# Real Roots of Univariate polynomials over a Finite Field – Their Existence and Extraction

Dr T R Padmanabhan
Professor Emeritus
Amrita Vishwa Vidyapeetham, Coimbatore, India
trp@amrita.edu

**Abstract**

The paper presents an elegant method to test univariate polynomials $Z_p(x)$ – $p$ being a prime – for the existence of real roots and then to extract them. The method is illustrated through representative examples.

**Key words**: Polynomial over finite fields, Multivariate cryptography, Root isolation

## 1 Introduction

Identification of real roots of univariate polynomials with coefficients in a finite field $Z_p$ is of interest in different fields like cryptography and computer algebra [1-3,5,6 ]. This paper presents an elegant method to ascertain the existence of real roots of such polynomials and then to identify them. Its application is illustrated through two representative examples. In fact the method can be looked upon as an extended application of the 'root squaring' approach used for the extraction of roots of polynomials used along with factorization of ($p$-1) based on the fundamental theorem of arithmetic [7].

## 2 Existence of Real Roots

Let $S(x)$ be a polynomial in the indeterminate $x$ expressed as

$$S\,(x) = \; x^n + \; a_{n-1}x^{n-1} + \; \cdots + \; a_1 x + \; a_0 \tag{1}$$

with $\{a_{n-1},\ a_{n-2},\ ,\ ,\ a_1,\ a_0\} \in Z_p$. The coefficient of $x^n$ is taken as unity for convenience but the results are equally valid for the general case. Let $\{\alpha_j\} \in C$ be the set of $n$ roots of $S(x)$. Let $\{\beta_j\}$ $\in Z_p$, be the set such that for all $\beta_j$

$$S(\beta_j) = 0(mod p) \tag{2}$$

Equation (2) implies that $\{\ \beta_j\ \}$ is the set of all real roots of $S(x)$ (mod($p$)) in $Z_p$. From $S(x)$ form the polynomial $S_{p-1}(y)$ (as explained later)

$$S_{p-1}\,(y) = \; y^n + \; b_{n-1}y^{n-1} + \; \cdots + \; b_1 y + \; b_0 \tag{3}$$

with the set $\left\{\alpha_j^{p-1}\right\}$ $\mathbb{C}$ being its $n$ roots. For any $\beta_j$ satisfying Equation (1) the corresponding

$$\gamma_j \equiv \ \beta_j^{p-1} \,(\text{mod } p)$$

satisfies Equation (3). Here again $\{\gamma_j\}$ represents the set of all real roots of $S_{p-1}(y)$ (mod($p$)) in $\mathrm{Z}_p$. Since $\beta_j \in \mathrm{Z}_p$

$$\gamma_j \equiv \ \beta_j^{p-1} \,(\text{mod } p) \ \equiv 1 \tag{4}$$

This leads to the identity

$$1 + \ b_{n-1} + \ \cdots + \ b_1 + \ b_0 \ \equiv 0 \ (\text{mod } p)$$

for all $\beta_j$. In other words if

$$1 + \ b_{n-1} + \ \cdots + \ b_1 + \ b_0 \ \ 0 \ (mod\ p)$$

a $\beta_j$ satisfying Equation (2) does not exist.
This constitutes a direct method of ascertaining the existence of real roots.
***Example 1***
$p = 751$ is a prime number. With a random selection of elements from $\mathrm{Z}_{751}$ we get
$\mathrm{S}(x) = x^7 + 67x^6 + 688x^5 + 439x^4 + 277x^3 + 256x^2 + 399x + 618$
The corresponding $\mathrm{S}_{750}(y)$ is
$\mathrm{S}_{750}(y) = y^7 + 280y^6 + 18y^5 + 647y^4 + 444y^3 + 198x^2 + 666x + 750$
which leads to
$1 + 280 + 18 + 647 + 444 + 198 + 666 + 750 = 0(\text{mod } 751)$
pointing to the possibility of real roots in $\mathrm{Z}_{751}$.
***Example 2***
Again with $\mathrm{Z}_{751}$(618 – the coefficient of $x^0$in $\mathrm{S}(x)$ in the above example – is changed to 619)
$\mathrm{S}(x) = x^7 + 67x^6 + 688x^5 + 439x^4 + 277x^3 + 256x^2 + 399x + 619$
The corresponding $\mathrm{S}(y)$ is
$\mathrm{S}(y) = y^7 + 713y^6 + 271y^5 + 430y^4 + 541y^3 + 229x^2 + 317x + 750$
leading to
$1 + 713 + 271 + 430 + 541 + 229 + 317 + 750 = 248(\text{mod } 751)$
implying the clear absence of real roots in $\mathrm{Z}_{751}$.

