جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة بابل – كلية التربية

قسم الرياضيات

التحليل الرياضي في تطوير أنظمة تشفير المفتاح المعلن المعتمدة على مسألة إعادة بناء متعددات الحدود

رسالة مقدمة الى

قسم الرياضيات – كلية التربية – جامعة بابل

وهي جزء من متطلبات نيل درجة الماجستير في علوم الرياضيات

من قبل

رومى كريم خضر عجينة

باشراف

الدكتور المهندس ستار بدر سدخان المالكي

٢٠٠٦ م

١٤٢٦ ه

Republic of Iraq
Ministry of Higher Education
and Scientific Research
University of Babylon
College of Education
Department of Mathematics

Mathematical Analysis in Developing the Public-Key Cryptosystems Based on the Polynomials Reconstruction Problem

A Research
Submitted to College of Education
Department of Mathematics
University of Babylon

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in

Mathematics

By

Ruma Karim Kuder Ajeena

Supervised by

Dr. Sattar B. Sadkhan Almaliky

June ٢٠٠٦

Supervisor Certification

I certify that this thesis was prepared under my supervision at the Department of Mathematics/College of Education in the

University of Babylon as a partial fulfillment of the requirements for the degree of Master of Science in Mathematics.

Signature:

Name: Dr. Eng. Sattar B. Almaliky

Date: / / ٢٠٠٦

Signature:

Name: Dr. Iftichar Mudhar Talib

Head of mathematics department

College of Education –University of Babylon

Date: / / ٢٠٠٦

Examination Committee Certificate

We certify that we have read this research entitled as an examining committee examined the student in its contents and that in our opinion it is adequate for the partial fulfillment of the requirements for the degree of Master of Science in Mathematics.

Signature :
Name: Dr. Ali Hussain Batoor

Scientific Grade : Asist . Professor
Date: / / ٢٠٠٦

(Chairman)

Signature :
Name: Dr. Luay A. A. Al - Swede

Scientific Grade : Asist . Professor
Date: / / ٢٠٠٦

(Member)

Signature:
Name: Hussain

Scientific Grade : Asist . Professor
Date: / / ٢٠٠٦

(Member)

Signature:
Name: Dr. Eng. Sattar Bader Almaliky
Scientific Grade : Professor
Date: / / ٢٠٠٦

(Supervisor)

Approved by the University Committee on Graduate Studies.

Signature :

Name: Dr. Luay A. A. Al – Swede

Dean of the College of Education

Scientific Grade : Asist . Professor *Date: / /*
٢٠٠٦

الإهداء

إلى مَن كانَ وَلمْ يَزَلْ مُعلمي عند جهْلي وقدوتي في حياتي وضيائي في الظلماتِ ، إلى السماءِ التي أمطَرتْ في زَمن الجفافِ والظمأ . . .

إلى روح والدي وهي تسكنُ دارَ الخلودِ

إلى مَن لا يَكلُ اللسانُ بالدعاءِ لها وفاءً . . .

إلى مَن لا تملُ العينُ من رؤيةِ وجهها . . .

إلى منَبع التضحيةِ ونحر الحنان وحُضن الأمانة . . .   والدَتي العزيزة

إلى أبلغ المعاني وأصدق المشاعر وأحلى الصور. . .   أخـــــي العزيز

وأخواتي العزيزات

إلى مَن ْعبروا معي محطاتِ الزمانِ خطوةً بعد خطوةٍ . .   أصدقائي الاوفياء

إلى مَن ْبنوا بنياني لبنةً تلو الاخرى . . . ينابيع العطاء

أساتذتي المخلصين. . مع وافر احترامي

إلى كل مَن ْساعدني في انجاز هذا البحث. . .

أهدي هذا الجهد المتواضع. . .

رومى

Abstract:

It is known that the Polynomial Reconstruction is one of the important problems in cryptography. Such problem is introduced in ١٩٩٩ and it was considered as a new hard computational problem. There are several public key cryptographic systems constructed on this problem.

This research provides an analytical study to a public key cryptosystem (PKC) that was based on Polynomial Reconstruction Problem (PRP), and takes into considerations the developments performed on the (PKC) and the corresponding attacking methods. The analysis considers mainly the mathematical background related to polynomials and the operation valid generally on these polynomials and especially in the finite fields such as $GF(2^m)$, $GF(q)$, and $GF(q^u)$. The coding problem is included in the public key cryptosystem that take the PRP into consideration. The Reed-Solomon Code is used in such type of PKC.

The PKC was based on PRP of Augot and it's modification with the Coron's attacks is analyzed mathematically in this research. We propose a modification in the decoding stage of the Augot's system by replacing the Lagrange interpolation method instead of Berlekamp-Welsh interpolation method. This proposition is investigated for the first time in such public key cryptosystem that was based on PRP. The promised result was introduced and the system was reviewed by IEEE Reviews in the conference ICTTA ٢٠٠٦ hold at April ٢٠٠٦ through the participation with a paper entitled.

" ***Evaluation of using Lagrange Interpolation method in polynomial Reconstruction problem*** PRP **".**

Another achievement was hold is a treatment of Augot's system in $GF(q)$ instead of $GF(2^m)$ as it was originally treated. A complete computer simulation using MATLAB is implemented.

Acknowledgement

I wish to express my gratitude to my supervisor Dr. Eng. Sattar B. . Sadkhan for his encouragement, guidance and support during this work

I would like to thank the present Dean of College of Education Dr. Luay A.A.Al – Swidi, for helping me and kind treatment since starting of my course study. Also, I would like to thank the present head of mathematics department Dr. Ifticher Mudhar Talib, Dr. Assa'd Al-Husaine and the staff of the mathematics ..and Computer Science departments for their cooperation

I wish to give my deepest gratitude to my family, especially to my . parents, whose efforts I truly appreciate

Thanks are also due to my friends in courses for their interest and . consideration

Lemma (I. ١): For every non zero element $\lambda \in GF(q)$, $\lambda^{q-1}=1$. Furthermore, an element $\lambda \in GF(q^u)$ lies in $GF(q)$ itself iff $\lambda^q=\lambda$ [١٥].

Lemma (I. ٢): For every non-zero element $\lambda \in GF(q),\ \ ord(\lambda)$

divides $q-1$ [١٥].

Lemma (I. ٣): If $\lambda,\ \beta \in F$ and F has characteristic q, then

$(\lambda+\beta)^q=\lambda^q+\beta^q$ [١٥].

Proof: By the binomial theorem

$$(\lambda+\beta)^q = \sum_{i=0}^{q}\binom{q}{i}\lambda^{q-i}\beta^i = \binom{q}{0}\lambda^q+\sum_{i=1}^{q-1}\binom{q}{i}\lambda^{q-i}\beta^i+\binom{q}{q}\beta^q \ .$$

Now $\binom{q}{i}$ is an integer, and for $1 \le i \le q-1$, $\binom{q}{i}=\dfrac{q(q-1).....(q-i+1)}{i(i-1).....2.1}$.

Since q exceeds all factors in the denominator, and q is prime, q in the numerator goes uncancelled. As a result, $\binom{q}{i}\equiv 0\ (\mathrm{mod}q)$ for $1 \le i \le q-1$.

Hence all intermediate terms vanish, and the result follows.

Theorem ٢.٧.٢.١: The minimal polynomial of element λ is unique [١٥].

Proof : Suppose $F = GF(q)$ and F has characteristic q. From Lemma (I.١) that λ satisfies the polynomial $x^{q-1}-1$ in $GF(q)[x]$. Since $\exists$ a polynomial in $GF(q)[x]$ for which λ is a root, there must be one of the least degree. This is minimal polynomial, suppose $\exists$ two monic polynomials $m_1(x)$ and $m_2(x)$ of least degree having λ as a root.

By the division algorithm for polynomials $\exists$ two polynomials $L(x)$, $r(x)$ $\ni$ $m_1(x) = L(x)m_2(x) + r(x)$, where $\deg r(x) < \deg m_2(x)$ or $r(x) = 0$.

