + 894675 \cdot x + 8024507 \equiv 0$ (mod 78654337).
Multiplying by modinv(883957,78654337) ≡ 53302828 gives the monic quartic:
$x^4 + 22164163\, x^3 + 5401965\, x^2 + 2468474\, x + 54885522 \equiv 0$ (mod 78654337).
Then functions quarta, quartb and quartc yield: a ≡ 310525, b ≡ 18812378, and c ≡ 63297543 (mod 78654337). So the depressed quartic is: $y^4 + 310527y^2 + 18812378y + 63297543 \equiv 0$ (mod 78654337). Employing qdisc(310525, 18812378, 63297543, 78654337) gives $67296421 \neq 0$ (mod 78654337). The coefficients of the resolvent cubic are obtained via: mod(2*310525,983243), mod(310525^2-4*63297543 ,78654337) and mod(-18812378^2,78654337). We then obtain the resolvent cubic: $z^3 + 621050z^2 +56985639z + 16588301 \equiv 0$ (mod 78654337). We solve this using: cunsolm(1,621050,56985639,16588301,78654337) to obtain "Cubic Has No Solution". So we use Sun's Theorem 5.2 to find the single root of the depressed quartic. My program quartons(310525,18812378,63297543,78654337) produces this root (and stores it as "tsol") as y ≡ 11316748. Then converting back to x gives x ≡ 64766460 (mod 78654337). See the output below.



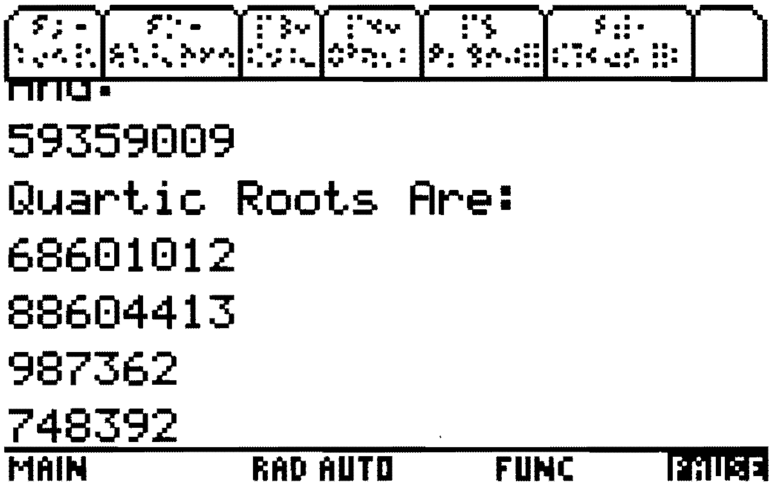
Example 5: $12x^4 - 8765x^3 + 76231 \cdot x^2 + 87654 \cdot x - 38523 \equiv 0$ (mod 786547).
Mulitplying by modinv(12,786547) ≡ 327728 gives the monic quartic:
$x^4 + 720271x^3 + 727354\, x^2 + 400578\, x + 586700 \equiv 0$ (mod 786547). Then functions quarta, quartb and quartc yield: a ≡ 566206, b ≡ 341268, and c ≡ 420194 (mod 786547). So the depressed quartic is: $y^4 + 566206y^2 + 341268y + 420194 \equiv 0$ (mod 786547). Employing qdisc(566206,341268,420194,786547) gives $319277 \not\equiv 0$ (mod 786547). The coefficients of the resolvent cubic are obtained via: mod(2*566206, 786547), mod(566206^2-4*420194, 786547) and mod(-341268^2, 786547). We then obtain the resolvent cubic: $z^3 + 345865z^2 +435024z + 166466 \equiv 0$ (mod 786547). We solve this using: cunsolm(1,345865,435024,166466, 786547) to obtain one solution: z ≡ 135315 (mod 786547). In this case, z is a quadratic residue modulo 786547 which is seen by:

sqrtmdp(135315, 786547) ≡ 308060 or 478487 (mod 786547). So we use Theorem 5.4 in Sun to compute $v^2 \equiv -u^4 - 2au^2 - 2bu \pmod{p}$. However we must choose u to be 478487 because the other choice of u (which is 308060) produces a result which is not a quadratic residue modulo 786547 and so v cannot be obtained. Therefore, we compute: $v^2 \equiv$ mod($-478487^4 - 2*566206*478487^2 - 2*341268*478487$,786547) ≡ 211986 (mod 786547). We conclude that v ≡ sqrtmdp(211986,786547) ≡ 510425 or 276122 (mod 786547). At this point, we may use either value of v to obtain our results. We compute: $y \equiv \frac{1}{2}(u \pm v/u) \pmod{p}$ to obtain solutions to the depressed quartic:
y_1 ≡ mod(modinv(2,p) * (478487 + 510425)*modinv(478487,786547)),786547) ≡ 294003 (mod 786547), and y_2 ≡ mod(modinv(2,p) * (478487 - 510425)*modinv(478487,786547)),786547) ≡ 184484 (mod 786547). Finally, converting back to x gives the two solutions of the original quartic:
x_1 ≡ mod(294003-modinv(4,786547)*720271,786547) ≡ 310527 (mod 786547), and
x_2 ≡ mod(184484-modinv(4,786547)*720271,786547) ≡ 310527 (mod 786547). Using quarsom(12,-8765,76231,87654,-38523,786547) gives the output below:



Example 6: $x^4 + 38010115x^3 + 12800302x^2 + 61736194x + 4296365 \equiv 0 \pmod{98475647}$.
Our quartic is already monic. Then functions quarta, quartb and quartc yield: a ≡ 50886725, b ≡ 81187793, and c ≡ 86473795 (mod 98475647).
So the depressed quartic is: $y^4 + 50886725y^2 + 81187793y + 86473795 \equiv 0 \pmod{98475647}$. Employing qdisc(50886725, 81187793, 86473795, 98475647) gives $37529554 \not\equiv 0$ (mod 98475647). The coefficients of the resolvent cubic are obtained via: mod(2*50886725, 98475647), mod(50886725^2-4*86473795, 98475647) and mod(-81187793^2, 98475647). We then obtain the resolvent cubic: $z^3 + 3297803z^2 + 36169352z + 49120745 \equiv 0 \pmod{98475647}$. We solve this using: cunsolm(1, 3297803, 36169352, 49120745, 98475647) to obtain three solutions: $z_1 \equiv 72991350$, $z_2 \equiv 7153099$, $z_3 \equiv 15033395$ (mod 98475647). Each of these is a quadratic residue

modulo 98475647. So we use Theorem 5.6 from Sun to conclude there are four solutions of the original quartic. Using sqrtmdp(72991350, 98475647) yields roots 29497012 and 69978635, sqrtmdp(7153099, 98475647) yields roots 39355608 and 59120039, sqrtmdp(15033395) yields roots 39116638 and 59359009. A computation shows that if $u_1 \equiv 28497012$, $u_2 \equiv 39355608$, and $u_3 \equiv 39116638$, then the condition: mod($u_1 * u_2 * u_3$,p) ≡ -b (mod p) is satisfied. We find that modinv(2,p) ≡ 49237824 which we store as variable "tin". Then we compute:
$y_1 \equiv$ mod(tin*($u_1 + u_2 + u_3$),p) ≡ 53484629, $y_2 \equiv$ mod(tin*($u_1 - u_2 - u_3$),p) ≡ 73488030
$y_3 \equiv$ mod(tin*($-u_1 + u_2 - u_3$),p) ≡ 84346626, $y_4 \equiv$ mod(tin*($-u_1 - u_2 + u_3$),p) ≡ 84107656. To convert back to x, we store modinv(4,p) = 24618912 as variable "fin". Then the computations: $x_i \equiv$ mod(y_i – fin * b1, p) for i = 1...4 yield the solutions of the quartic:
$x_1 \equiv 68601012$, $x_2 \equiv 88604413$, $x_3 \equiv 987362$, $x_4 \equiv 748392$ (mod 98475647). Using quarsom(1,38010115,12800302,61736194,4296365,98475447) gives the output below:



References

1. J.N. Fadyn, *Solving Quadratic Congruences Modulo a Prime on The TI-89,* Proceedings of the ICTCM 2010.
2. J.N. Fadyn, *Solving Cubic Congruences Modulo a Prime on The TI-89,* Proceedings of the ICTCM 2011.
3. Z.H. Sun, *Cubic and Quartic Congruences Modulo A Prime*, Journal of Number Theory, 102, No. 1, 41-89 (2003).
4. Zentralblatt Math 1868-2008, Zbl 1033.11003 , 2008.