# 3 Extraction of Real Roots

Referring to Equation (1) we are interested in finding out all $\beta_j \in \mathrm{Z}_p$ such that $\mathrm{S}(\beta_j) = 0(\text{mod } p)$. Let g be a primitive element of $\mathrm{Z}_p$(an element having order p – 1). Let ($p$-1) be factored as

$$p - 1 = \ q_1^{e_1} q_2^{e_2} \ldots \ q_k^{e_k} \tag{5}$$

$q_1$, $q_2$, . . $q_k$ being primes. Let

$$g_1 = \ g^{q_1{}^{e_1}} \tag{6}$$

and

$$q_2^{e_2} q_3^{e_3} \ldots \ q_k^{e_k} = q \tag{7}$$

Then

$$g_1^q = g^{p-1} \equiv 1\,(mod\ p)$$

A brute force approach to identify all $\beta_j$ values satisfying Equation (2) is to evaluate S($x$) for all $x$ $\in$ $Z_p$and to pick out $\beta_j$ as those satisfying S($x$) = 0(mod $p$). Let $S_{q_1^{e_1}}(z)$ be the polynomial formed from S($x$) such that

$$S_{\,q_1^{e_1}}\left(z = \beta_j^{q_1^{e_1}}\right) = 0$$

whenever
S($\beta_j$) = 0.
If we identify all the $\delta_j$ such that $S_{q_1^{e_1}}(\delta_j) \equiv 0(\text{mod } p)$, all the $(q_1^{e_1})^{th}$ roots of $\delta_j$ can be obtained and $\beta_j$ selected there from such that S($\beta_j$) = 0(mod $p$). The search for $\delta_j$ is limited to a total of $q_2^{e_2} q_3^{e_3} \ldots q_k^{e_k} = q$ numbers which is more often much smaller than ($p$ - 1) which is the range of search for $\beta_j$. Once a $\delta_j$ is identified one has to search for the corresponding $\beta_j$ by substituting all the $q_1^{e_1}$ roots of $\delta_j$ in S($x$). A real root is identified here through a maximum of ($q + q_1^{e_1}$) polynomial evaluations which is conspicuously smaller than ($p$-1).

# 4 Formation of $\mathbf{S_{q_1^{e_1}}(z)}$

Let $a \in$ C be a root of S($x$) in Equation (1) – a polynomial with real coefficients. The polynomial S($x$) S(-$x$) has $a^2$ as its roots; further the coefficients of odd powers of $x$ are zero here. With this Equation (1) becomes

$$S\left(x^2\right) = x^{2n} + b_{n-1}x^{2n-2} + \cdots + b_1x^2 + b_0 \tag{8}$$

All $b_j$ in Equation (8) are formed as respective $\Sigma$ $a_l$ $a_k$ (mod $p$) values; hence {$b_{n-1}$, $b_{n-2}$, . . . $b_1$, $b_0$} $\in$ $Z_p$. Proceeding on the same lines with {1, $\lambda$, $\lambda^2$} $\in$ C as the cube roots of unity, the product polynomial S($x$) S($x\lambda$) S($x\lambda^2$) has $a^3$as its roots; it has the form

$$S\left(x^3\right) = x^{3n} + c_{n-1}x^{3n-3} + \cdots + c_1x^3 + c_0. \tag{9}$$

Further only the coefficients of $x^{3j}$ in Equation (9) can be non-zero; All $c_j$ in Equation (9) are formed as respective $\Sigma$ $a_m$ $a_l$ $a_k$ (mod $p$) values and hence {$c_{n-1}$, $c_{n-2}$, . . . $c_1$, $c_0$} $\in$ $Z_p$. The procedure can be generalized to get the polynomial with $a^b$as its roots for any desired value of $b$.
Let $\lambda_1$ be a $q_1{}^{th}$root of 1. If S($x$) = 0(mod $p$) for $\beta_j$, S($x\lambda_1$) = 0(mod $p$) for $x = \beta_j\lambda_1^{q_1-1}$. Considering all the $q_1{}^{th}$distinct roots of 1, $x\lambda_1^j$ for all $j$ in {0, 1, 2, . . . $q_1$-1} have respective roots in the corresponding polynomials S($\beta_j\lambda_1^j$). Consider the product polynomial

$$S_{q_1}(z) = \prod_{j=0}^{q_1-1} S(x\lambda_1^j) \tag{10}$$

It is characterised by the following:

1. Coefficients of $z^k = 0$ for $k \neq 0$ (mod $q_1$).
2. $\beta_j^{q_1}$ are the roots of $S_{q_1}(z)$.

Starting with $S_{q_1}(z)$ following the above procedure once again, the polynomial $S_{q_1^2}(z)$ with $z_j^{q_1^2}$ as its roots can be formed; repeating the procedure $e_1$times one can form $S_{q_1^{e_1}}(z)$ the polynomial whose roots are $\beta_j^{q_1^{e_1}}$.