Since $m_1(\lambda) = 0$ and $m_2(\lambda) = 0$ by def of minimal polynomial, we have $r(\lambda) = 0$. But $m_2(x)$ has least degree which implies $r(x) = 0$ and hence $m_2(x)$ divides $m_1(x)$.

Similarly, we can show that $m_1(x)$ divides $m_2(x)$ and since $m_1(x)$ and $m_2(x)$ are monic, $m_1(x) = m_2(x)$.

Lemma ٢.٧.٢.١: Let F be a finite field of characteristic q, Let $\lambda \in F^*$ and Let $C(\lambda)$ be the set of conjugates of λ with respect to $GF(q)$. Then $m_\beta(x) = \prod_{\beta \in C(\lambda)} (x - \beta)$ is a polynomial with coefficients from $GF(q)$ [١٥].

Proof : Let $m(x) = \sum_{i=0}^{t} m_i x^i$. The coefficients $m_i \in F$, we need to prove that they are in fact in the ground field $GF(q)$. First note that

$$m(x)^q = \prod_{\beta \in C(\lambda)} (x-\beta)^q$$

$$= \prod_{\beta \in C(\lambda)} (x^q - \beta^q)$$

$$= \prod_{\beta \in C(\lambda)} (x^q - \beta) = m(x^q) = \sum_{i=0}^{t} m_i x^{iq} ,$$

with the following second equality from (Lemma (I.٣)) and the third since $\{\beta : \beta \in C(\lambda)\} = \{\beta^q : \beta \in C(\lambda)\}$.

On the other hand note that $m(x)^q = \sum_{i=0}^{t} (m_i x^i)^q = \sum_{i=0}^{t} m_i{}^q x^{iq}$

Hence $m_i = m_i^q$ implying by (Lemma (I.١)) that $m_i \in GF(q)$ for $0 \le i \le t$. This completes the proof.

Properties of Trace Operator :

Property ١:

When λ is in $GF(q^u)$, $Tr_q^{q^u}(\lambda)$ has values in $GF(q)$.

Proof: $[Tr_q^{q^u}(\lambda)]^q = (\sum_{i=0}^{u-1} \lambda^{q^i})^q$ (Definition (٢.٧.٣.١))

$= \sum_{i=0}^{u-1} \lambda^{q^{i+1}}$ (By Lemma (٢.٧.١.١))

$= \sum_{i=1}^{u-1} \lambda^{q^i} + \lambda$ (If $\lambda \in GF(q^u)$ then $\lambda^{q^u} = \lambda$)

$= Tr_q^{q^u}(\lambda)$. (Definition (٢.٧.٣.١)).

Property ٢: Conjugate field elements have the same trace operator, i.e. $Tr_q^{q^u}(\lambda^q) = Tr_q^{q^u}(\lambda)$ for $\lambda \in GF(q^u)$.

Proof: From ***Property* ١** we have

$$[Tr_q^{q^u}(\lambda)]^q = Tr_q^{q^u}(\lambda).$$ (I.١)

And from Definition (٣٢), we get

$$[Tr_q^{q^u}(\lambda)]^q = Tr_q^{q^u}(\lambda^q)$$ (I.٢)

from (I.١) and (I.٢) we have, $Tr_q^{q^u}(\lambda^q) = Tr_q^{q^u}(\lambda)$.

***Property* ٣:** The trace operator is linear map: for $a,b\in$ $GF(q)$ and $\lambda,\beta\in GF(q^u)$, then $Tr_q^{q^u}(a\lambda+b\beta)=aTr_q^{q^u}(\lambda)+bTr_q^{q^u}(\beta)$

Proof : $Tr(a\lambda+b\beta)=\sum_{i=0}^{u-1}(a\lambda+b\beta)^{q^i}$ (Definition (٢.٧.٣.١))

$$=\sum_{i=0}^{u-1}(a^{q^i}\lambda^{q^i}+b^{q^i}\beta^{q^i})$$ (Definition (٢.٧.١.٣))

$$=\sum_{i=0}^{u-1}(a\lambda^{q^i}+b\beta^{q^i})$$ (Theorem (٢.٧.١.٢))

$$=\sum_{i=0}^{u-1}a\lambda^{q^i}+\sum_{i=0}^{u-1}b\beta^{q^i}$$

$$=a\sum_{i=0}^{u-1}\lambda^{q^i}+b\sum_{i=0}^{u-1}\beta^{q^i}$$

$$=aTr_q^{q^u}(\lambda)+bTr_q^{q^u}(\beta)$$ (Definition (٢.٧.٣.١)).

Property ٤: For each choice of b in $GF(q)$, there are q^{u-1} elements λ in $GF(q^u)$ for which $Tr_q^{q^u}(\lambda)=b.$

Proof : Every element λ in $GF(q^u)$ has $Tr_q^{q^u}(\lambda)=b$ iff λ is a root of the trace operator equation

$$x+x^{q}+x^{q^2}+.....+x^{q^{u-1}}-b=0,\ b\in GF(q).$$

Every element of $GF(q^u)$ must be the root of exactly one such equation, and each of the q equations has exactly q^{u-1} roots. Since all roots of the trace operator equations are accounted for by elements of $GF(q^u)$, there must be exactly q^{u-1} elements of $GF(q^u)$ with trace b in $GF(q)$.

Property ٥: If $GF(q)\subset GF(q^k)\subset GF(q^u)$ then

$$Tr_q^{q^u}(\lambda)=Tr_q{}^{q^k}[Tr_{q^k}^{q^u}(\lambda)],\quad \forall\lambda\in GF(q^u).$$

Proof: Consider the nested trace polynomial expression

$$Tr_q^{q^k}[(Tr_{q^k}^{q^u}(x)]=\sum_{j=0}^{k-1}\left(\sum_{i=0}^{\frac{u}{k}-1}x^{q^{ki}}\right)^{q^j}$$ (Definition (٢.٧.٣.١))

$$=\sum_{j=0}^{k-1}\sum_{i=0}^{\frac{u}{k}-1}x^{q^{ki+j}}$$ (Definition (٢.٧.١.٣))

$$=\sum_{n=0}^{u-1} x^{q^n} \qquad \text{(for } n=ki+j \text{)}$$

$$=Tr_q^{q^u}(x).$$

Property ٦: Let $GF(q^u)$ be the smallest field containing λ, and let the minimum polynomial of $m_\lambda(x)$ be denoted by

$m_\lambda(x)=\sum_{i=0}^{u} a_i x^{u-i}$, then $a_1=-Tr_q^{q^u}(\lambda)$.

Proof: From Lemma (٢.٧.٢.١), we get

$$m_\lambda(x)=\prod_{i=0}^{u-1}(x-\lambda^{q^i})$$

$$=(x-\lambda)(x-\lambda^q)(x-\lambda^{q^2})..........(x-\lambda^{q^{u-1}})$$

$$=x^u\pm..............-(\lambda+\lambda^q+\lambda^{q^2}+.......+\lambda^{q^{u-1}})x+ (\lambda\lambda^q\lambda^{q^2}.....\lambda^{q^{u-1}}).$$

Then $a_1=-\ (\lambda+\lambda^q+\lambda^{q^2}+.......+\lambda^{q^{u-1}})$. (I.٣)

And $Tr_q^{q^u}(\lambda)=\sum_{i=0}^{u-1}\lambda^{q^i}$

$$=\lambda+\lambda^q+\lambda^{q^2}+.......+\lambda^{q^{u-1}} \qquad \text{(I.٤)}$$

From (I.٣) and (I.٤) we have

$$a_1=-Tr_q^{q^u}(\lambda).$$

Proposition ٢.٧.٣.١***:*** For all $p \in GF(q^u)[X],$ we have $Tr[ev(p)] = ev[Tr(p)].$.

