solution to cubic equation                         January 09, 1988

The following shows how to solve a cubic equation in finite field math. For coding purposes, tables for powers of x should be used, as well as solutions to the following equations: x**2 = a; x**3 = a; and x**2 + x + a = 0; where a is the index to each of the tables. Here is the process used to solve a cubic equation, and find roots R, S, and T. (On page 4, a quadratic equation is solved).

```
     x**3 + ax**2 + bx + c = 0

     if(c == 0){
          R = 0 is a root
          goto page 3}

     substitute x=t+a
     (t+a)**3 + a(t+a)**2 + b(t+a) + c = 0
     (t+a)(t**2 + a**2) + at**2 + a**3 + bt + ab + c = 0
     t**3 + a**2t + at**2 + a**3 + at**2 + a**3 + bt + ab + c = 0

     cancel terms  at**2 and a**3
     t**3  +  (a**2 + b)t  +  (ab + c) = 0

     substitute d = a**2 + b,  e = ab + c
     t**3  +  dt  + e = 0

     if((e) == 0){
          t=0 is a root
          x=a is a root
          divide original equation by (x+a)


                        x**2 + (0)x +    (b)
                ________________________________
         (x+a)| x**3 + (a)x**2 + (b)x +    (c)
                x**3 + (a)x**2
                ________________
                       (0)x**2 + (b)x
                       (0)x**2 + (0)x
                       ______________
                                 (b)x +    (c)
                                 (b)x +   (ab)
                                 _______________
                                        (ab+c)
          remainder, (ab+c) == e == 0
          leaving
          x**2 + b = 0
          x**2 = b
          x = b**(1/2)        (use table)
          2 roots, x=a, and x=b**(1/2), done}

     if(d == 0){
          t**3 + (0)t + e = 0
```

```
     t**3 + e = 0
     t**3 = e
     use table to get t
     x = t + a
     call this first root R: R = t + a
     continue on page 3}

once again
t**3  +  dt  + e = 0          (d != 0 and e != 0)

substitute t = u + d/u
(u + d/u)**3 + d(u + d/u) + e = 0
(u + d/u)(u**2 + d**2/u**2)  +  du  + d**2/u + e = 0
u**3 + d**2/u + du + d**3/u**3 + du + d**2/u + e = 0

cancel terms  d**2/u and du
u**3 + e + d**3/u**3 = 0

multiply both sides by u**3
u**6 + eu**3 + d**3 = 0

substitute v = u**3
v**2 + ev + d**3 = 0

substitute v = ew
(ew)**2 + e(ew) + d**3 = 0
e**2w**2 + e**2w + d**3 = 0

divide by e**2      (note: e != 0)
w**2 + w + d**3/e**2 = 0

find root (r) using d**3/e**2 as index (x**2+x+a=0 table)
w=r
v=er
u = v**(1/3)   (use table)
t=u + d/u
x=t + a

call this first root R: R = t + a
```

```
solution to cubic equation                       January 09, 1988

    found first root, R
    divide original equation by (x+R)

                      x**2 +       (R+a)x +       (R**2+aR+b)
                ____________________________________________________
   (x+R)| x**3 +    (a)x**2 +         (b)x +                 (c)
          x**3 +    (R)x**2
          ________________
                 (R+a)x**2 +          (b)x
                 (R+a)x**2 +    (R**2+aR)x
                 ________________________
                             (R**2+aR+b)x                    (c)
                             (R**2+aR+b)x +    (R**3+aR**2+bR)
                             ________________________________
                                            (R**3+aR**2+bR+c)

    note that remainder R**3+aR**2+bR+c
    is equal to 0, since R is a root of x**3+ax**2+bx+c=0

    need to solve
    x**2 + (R+a)x + (R**2+aR+b) = 0

    if (R == 0){
         then c == 0
         equation becomes
         x**2 + (0+a)x +(0**2+a0+b) = 0
         x**2 + ax + b = 0
         substitute f = a, g = b}

    if (R != 0){
         equation is
         x**2 + (R+a)x + (R**2+aR+b) = 0
         simplify (R**2+aR+b), start with original equation
         x**3 + ax**2 + bx + c = 0
         R**3 + aR**2 + bR + c = 0
         R**3 + aR**2 + bR = c
         R**2 + aR    + b  = c/R
         substitute (c/R) for (R**2+aR+b)
         equation becomes
         x**2 + (R+a)x + (c/R) = 0
         substitute f = R+a, g = c/R}

    if (R == a){
         then e == 0, this case handled already}

    need to solve
    x**2 + fx + g = 0
```

```
     to solve
     x**2 + fx + g = 0

     substitute x=fy
     (fy)**2 + f(fy) + g = 0
     f**2y**2 + f**2y + g = 0
     y**2 + y + g/f**2 = 0

     index into table to find second root, call it s
     y = s
     x = fs
     found 2nd root, call it S

     dividing again

                       x +          (S+f)
          _______________________________
    (x+S)| x**2 +   (f)x +            (g)
           x**2 +   (S)x**2
           ________________
                  (S+f)x**2 +         (g)
                  (S+f)x**2 +   (S**2+fS)
                  _______________________
                               (S**2+fS+g)

     note that remainder S**2+fS+g
     is equal to 0, since S is a root of x**2+fx+g=0

     the last root T is found from   x + (S+f) = 0
     T = (S+f)

     now all 3 roots, x=R, x=S, x=T have been determined

check:

     if R, S, and T are the roots, then
     (x+R)(x+S)(x+T) = 0
     is solution to original equation
     x**3 + ax**2 + bx + c = 0

     this leads to

     R + S + T    = a         [1]
     RS + RT + ST = b         [2]
     RST          = c         [3]

     first R is found
     if(R == 0){
          S + T = a      (from [1])
          T = S+a
          ST    = b      (from [2])
          S(S+a) = b
```

```
S**2 + aS + b = 0
f = a
g = b
S**2 + fS + b = 0
this corresponds with R==0 case on page 3}
```

```
if(R == a){
     a + S + T = a        (from [1])
     S + T = 0
     S = T
     aS + aT + ST = b     (from [2])
     a(S + T) + ST = b
     a( 0 ) + ST = b
     ST = b
     S(S) = b
     S = b**(1/2)
     this corresponds with e==0 case on page 1}

R + S + T = a             ([1])
T = R + S + a
RST = c                   ([3])
ST = c/R
S(R+S+a) = c/R
S(S+(R+a)) = c/R
S**2 + (R+a)S + (c/R) = 0
f = (R+a)
g = (c/R)
S**2 + fS + g = 0
this corresponds with last equation on page 3

now S can be determined, making R and S known

once R and S are knowns, then

R + S + T = a        ([1])
T = a + R + S
T = S + (R+a)
f = (R+a)
T = S + f
this corresponds with final root finding on page 4
```