# 5 Formation of Additional Polynomials and Root Extraction

A total of q values of z are to be tried out with $S_{q_1^{e_1}}(z)$ to identify all the $\beta_j^{q_1^{e_1}}$ values. The equation formation can be continued further and the range for search of roots reduced. With $\lambda_2$ being the $q_2{}^{th}$root of 1, form the product polynomial $S_{q_1^{e_1}q_2}(z)$ from $S_{q_1^{e_1}}(z)$ as

$$S_{q_1^{e_1}q_2}(z) = \prod_{j=0}^{q_2-1} S(z\lambda_2^j). \tag{11}$$

Equation (11) is characterized by the following:

1. Coefficients of $x^k = 0$ for $k \neq 0 \pmod{q_2}$.
2. $\beta_j^{q_1^{e_1}q_2}$ are its roots.

Repeating the equation formation successively $e_2$times we get the polynomial $S_{q_1^{e_1}q_2^{e_2}}(z)$. The procedure can be continued as much as desired – if necessary until we get the polynomial with $\beta_j^{p-1}$ as its roots; or it can be terminated when desired and its real roots extracted through a brute force search. In general the polynomial $S_b(x)$ has $\beta_j^b$ as its real roots with $b \in Z_p$. With every $\beta_j^b$ all its $b^{th}$ roots have to be examined to identify the correct $\beta_j$. Different alternatives are possible as brought out through the two representative examples below.

**Example 3**

S($y$) in Example 1 is $S_{750}(x)$ obtained as explained above. With
$750 = 5^3 \times 3 \times 2$
We have

$$S_{5^3\times3\ (=375)} = x^7 + 724x^6 + 129x^5 + 166x^4 + 349x^3 + 611x^2 + 272x + 1$$

Here and in the following example the indeterminate in the polynomials to be solved is retained as $x$ itself throughout. 3 is a primitive element of $Z_{751}$ and $S_{375}$(x) is to be evaluated only for two values of $x$ – $3^{5^3\times3\ (=375)} = 750 \pmod{751}$ and $3^{5^3\times3\times2\ (=750)} = 1 \pmod{751}$; $S_{375}(x) = 0 \pmod{751}$ in both the cases. The subsequent computations are summarized in Figure 1. 1(mod 751) eventually yields the real root 165 (mod 751) through the sequence shown in Figure 2. Similarly 750 (mod 751) yields 24 (mod 751) as the second real root of the polynomial.

**Example 4**

The polynomial considered is
$S(x) = x^8+10195x^7+25179x^6+25729x^5+29803x^4+33100x^3+219x^2+28382x+18831$
with random coefficients in $Z_{34607}$, 34607 being a prime. 10 is a primitive element in $Z_{34607}$. We have
$34606 = 11^3\times13\times2$. The polynomial with $x^{34606}$ as roots is
$S_{34606}(x) = x^8+33249x^7+22604x^6+5471x^5+17554x^4+21736x^3+18273x^2+19359x+1$
$S_{34606}(1) = 1+33249+22604+5471+17554+21736+18273+19359+1 = 0 \pmod{34606}$
showing the possibility of existence of real roots. The root extraction is carried out by forming the polynomials – $S_{11}$(x), $S_{11^2(=121)}(x)$, $S_{11^3(=1331)}(x)$, $S_{11^3\times13(=17303)}(x)$, $S_{11^3\times13\times2(=34606)}(x)$ in the same