Proof: The $j-th$ component of $Tr[ev(p)]$ is

$$Tr[p(x_j)] = Tr(\sum_{i=0}^{k} p_i \cdot x_j^i).$$

From (Remark (٢.٧.٣.٢), and the fact that $x_j \in GF(q)$, we obtain:

$$Tr[p(x_j)] = \sum_{i=0}^{k} Tr(p_i) x_j^i$$

which is the $j-th$ component of $ev[Tr(p)].$

Theorem ٢.٧.٣.١***:*** Let V be a finite dimensional vector space over $F.$ then the dual space V^* is also finite dimensional, and $\dim V = \dim V^*$ [٤].

Proof: Let $\{v_1, v_2, ..., v_n\}$ be a basis of V. We shall find a basis of V^*. According to Definition (٢.٧.٣.٣), $\forall\, i = 1,2,.....,n\ \exists$ a functional, which we denote by v_i^* ∍

$$< v_i^*, v_j > = \begin{cases} 1 & if\ i = j, \\ 0 & if\ i \neq j. \end{cases}$$

We shall prove that $\{v_1^*, v_2^*, ..., v_n^*\}$ is a basis of V^*.

Let $\varphi \in V^*$ and let $c_i = < \varphi, v_i > = \varphi(v_i).$ We contend that

$\varphi = c_1 v_1^* + ... + c_n v_n^*$.

For each $i,$ we have

$< c_1 v_1^* + ... + c_n v_n^*, v_i > = c_i < v_i^*, v_i > = c_i$. Since $c_i = \varphi(v_i)$, it follows that φ and $c_1 v_1^* + ... + c_n v_n^*$ have the same values on all elements of the basis $\{v_1, v_2, ..., v_n\}$. Hence they have the same values on linear combinations of these basis elements, and hence are equal on V. Therefore, $v_1^*, v_2^*, ..., v_n^*$ generate V^*.

To prove that they are linearly independent, suppose that

$x_1 v_1^* + ... + x_n v_n^* = 0$ with elements $x_i \in F.$

Evaluate this expression on v_i. We find

$0 =< x_1 v_1^* + ... + x_n v_n^*, v_i > = x_i < v_i^*, v_i > = x_i$. Hence all $x_i = 0,$ then $v_1^*, v_2^*, ..., v_n^*$ are linearly independent. That is, $v_1^*, v_2^*, ..., v_n^*$ are basis of V^*, and is called the dual basis of $\{v_1, v_2, ..., v_n\}$.

Example (II. ١): Let us have a polynomial $p(x) = 5 + x - 11x^2$ in $Q[x]$ that has degree ٢. Then it is required to find the leading term $lt(p))$ and leading coefficient $(lc(p))$.

Solution:

From (Definition (٢.١.٧), we have $(lt(p)) = -11x^2$ and it has $(lc(p)) = -11$. Consider as a polynomial in $Z/_{11}Z[x]$, $p(x)$ has degree ١, $lt(p) = x$ and $lc(p)$ $= 1(\text{mod } 11)$ [٢٩].

Example (II. ٢): Let us have a polynomial $f(x)=(2x+1)^3$ in $Q[x]$ that has degree ٣.

Then it is required to find the leading term $lt(p))$ and leading coefficient $(lc(p))$.

Solution:

From (Definition (٢.١.٧)), we have $lt(p)=8x^3$ and it has $lc(p)=8$ [٢٩].

Example (II. ٣): Let us have a field Z_5. Then it is required to generate a monic polynomial over Z_5.

Solution:

Let $f(x)=x^2+3x+1$ be a polynomial over Z_5, since the $lc(f)=1$.Then (from Definition (٢.١.٨)), $f(x)$ is a monic polynomial .

Example (II. ٤): Let us have polynomials $f(x)=x^5+2x+1$and $g(x)=x+3$ over F . Then it is required to find the coefficients are equal to zero.

Solution:

Since $\deg(f) =$ ٥ $> \deg(g) =$ ١. From (Remark (٢.١.٣)), then the coefficients b_2, b_3, $b_4, b_5 = 0$.

Example (II. ٥): Let us have polynomials $f(x) = x^5 + 2x + 1$ and $g(x) = x + 3$ in $F[x]$. Then it is required to find the degree of sum polynomials.

Solution:

Since $f(x) + g(x) = x^5 + 3x + 4$. From (Remark (٢.١.٣)), that is $\deg(f + g) =$ ٥ $= n$.

Example (II. ٦): Let us have polynomials $f(x) = -3x^5 + 2x^2 + 1$ and $g(x) = 3x^5 + x^3 + 2$ over F. Then it is required to find the degree of sum polynomials.

Solution:

Since $f(x) + g(x) = 0x^5 + x^3 + 2x^2 + 3$.From (Remark (٢.١.٣)), that is

i.e the degree of sum polynomials is less then $n =$٥.$\deg(f + g) = 3$.

Example (II. ٧): Let us have a polynomial $f(x) = x^3 + 2x^2 + 2$ and $g(x) = 2x^2 + x + 1$ over F. Then it is required to find the product of $f(x)$ and $g(x)$.

Solution: By (Remark (٢.١.٤)), we have

$$f(x).\ g(x) = 2x^5 + 5x^4 + 3x^3 + 6x^2 + 2x + 2.$$

Example (II. ٨): Let us have a polynomial $f(x) = x^6 - 1$ over $Z/_2[Z]$.Then it is required to find the divisor of $f(x)$.

Solution: Since $f(x) = (x^2 - 1)(x^4 + x^2 + 1)$ over $Z/_2[Z]$. From (Remark (٢.١.٥)), then $x^2 - 1$ is a divisor of $f(x)$ over $Z/_2[Z]$.

Example (II. ٩): Let us have polynomials $f(x)=x^4+2x^3+3x^2+2x+1$ and $g(x)=x^2-1$ in $Q[x]$. Then it is required to find the division of $f(x)$ by $g(x)$.

Solution:

From (Theorem (٢.١.٢)), and by long division, we can find the $quot(x)$ and the $rem(x)$ when dividing $f(x)$ by $g(x)$. So from equation (٢.١.٣) we have

$x^4+2x^3+3x^2+2x+1=(x^2+2x+4)(x^2-1)+(4x+5)$. We conclude that

and $rem(x)=4x+5$. x^2+2x+4 $quot(x)=$

Example (II. ١٠): Let us have a polynomial $f(x)=x^2+1$ in $R[x]$ over R. Then it is required to find the divisor of $f(x)$.

Solution: From (Remark (٢.١.٦)), we have

$x^2+1=(x-i)(x+i)$, where $i=\sqrt{-1}$.

Example (II. ١١): Let us have polynomials $f(x)=x^3+2x+1$ and $g(x)=x+1$ over $Z/_3Z[x]$. Then it is required to find the degree of $rem(x)$.

Solution:

From equation (٢.١.٣), and by long division, we can find,

. By (Remark (٢.١.٧)), then $=(x+1)(x^2+2x)+1\, g(x)quot(x)+rem(x)=f(x)$

$\deg(rem)=0$.

Example (II. ١٢): Let us have polynomials $f(x)=x^2-1$, $g(x)=x^3-1$, $h(x)=x-1$, $Z(x)=x^2+1$ and $V(x)=x^4-1$ over $Q[x]$. Then it is required to find the GCD of $f(x)$ and $g(x)$, and Lcm of $f(x)$ and $Z(x)$.

Solution:

By (Definition (٢.٢.١)), the polynomial $h(x)$ is a common divisor of $f(x)$ and $g(x)$, since $f(x)=(x-1)(x+1)$ and $g(x)=(x-1)(x^2+x+1)$. In fact from (Definition (٢.٢.٢)), $h(x)$ is a GCD of $f(x)$ and $g(x)$.And by (Definition (٢.٢.٣)), the common multiple of $f(x)$ and $Z(x)$ is $V(x)$. In fact from (Definition (٢.٢.٤)), $V(x)$ is a LCM of $f(x)$ and $Z(x)$.