code:

```
     if(c == 0){
          t = a
          goto tdone}

     d=a**2+b
     e = ab+c
     if(e == 0){
          R = a
          S = b**(1/2)                         (use table)
          T = S
          done}
     if(d == 0){
          t = e**(1/3)                         (use table)
          goto tdone;}

     r = root of w**2 + w + (d**3/e**2)      (use table)
     (note: r != 0, since d != 0)

     u = (er)**(1/3)                           (use table)
     t = u + d/u

  tdone:
     R = t + a
     f = t                                     (t = R+a)
     if(R == 0){
          g = b}
     else{
          g = c/R}

     (note: f != 0, since R==a, e==0 case handled already)

     s = root of y**2 + y + (g/f**2)          (use table)
     S = fs
     T = S + f
     done
```

The above code will solve all possible valid cubic equations with 3 roots, and in addition detect all other combinations as invalid. Failure will be indicated when using the cube root and quadratic tables (zero values returned indicate failure).

```
     # of valid root combination for a, b, c =  2829056
     # of invalid combinations               = 13948160
                                               ________
     total # of combination (256**3)           16777216

     # of valids = sum i[1 to 256]: sum j[1 to i]: j
                 = sum i[1 to 256]: (i**2 + i)/2
                 = (256)(257)(258)/6 = 2829056
```