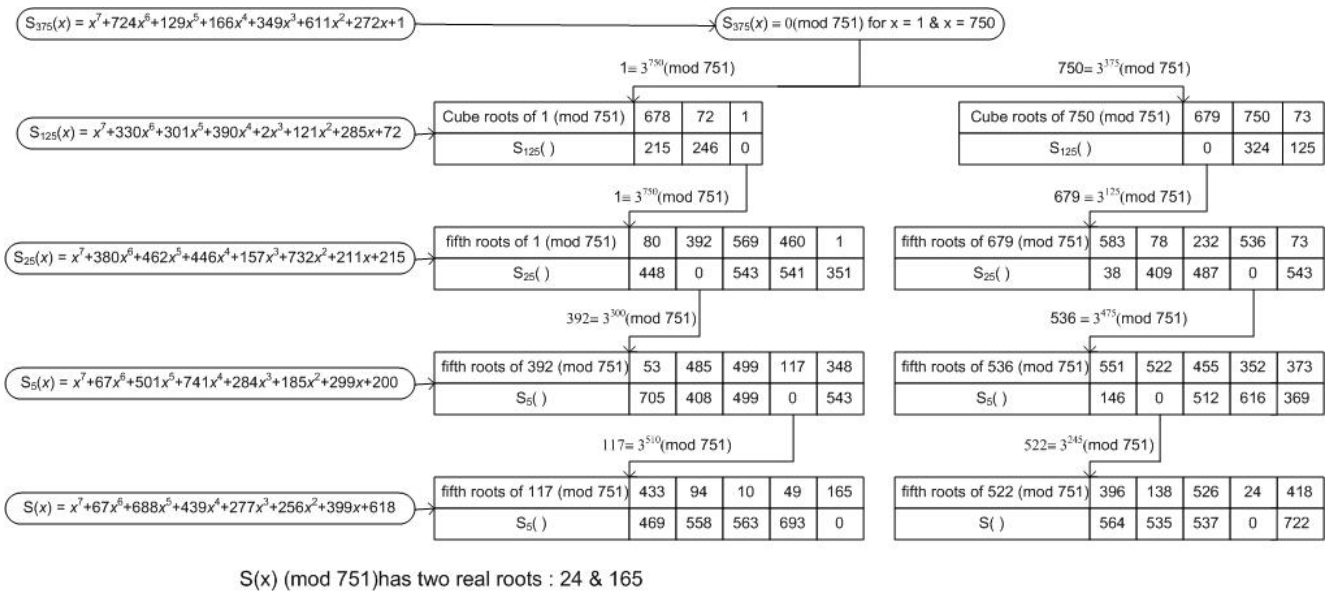


Figure 1: Extraction of real roots of a polynomial in $Z_{751}$

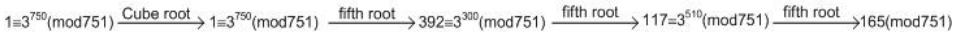


Figure 2: Root extraction sequence to arrive at the real root 165(mod751)

sequence and solving them in the reverse order. The steps in root extraction are summarized in Figure 3. The polynomial is seen to have two real roots– 17386(mod 34607) and 22712(mod 34607).

**Observations:**

The following observations are in order here:

1. In Examples 3 and 4 polynomial formation was continued up to $S_{(p-1)/2}(x)$ and search range minimized. This is not necessary to be done; one may stop the polynomial formation earlier and go in for a correspondingly wider search. Thus in Example 4, one may start with $S_{1331}(x)$ and search amongst all 26 possible candidate elements for real roots.

2. Different possibilities of using the $q_i$-$e_i$ combinations – Equation (5) – with the respective derived polynomials can be carefully studied to identify the optimal sequences of polynomial formation; this may call for more investigations – especially as the size of the prime field increases.

3. $Z_p$with strong primes characterized by corresponding large $q_i$ values make real root identification difficult.

# 6 Conclusions

The method presented to check for existence and to identify real roots of polynomials in $Z_p(x)$ has the potential to simplify such root extraction conspicuously. In turn strengths of multivariate cryptography schemes may be reexamined. The approach presented may also play a decisive role in the generalized number field sieve used for integer factorization [4].

**Acknowledgements**
The author thanks M Sivasankar, Department of Mathematics, School of Engineering Coimbatore, Amrita Vishwa Vidyapeetham, for the fruitful discussions.

**References**

[1] A. G. Akritas, Strzebonski, A. M. A comparative study of two root isolation methods, Nonlinear Analysis: Modeling and Control 10-4 (2005), pp. 297-304.
[2] D. Lazard,. Solving zero-dimensional algebraic systems, Journal of Symbolic Computation 13-2 (1992), pp. 117- 131.
[3] D. Lazard, Rouillier, F., Solving parametric polynomial systems, Journal of Symbolic Computation 42 (2007), pp. 636 – 667.
[4] A.K. Lenstra, H.W.Lenstra,Jr. (eds.), The Development of the Number Field Sieve, Lecture Notes in Mathematics, vol.1554, Springer-Verlag, Berlin 1993.
[5] F. Rouillier, Solving zero-dimensional systems through the rational univariate representation, Journal of Applicable Algebra in Engineering, Communication and Computing 9-5 (1999), pp. 433 – 461.
[6] F. Rouillier, Zimmermann, P., Efficient isolation of polynomial real roots, 2003. Journal of Computational and Applied Mathematics 162-1 (2003), pp. 33 – 50.
[7] V. Shoup, A Computational Introduction to Number Theory and Algebra, Cambridge University Press, Cambridge 2008.
Figure 3


Figure 3: Extraction of real roots of a polynomial in $Z_{34607}$