Example (II. ١٣): Let us have polynomials $f(x)=x^4+3x^3-x^2-4x-3$ and $g(x)$ $=3x^3+10x^2+2x-3$ over F. Then it is required to find the GCD of $f(x)$ and $g(x)$.

Solution: From equation (٢.١.٣), we divide $f(x)$ by $g(x)$ but first multiply $f(x)$ by ٣ (to avoid fractional coefficients):

$$3f(x)=g(x)quot_1(x)+rem_1(x)$$

$$=(3x^3+10x^2+2x-3)(x+1)+(5x^2+25x+30).$$

Thus, the first remainder, after dividing by ٥, will be $rem_1=x^2+5x+6$. We divide the polynomial $g(x)$ by it :

$$g(x)=rem_1(x)quot_2(x)+rem_2(x)$$

$$=(x^2+5x+6)(3x-5)+(9x+27).$$

The second remainder, after dividing by ٩, is thus $rem_2=x+3$. Since

$$rem_1(x)=rem_2(x)quot_3(x)+rem_3(x)$$

$=(x+3)(x+2)+0$, then from (Theorem (٢.٢.١)), it follows that $rem_2(x)$ will be the last remainder which exactly divides the preceding remainder. It will consequently be the desired GCD. That is $GCD(f,g)=x+3.$

Example (II. ١٤): Let us have the polynomials $f(x)=x^3-x^2+3x-10$ and $g(x)$ $=x^3+6x^2-9x-14$ over F . Then it is required to find the polynomials and $v(x)$ which satisfy equation (٢.٢.٧) .$u(x)$

Solution: From (٢.١.٣) , we have $f(x)=g(x)quot_1(x)+rem_1(x)$

$$=(x^3+6x^2-9x-14)(1)+(-7x^2+12x+4).$$

Also, $g(x)=rem_1(x)quot_2(x)+rem_2(x)$

$$=(-7x^2+12x+4)(-\frac{1}{7}x-\frac{54}{49})+(\frac{235}{49}x-\frac{470}{49}).$$

$$rem_1(x)=rem_2(x)quot_3(x)+rem_3(x)$$

$$=(x-2)(-7x-2)+0.$$

Thus, from (Theorem (٢.٢.١)), $GCD(f(x),g(x))=x-2.$ And by ((Theorem (٢.٢.٢)) , $u(x)=\frac{7}{235}x+\frac{54}{235}$, $v(x)=\frac{-7}{235}x-\frac{5}{235}.$

Example (II. ١٥): Let us have the polynomials $a(x)$ and $b(x)$ in $Z/_5Z[x]$, $a(x)=x^8+4x^7+4x^6+4x^5+4x^4+2x^3+x+2$ and $b(x)=x^6+3x^5+4x^4+2x^3+3x^2+2$. Then it is required to apply the extended Euclidean algorithm to the polynomials for finding the GCD of $a(x)$ and $b(x)$, and finding the two polynomial $u(x)$, $v(x)$.

Solution: First apply the division algorithm to $a(x)$ and $b(x)$ yielding, from equation (٢.١.٣) we have:

$a(x) = (x^2 + x + 2)b(x) + (2x^5 + x^4 + 2x^2 + 4x + 3),$ i.e. yield $quot_2(x) = x^2 + x + 2,$ $rem_2(x) = 2x^5 + x^4 + 2x^2 + 4x + 3$ and to find $u_2(x)$ and $v_2(x).$

$u_k(x) = u_{k-2}(x) - quot_k(x).\ u_{k-1}(x)$ and $v_k(x) = v_{k-2}(x) - quot_k(x).\ v_{k-1}(x)$ where $u_0(x) = v_1(x) = 1,$ $v_0(x) = u_1(x) = 0$.

$$u_1(x) - quot_2(x). = u_0(x)\ u_2(x)$$

$$= 1 - (x^2 + x + 2)(0)$$

$$= 1.$$

$$v_1(x) - quot_2(x). = v_0(x)\ v_2(x)$$

$$= 0 - (x^2 + x + 2)(1)$$

$$= -x^2 - x - 2.$$

$+ rem_3(x).$ Yields $quot_3(x) = 3x,\ (2x^5 + x^4 + 2x^2 + 4x + 3)\ quot_3(x).\ b(x) =$

$.\ 4x^4 + x^3 + x^2 + x + 2\ rem_3(x) =$

$$u_2(x) - quot_3(x). = u_1(x)\ u_3(x)$$

$$= 0 - 3x(1)$$
$$= -3x.$$

$$v_2(x) - quot_3(x). = v_1(x)\ v_3(x)$$

$$= 1 - (3x)\ (-x^2 - x - 2)$$

$$= 1 + x + 3x^2 + 3x^3.$$

.Yields $quot_4(x) = 3x + 2,\ rem_4(x)\ rem_4(x)\ rem_3(x) + = quot_4(x).\ rem_2(x)$

$$= 2x^2 + x + 4.$$

$$u_3(x) - quot_4(x).\, u_2(x)\, u_4(x) =$$

$$= 1 - (3x+2)(-3x)$$

$$= 4x^2 + x + 1.$$

$$v_4(x) = v_2(x) - quot_4(x).v_3(x)$$

$$= (x^2 - x - 2) - (3x+2)(1 + x + 3x^2 + 3x^3)$$

$$= x^4 + 4x + 1.$$

. Yields $quot_5(x) = 2x^2 + 2x + 3.\ rem_5(x)\ rem_4(x) + = quot_5(x).\ rem_3(x)$

Thus, from (Theorem (٢.٢.١)), the GCD $(a(x), b(x))$ is $2x^2 + x + 4.\ \ rem_5(x) = 0.$
i.e. from (Theorem (٢.٢.٣)), $rem_4(x) = u_4(x)\ a(x) + v_4(x).b(x)$ [١٥].

The steps in the Algorithm can be summarized by the following Table (II.١):

Table II. ١: shows the Extended Euclidean algorithm for polynomials

k	$u_k(x)$	$v_k(x)$	$rem_k(x)$	$quot_k(x)$
٠	١	٠	a(x)	------
١	٠	١	b(x)	------
٢	١	$- x^{٢} - x - ٢$	$٢x^{٥} + x^{٤} + ٢x^{٢} + ٤x + ٣$	$x^{٢} + x + ٢$

٣	$–٣x$	$٣x^{٣}+٣x^{٢}+x+١$	$٤x^{٤}+ x^{٣} + x^{٢} +x+٢$	$٣x$
٤	$٤x^{٢} +x+١$	$x^{٤}+٤x+١$	$٢x^{٢}+x+٤$	$٣x +٢$
٥			٠	$٢x^{٢}+٢x+٣$

Example (II. ١٦): Let us have a polynomial function $a(x)=x^2-2x+2$ in $R[x]$ .Then it is required to find the evaluation of $a(x)$ at ٣.

Solution: From (Definition (٢.٣.١)), we have $a(x)$ is the quadratic function $a:R\longrightarrow R$. If $r=3$, $a(3)=3^2-2(3)+2=5$, its graph is a parabola. By completing the square $x^2-2x+2=(x^2-2x+1)+1$

$$=(x-1)^2+1.$$

It follows that the polynomial function has no zeros, since $(r-1)^2+1$ is a positive for every real number.

Example (II. ١٧): Let us have a polynomial $p(x)=x^3-x$ over $Z/_3Z[x]$. Then it is required to find the roots of $p(x)$.

Solution: The corresponding polynomial function is the zero function. Every element of $Z/_3Z[x]$ is a zero (root) of $p(x)$. From (Definition (٢.٣.١)), that is, $p(0)=0$, $p(1)=1^3-1=0$, $p(2)=(2^3-2)\text{mod}3=0$. Hence ٠,١ and ٢ are roots of $p(x)$.

Example (II. ١٨): Let us have a polynomial $f(x)=x^2+3x+1$. Then it is required to find the ٢th derivative of $f(x)$.

Solution: By (Remark (٢.٤.١)), we have $f^{(2)}(x)=2!(1)=2$.

Example (II. ١٩): Let us have a polynomial $f(x)=2x^2+4$ over Q. Then it is required to consider the polynomial $f(x)$.

Solution: From (Definition (٢.٥.١)), the polynomial $f(x)=2x^2+4$ is irreducible over Q but reducible over Z.

Example (II. ٢٠): Let us have a polynomial $f(x)=2x^2+4$ over R Then it is required to consider the polynomial $f(x)$.

Solution: From (Definition (٢.٥.١)), the polynomial $f(x)=2x^2+4$ is irreducible over R but reducible over C.

Example (II. ٢١): Let us have a polynomial $f(x)=x^4-1$over $Q[x]$. Then it is required to find the factorization polynomial $f(x)$.

Solution: From (Theorem (٢.٥.٣)), the factorization in irreducible of $f(x)$ in $Q[x]$ is $f(x)=(x^2+1)(x+1)(x-1)$. From (Definition (٢.٥.١)), the first factor is irreducible, since it has no rational zeros. Consider as a polynomial $f(x)$ in $C[x]$, the factorization is $f(x)=(x+i)(x-i)(x+1)(x-1)$.Consider as a polynomial $f(x)$ in $Z/_2Z[x]$, the factorization is $f(x)=(x+1)^4$ [١٠].

Example (II. ٢٢): Let us have a polynomial $f(x)=x^4+2x^2+1$ in $Q[x]$.Then it is required to consider the polynomial $f(x)$ is irreducible or not.

Solution: In $Q[x]$. From (Remark(٢.٥.١)), the polynomial $f(x)=x^4+2x^2+1=(x^2+1)^2$ is reducible , but has no zero in Q [١٠].

Example (II. ٢٣): Let us have a degree of the polynomial $p(x)$ is $k=2$, that length $n=3$ over finite field $F_q = F_{11}$, and the data points are showen in Table (II.٢) . Then it is required to generate a polynomial $p(x)$ over F_{11}.

Table II. ٢: shows the data points (x, p(x)).

x	$p(x)$
١	١
٦	٩
٧	١
٨	٣

Solution: Applying the ***Direct Method of Interpolation*** to find a polynomial $p(x)$. For second order polynomial interpolation, we choose $p(x)=a_2x^2+a_1x+a_0$. We can construct $p(x)$ from three of the shadows (data points). Using $(6, 9)$, $(7, 1)$, $(8, 3)$ Then from equation (٢.٦.١.١٥), we have

$$p(6)=a_2(6)^2+a_1(6)+a_0=9$$

$$p(7)=a_2(7)^2+a_1(7)+a_0=1$$

$$.\ p(8)=a_2(8)^2+a_1(8)+a_0=3$$

Writing the three equations in matrix form

$$\begin{bmatrix} 1 & 6 & 36 \\ 1 & 7 & 49 \\ 1 & 8 & 64 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} 9 \\ 1 \\ 3 \end{bmatrix}$$

And the solution of the above three equations by using ***Gaussian Elimination*** gives:

$$p(x)=(5x^2-73x+267)\mathrm{mod}11$$

$$=5x^2+4x+3.$$

Example (II. ٢٤): Let us have a degree of the polynomial $p(x)$ is $k-1=2$, that length $n=3$ over finite field $F=Z_{11}$, data points $(1,1)$, $(6,9)$ and $(7,1)$. Then it is required to generate a polynomial $p(x)$ over Z_{11}.

Solution: Applying the ***Lagrange Interpolation*** to find a polynomial $p(x)$ at data points $(1,1)$, $(6,9)$ and $(7,1)$. From equation (٢.٦.١.١٦), we can compute the polynomial $p(x)$:

$$p(x)=7*(x-6)(x-7)+18*(x-1)(x-7)+2*(x-1)(x-6)$$

$$=(27x^2-249x+432)\ \mathrm{mod}11$$

$$=5x^2+4x+3.$$

Example (II. ٢٥) : Let us have a degree of the polynomial $p(x)$ is $k-1=3$, that length $n=4$ in the field $F=Z_{17}$, data points $(1,8)$, $(2,7)$, $(3,10)$ and $(4,2)$ .Then it is required to generate a polynomial $p(x)$ over Z_{17}.

Solution: Applying the ***Lagrange Polynomial Interpolation*** to find a polynomial $p(x)$ at data points $(1,8)$, $(2,7)$, $(3,10)$ and $(4,2)$. From equation (٢.٦.١.١٦), we can compute the polynomial $p(x)$:

$$p(x)=[112(x-2)(x-3)(x-4)+63(x-1)(x-3)(x-4)+80(x-1)(x-2)(x-4)+$$
$$6(x-1)(x-2)(x-3)]\bmod 17$$

$$=[261x^3-2108x^2+5295x-4120]\bmod 17$$

$$=6x^3+8x+11.$$

Example (II. ٢٦) : Let us have a Berlekamp – Welch Interpolation with the degree $k=3, w=1$. Then it is required to generate a unique polynomial $p(x)$.

Solution: We interpolate to find the polynomial $p(x)$ of degree ٢ ∍ $p(0)=1, p(1)=3, p(2)=7$, $p(3)=13$ and $p(4)=21$.

Since $w=1$ then there exist corrupted at the position ١ ∍ $E(1)=0$. So the receiver ٠ instead of ٣ in the packet. Let $E(x)=x-e$ be the error- locator polynomial, where e is unknown, and let $R(x)$ be a polynomial defined at $x=0,1,2,3,4$ ∍ satisfy equation (٢.٦.٣.١٩). By using the relationship of equation (٢.٦.٣.١٩), we can obtain a linear system whose solutions will be the coefficient of p and E.

Let $Q(x)=ax^3+bx^2+cx+d=p(x)E(x)$, where a, b, c, d are unknown coefficients. So from equation (٢.٦.٣.٢٠), we have $ax^3+bx^2+cx+d=R(x)E(x)$ which we can rewrite as:

$$ax^3+bx^2+cx+d+R(x)e=R(x)x$$

Now we substitute $x=0,1,2,3,4$ in equation (٢.٦.٣.٢٠) to get five linear equations: If $x=0$, then $d+e=0$ (II.١)

If $x=1$, then $a+b+c+d=0$ (II.٢)

If $x=2,$ then $8a+4b+2c+d+7e=14$ (II.٣)

If $x=3,$ then $27a+9b+3c+d+13e=39$ (II.٤)

If $x=4,$ then $64a+16b+4c+d+21e=84$ (II.٥)

By using the ***Gaussian Elimination*** to find the values of the unknown a, b, c, d, e ∋ a = ١, b = ٠, c = ٠ , d = -١ , e =١ , from equation (٢.٦.٣.١٨), we have $E(x)=x-1$. Hence $Q(x)=x^3-1,$ and by equation (٢.٦.٣.٢١), we obtain

$$=\frac{x^3-1}{x-1}=\frac{(x-1)\ (x^2+x+1)}{(x-1)}=x^2+x+1.\ \ p(x)=\frac{Q(x)}{E(x)}$$

Example (II. ٢٧): Let us have a field prime field $GF(29)$. Then it is required to compute of arithmetic operations in $GF(29)$.

Solution: let the elements of $GF(29)$ are $\{0,1,\ldots.,28\}$, then

(i) Addition: $17+20=8$, since $37 \bmod 29=8.$

(ii) Subtraction: $17-20=26$, since $-3 \bmod 29=26.$

(iii) Multiplication: $17*20=21$, since $340 \bmod 29=21.$

(iv) Inversion: $17^{-1}=12$, since $17*12 \bmod 29=1.$

Example (II. ٢٨): Let us have a field $GF(2^3)$. Then it is required to generate the elements of $GF(2^3)$.

Solution: We can generate the elements $(0,1,\lambda,\lambda^2,.....,\lambda^6)$ in $GF(2^3)$ that are the ٨ binary polynomials of degree at most ٢, reduction polynomial $f(\lambda)$ $=\lambda^3+\lambda+1$ by the Table (II.٣).

Table II. ٣: The Galois Field of $GF(2^3)$ ***with Reduction Polynomial*** $f(\lambda)$ $=\lambda^3+\lambda+1$**.**

Representation powers	Representation binary	Representation polynomial	Representation decimal
0	000	٠	٠
1	100	١	١
λ	010	x	٢
λ^2	001	x^2	٤
$=1+\lambda\ \lambda^3$	110	$1+x$	٣
$\lambda+\lambda^2\ \lambda^4=$	011	$x+x^2$	٦
$\lambda^5=1+\lambda+\lambda^2$	111	$1+x+x^2$	٧
$\lambda^6=1+\lambda^2$	101	$1+x^2$	٥

Example (II. ٢٩): Let us have a field $GF(2^4)$. Then it is required to generate the elements of $GF(2^4)$.

Solution: We can generate the elements $(0,1,\lambda,\lambda^2,.....,\lambda^{14})$ in $GF(2^4)$ that are the ١٦ binary polynomials of degree at most ٣, reduction polynomial $f(\lambda)$ $=\lambda^4+\lambda+1$ by the Table (II.٤).

Table II.٤ : The Galois Field of $GF(2^4)$ ***with Reduction Polynomial***

.$=\lambda^4+\lambda+1\ f(\lambda)$

Representation powers	Representation binary	Representation polynomial	Representation decimal
0	0000	٠	٠
1	1000	١	١
λ	0100	x	٢
λ^2	0010	x^2	٤
λ^3	0001	x^3	٨
$\lambda^4=1+\lambda$	1100	$1+x$	٣
$\lambda^5=\lambda+\lambda^2$	0110	$x+x^2$	٦
$\lambda^6=\lambda^2+\lambda^3$	0011	x^2+x^3	١٢
$\lambda^7=1+\lambda+\lambda^3$	1101	$1+x+x^3$	١١
$\lambda^8=1+\lambda^2$	1010	$1+x^2$	٥
$\lambda^9=\lambda+\lambda^3$	0101	$x+x^3$	١٠
$\lambda^{10}=1+\lambda+\lambda^2$	1110	$1+x+x^2$	٧
$\lambda^{11}=\lambda+\lambda^2+\lambda^3$	0111	$x+x^2+x^3$	١٤
$\lambda^{12}=1+\lambda+\lambda^2+\lambda^3$	1111	$1+x+x^2+x^3$	١٥
$\lambda^{13}=1+\lambda^2+\lambda^3$	1011	$1+x^2+x^3$	١٣
$\lambda^{14}=1+\lambda^3$	1001	$1+x^3$	٩

Example (II.٣٠): Let us have a field $GF(2^5)$. Then it is required to generate the elements of $GF(2^5)$.

Solution: We can generate the elements $(0,1,\lambda,\lambda^2,.....,\lambda^{30})$ in $GF(2^5)$ are the ٣٢ binary polynomials of degree at most ٤, reduction polynomial $f(\lambda)$ $=\lambda^5+\lambda^2+1$ by the Table (II.٥).

Table II. ٥: The Galois Field of $GF(2^5)$ with Reduction Polynomial

٠$=\lambda^5+\lambda^2+1 \; f(\lambda)$

Representation powers	Representation binary	Representation polynomial	Representation decimal
0	00000	٠	٠
1	10000	١	١
λ	01000	x	٢
λ^2	00100	x^2	٤
λ^3	00010	x^3	٨
λ^4	00001	x^4	١٦
$\lambda^5=1+\lambda^2$	10100	$1+x^2$	٥
$\lambda^6=\lambda+\lambda^3$	01010	$x+x^3$	١٠
$\lambda^7=\lambda^2+\lambda^4$	00101	x^2+x^4	٢٠
$\lambda^8=1+\lambda^2+\lambda^3$	10110	$1+x^2+x^3$	١٣
$\lambda^9=\lambda+\lambda^3+\lambda^4$	01011	$x+x^3+x^4$	٢٦
$\lambda^{10}=1+\lambda^4$	10001	$1+x^4$	١٧
$\lambda^{11}=1+\lambda+\lambda^2$	11100	$1+x+x^2$	٧
$\lambda^{12}=\lambda+\lambda^2+\lambda^3$	01110	$x+x^2+x^3$	١٤
$\lambda^{13}=\lambda^2+\lambda^3+\lambda^4$	00111	$x^2+x^3+x^4$	٢٨
$\lambda^{14}=1+\lambda^2+\lambda^3+\lambda^4$	10111	$1+x^2+x^3+x^4$	٢٩
$\lambda^{15}=1+\lambda+\lambda^2+\lambda^3+\lambda^4$	11111	$1+x+x^2+x^3+x^4$	٣١
$\lambda^{16}=1+\lambda+\lambda^3+\lambda^4$	11011	$1+x+x^3+x^4$	٢٧
$\lambda^{17}=1+\lambda+\lambda^4$	11001	$1+x+x^4$	١٩
$\lambda^{18}=1+\lambda$	11000	$1+x$	٣
$\lambda^{19}=\lambda+\lambda^2$	01100	$x+x^2$	٦

$\lambda^{20}=\lambda^2+\lambda^3$	00110	x^2+x^3	١٢
$\lambda^{21}=\lambda^3+\lambda^4$	00011	x^3+x^4	٢٤
$\lambda^{22}=1+\lambda^2+\lambda^4$	10101	$1+x^2+x^4$	٢١
$\lambda^{23}=1+\lambda+\lambda^2+\lambda^3$	11110	$1+x+x^2+x^3$	١٣
$\lambda^{24}=\lambda+\lambda^2+\lambda^3+\lambda^4$	01111	$x+x^2+x^3+x^4$	٣٠
$\lambda^{25}=1+\lambda^3+\lambda^4$	10011	$1+x^3+x^4$	٢٥
$\lambda^{26}=1+\lambda+\lambda^2+\lambda^4$	11101	$1+x+x^2+x^4$	٢٣
$\lambda^{27}=1+\lambda+\lambda^3$	11010	$1+x+x^3$	١١
$\lambda^{28}=\lambda+\lambda^2+\lambda^4$	01101	$x+x^2+x^4$	٢٢
$\lambda^{29}=1+\lambda^3$	10010	$1+x^3$	٩
$\lambda^{30}=\lambda+\lambda^4$	01001	$x+x^4$	١٨

Example (II.٣١): Let us have a field $GF(3^2)$. Then it is required to generate the elements of $GF(3^2)$.

Solution: We can generate the elements $(0,1,\lambda,\lambda^2,\ldots..,\lambda^7)$ in $GF(3^2)$ are the ٩ polynomial of degree at most ١, reduction polynomial $f(x)=x^2+x+2$ by the Table (II.٦) :

Table II. ٦: The Galois Field of $GF(3^2)$ ***with Reduction Polynomial***

$=x^2+x+2.\ f(\lambda)$

Representation powers	Representation binary	Representation polynomial	Representation decimal
0	00	٠	٠
1	10	١	١
λ	01	x	٣
$=1+2\lambda\ \lambda^2$	12	$1+2x$	٧
$=2+2\lambda\ \lambda^3$	22	$2+2x$	٨

$2\ \lambda^{4}=$	20	٢	٢
$\lambda^{5}=2\lambda$	02	$2x$	٦
$\lambda^{6}=2+\lambda$	21	$2+x$	٥
$\lambda^{7}=1+\lambda$	11	$1+x$	٤

Example (II.٣٢): Let us have a field $F=GF(2^3)$, $f(x)=x^3+x+1$ be an irreducible polynomial over $GF(2^3)$. Then it is required to generate the elements of $GF(2^3)$ by using the Zech's log table.

Solution: By using example (II.٢٨). Then $F=\{0,1,x,1+x,x^2,x+x^2,1+x^2,1+x+x^2\}$. $\forall\, i,\ 0\leq i\leq 6$ the integer , from equation (٢.٧.٢٣), we get :

$$1+\lambda^{0}=100+100=0$$

$$1+\lambda^{1}=100+010=110=\lambda^{3}$$

$$1+\lambda^{2}=100+001=101=\lambda^{6}$$

$$1+\lambda^{3}=100+110=010=\lambda$$

$$1+\lambda^{4}=100+011=111=\lambda^{5}$$

$$1+\lambda^{5}=100+111=011=\lambda^{4}$$

$$1+\lambda^{6}=100+101=001=\lambda^{2}$$

and defining $\lambda^{\infty}=0$. The Zech's Log table is

Table II.٧: The Zech's Log of $GF(2^3)$ with Reduction Polynomial

$.\, f(x)=x^3+x+1$

i	$Z(i)$
∞	٠
٠	∞
١	٣
٢	٦
٣	١
٤	٥
٥	٤
٦	٢

With this table, representing elements of $F=GF(2^3)$ as power of the generator $\lambda=x$, both multiplication and addition are easily performed. For multiplication, we add exponents and reduce modulo $q-1=7$, so from equation (٢.٧.٢٢), we get :

$$.\lambda^6=\lambda^{10(\bmod 7)}=\lambda^3\,\lambda^4$$

And for example of add, and by equation (٢.٧.٢٤), we have

$$\lambda^3+\lambda^5=\lambda^3(1+\lambda^2)$$

$=\lambda^3\lambda^6$ (by using Zech's Log table (II.٧))

$$=\lambda^{9(\bmod 7)}$$

$$=\lambda^2.$$

Example (II.٣٣): Let us have a field binary field $GF(2^4)$. Then it is required to compute of arithmetic operations in $GF(2^4)$.

Solution: let the elements of $GF(2^4)$ are the ١٦ binary polynomials of degree at most ٣, from example (II.٢٩) . Then

(i) Addition: $(x^3+x^2+1)+(x^2+x+1)=x^3+x$, (from Remark (٢.٧.١))

(ii) Subtraction: $(x^3+x^2+1)-(x^2+x+1)=x^3+x$. (from Remark (٢.٧.١)), we have $-a=a \; \forall a \in F_{2m}$.

(iii) Multiplication: $(x^3+x^2+1)\cdot(x^2+x+1)=x^2+1$, since

$(x^3+x^2+1)\cdot(x^2+x+1)=x^5+x+1$and $(x^5+x+1)\mathrm{mod} \;\; (x^4+x+1)=x^2+1.$

(iv) Inversion: $(x^3+x^2+1)^{-1}=x^2$, since $(x^3+x^2+1)\cdot x^2 \mathrm{mod} \;\; (x^4+x+1)=1.$

Example (II.٣٤): Let us have a field $GF(3^2)$ over the finite field $GF(3)$, $x+1=(1,1)$ and $x+2=(1,2)$ are elements in $GF(3^2)$. Then it is required to show the $(1,1)$ and $(1,2)$ are basis of $GF(3^2)$ over $GF(3)$.

Solution:

Firstly, to show that $(1,1)$ and $(1,2)$are linearly independent. Suppose that a,b are numbers ∋ $a(1,1)+b(1,2)=(0,0)$. Then

$$a+b=0 \qquad \text{(II.٦)}$$

and $$a+2b=0. \qquad \text{(II.٧)}$$

Subtracting the equation (II.٦) from the equation (II.٧), we get $b=0 \Rightarrow a=0$. Hence a,b are both zero. That is, the vectors are linearly independent. Secondly, to show that $(1,1)$ and $(1,2)$ are generate to $GF(3^2)$, let (a,b) be an arbitrary element of $GF(3^2)$, we have to show that ∃ numbers $x, y \ni x(1,1)+y(1,2)=(a,b)$. In other words, we must solve the system of equations:

$$x+y=a$$ (II.٨)

$$x+2y=b$$ (II.٩)

Again subtract the equation (II.٨) from the equation (II.٩) , we get :

and finally $x=2a-b$. Hence, (from Definition (٢.٧.٦)), the vectors $y=b-a$ $(1,1)$ and $(1,2)$ are basis of $GF(3^2)$ over $GF(3)$.

Example (II. ٣٥): Let us have a field $GF(2^4)$, and $f(x)=x^4+x+1$ be a primitive polynomial over $GF(2^4)$. Then it is required to find the primitive elements of the $GF(2^4)$.

Solution: From (Definition (٢.٧.١.١)), the primitive elements are $2,3,5$ but $4,6,8$ are not primitive elements, since the powers of $3=\lambda^4$ of $GF(2^4)$ are : (Using the table (II.٤)),

$$(\lambda^4)^1=\lambda^4,\ (\lambda^4)^2=\lambda^8,\ (\lambda^4)^3=\lambda^{12},\ (\lambda^4)^4=\lambda^{16\text{mod}15}=\lambda, (\lambda^4)^0=1$$

$$,\ (\lambda^4)^6=\lambda^{24\text{mod}15}=\lambda^9,\ (\lambda^4)^7=\lambda^{28\text{mod}15}=\lambda^{13}, (\lambda^4)^5=\lambda^{20\text{mod}15}=\lambda^5$$

$$,\ (\lambda^4)^9=\lambda^6,\ (\lambda^4)^{10}=\lambda^2,\ (\lambda^4)^{11}=\lambda^{14}, (\lambda^4)^{12}=\lambda^3,\ (\lambda^4)^{13}=\lambda^7,\ (\lambda^4)^8=\lambda^2$$

and $(\lambda^4)^{14}=\lambda^{11}$.

The $3=\lambda^4$ which generates all the ١٥ non-zero elements of $GF(2^4)$. But the powers of $8=\lambda^3$ of the field $GF(2^4)$ are $(\lambda^3)^0=1$, $(\lambda^3)^1=\lambda^3$, $(\lambda^3)^2=\lambda^6$, $(\lambda^3)^3=\lambda^9$, $(\lambda^3)^4=\lambda^{12}$, and $(\lambda^3)^5=\lambda^{15\mathrm{mod}15}=\lambda^0=1$.

The element $8=\lambda^3$ is not a primitive element of $GF(2^4)$, since it doesn't generate all the ١٥ non-zero elements of $GF(2^4)$. Similarly we can check the all elements in the $GF(2^4)$.

Example (II.٣٦): A list of primitive polynomials is given in Table (II.٨) [٣].

From (Remark (٢.٧.١.١)), we get :

Table II.٨: shows the Default Primitive Polynomial over $GF(2^m)$.

m	Default primitive polynomials for $GF(2^m)$	Decimal
٢	x^2+x+1	٧
٣	x^3+x+1	١١
٤	x^4+x+1	١٩
٥	x^5+x^2+1	٣٧
٦	x^6+x+1	٦٧
٧	x^7+x+1	١٣١
٨	$x^8+x^4+x^3+x^2+1$	٢٨٥
٩	x^9+x^4+1	٥٢٩
١٠	$x^{10}+x^3+1$	١٠٣٣
١١	$x^{11}+x^2+1$	٢٠٥٣
١٢	$x^{12}+x^6+x^4+x+1$	٤١٧٩
١٣	$x^{13}+x^4+x^3+x+1$	٨٢١٩

١٤	$x^{14}+x^5+x^3+x+1$	١٦٤٢٧
١٥	$x^{15}+x+1$	٣٢٧٧١
١٦	$x^{16}+x^5+x^3+x^2+1$	٦٥٥٨١

Example (II. ٣٧): Let us have a polynomial $f(x)=x^4+x+1$ over $GF(2)$. Then it is required to find $f^2(x)=f(x^2)$.

Solution: From (Definition (٢.٧.١.٣)), we have

$$f^2(x)=(x^4+x+1)^2$$

$$\begin{aligned}&=x^8+x^2+1+2x^5+2x^4+2x\\&=x^8+x^2+1\\&=f(x^2).\end{aligned}$$

Example (II. ٣٨): Let us have a polynomial $f(x)=x^2+x+1$ in $Z_2[x]$ over Z_2. Then it is required to consider the primitive polynomial $f(x)$ over Z_2.

Solution: Let $x^k-1=x^{q^u-1}-1=x^3-1,$ and $f(x)=x^2+x+1$. From equation (٢.٧.١.٣٢), $f(x)$ is a primitive polynomial over Z_2.

Example (II. ٣٩): Let us have a polynomial $f(x)=x^2+1$ over Z_3. Then it is required to consider the primitive polynomial $f(x)$ over Z_3.

Solution: Let $x^k-1=x^8-1$. From equation (٢.٧.١.٣٢), $f(x)$ is not a primitive polynomial over Z_3.

Example (II.٤٠): Let us have a polynomial $g(x)=2x+3$ over $GF(5^2)$ and the reduction $f(x)=x^2+x+1$. Then it is required to consider the primitive polynomial $g(x)$ over $GF(5^2)$.

Solution: Let $q^u-1=5^2-1=2^3*3=S_1^3*S_2=24$. From equation (٢.٧.١.٣٣), we get :

and $(2x+3)^{\frac{24}{2}} \bmod(x^2+x+1)=(2x+3)^{12}\bmod(x^2+x+1)=4\neq 1$

. Hence, $g(x)$ is a $(2x+3)^{\frac{24}{3}} \bmod (x^2+x+1)=(2x+3)^8 \bmod (x^2+x+1)=x\neq 1$ primitive polynomial over $GF(5^2)$.

Example (II.٤١): Let us have a field $GF(2^4)$, and $\beta=\lambda$ be an element in $GF(2^4)$.Then it is required to generate the minimal polynomial of β.

Solution: We form the following sequence $\beta=\lambda,\ \beta^2=\lambda^2,\ \beta^{2^2}=\lambda^4,$ $\beta^{2^3}=\lambda^8,\ \beta^{2^4}=\lambda^{16 \bmod 15}=\lambda,\ \beta^{2^5}=\lambda^{32 \bmod 15}=\lambda^2,$......................

Notice that repetition begins at β^{2^4}. Therefore, the minimal polynomial of λ has $\lambda,\lambda^2,\lambda^4,\lambda^8$ as all its roots. Thus, from (Theorem (٢.٥.٣)) and (Remark (٢.٧.١)) $m_1(x)=(x+\lambda)(x+\lambda^2)(x+\lambda^4)(x+\lambda^8)$. (II.١٠)

Expanding the right-hand side of equation (II.١٠) with the aid of table (II.٤), we obtain :

$$m_1(x)=x^4+(\lambda+\lambda^2+\lambda^4+\lambda^8)x^3+(\lambda^3+\lambda^5+\lambda^6+\lambda^9+\lambda^{10}+\lambda^{12})x^2$$
$$+(\lambda^7+\lambda^{11}+\lambda^{13}+\lambda^{14})x+\lambda^{15},$$

since $\lambda+\lambda^2+\lambda^4+\lambda^8=\lambda+\lambda^2+\lambda+1+\lambda^2+1=0$

$\lambda^7+\lambda^{11}+\lambda^{13}+\lambda^{14}=1,\ \lambda^{15}=1.\ \lambda^3+\lambda^5+\lambda^6+\lambda^9+\lambda^{10}+\lambda^{12}=0,$

Hence, $m_1(x)=x^4+x+1.$

In the similar method, we can find $m_2(x)=x^4+x+1$. Now, we find the $m_3(x)$:

$$\beta^{2^1}=(\lambda^3)^{2^1}=\lambda^6,\qquad \beta^{2^2}=(\lambda^3)^{2^2}=\lambda^{12},\qquad \beta^{2^0}=(\lambda^3)^{2^0}=\lambda^3,$$
$$\beta^{2^3}=(\lambda^3)^{2^3}=\lambda^{24\bmod 15}=\lambda^9,\ \ \beta^{2^4}=(\lambda^3)^{2^4}=\lambda^3,\ldots\ldots\ldots\ldots$$

In this sequence there exist only four distinct elements $\lambda^3,\lambda^6,\lambda^9,\lambda^{12}$ as all its roots. Thus from (Theorem (٢.٥.٣)),

$$m_3(x)=(x+\lambda^3)(x+\lambda^6)(x+\lambda^9)(x+\lambda^{12})$$

$$=x^4+(\lambda^3+\lambda^6+\lambda^9+\lambda^{12})x^3+(\lambda^9+\lambda^{12}+\lambda^{15}+\lambda^{15}+\lambda^3$$
$$+\lambda^6)x^2+(\lambda^3+\lambda^6+\lambda^9+\lambda^{12})x+\lambda^0,$$

since $(\lambda^3+\lambda^6+\lambda^9+\lambda^{12})=1,\ (\lambda^9+\lambda^{12}+\lambda^3+\lambda^6)=1,\ \lambda^0=0$. Hence, $m_3(x)=x^4+x^3+x^2+x+1$. Also, $m_4(x)=x^4+x+1$. Now, we find the $m_5(x)$:

$$\beta^{2^1}=(\lambda^5)^{2^1}=\lambda^{10},\ \beta^{2^2}=(\lambda^5)^{2^2}=\lambda^5,\ldots..\beta^{2^0}=(\lambda^5)^{2^0}=\lambda^5,$$

In this sequence there exist only two distinct elements λ^5, λ^{10} are roots.

Thus $m_5(x)=(x+\lambda^5)(x+\lambda^{10})$

$$=x^2+(\lambda^5+\lambda^{10})x+\lambda^{15}$$

$$=x^2+x+1.$$

Since $\lambda^5+\lambda^{10}=1,\ \lambda^{15}=1.$ Also, $m_6(x)=x^4+x^3+x^2+x+1.$Now, we find $m_7(x)$ as:

$$\beta^{2^1}=(\lambda^7)^{2^1}=\lambda^{14},\ \beta^{2^2}=(\lambda^7)^{2^2}=\lambda^{13}, \beta^{2^0}=(\lambda^7)^{2^0}=\lambda^7,$$

$$\beta^{2^5}=(\lambda^7)^{2^5}=\lambda^{14},\dots\dots\dots\dots\beta^{2^4}=(\lambda^7)^{2^4}=\lambda^7,\ \beta^{2^3}=(\lambda^7)^{2^3}=\lambda^{11},$$

$$m_7(x)=x^4+(\lambda^7+\lambda^{11}+\lambda^{13}+\lambda^{14})x^3+(\lambda^3+\lambda^5+\lambda^9+\lambda^6+\lambda^{10}$$
$$+\lambda^{12})x^2+(\lambda+\lambda^2+\lambda^4+\lambda^8)x+\lambda^0,$$

$$,\ x^4+x^3+1\, m_7(x)=$$

since$\lambda^7+\lambda^{11}+\lambda^{13}+\lambda^{14}=1,\ \lambda^3+\lambda^5+\lambda^9+\lambda^6+\lambda^{10}+\lambda^{12}=0,\ \lambda+\lambda^2+\lambda^4+\lambda^8=0$

and $\lambda^0=1.$then

$$m_0(x)=x+1.$$

$$m_8(x).\ m_4(x)=m_2(x)=m_1(x)=$$

$$m_{12}(x).\ m_9(x)==m_6(x)=m_3(x)$$

$$.=m_{10}(x)\ m_5(x)$$

$$m_{14}(x).\, m_{13}(x)==m_{11}(x)=m_{7}(x)$$

Example (II. ٤٢): Let us have a field $GF(11)$, $n=5$, and $f(x)=9x^{3}+x^{2}+7x+4$.

Then it is required to generate the ev mapping.

Solution: From (Definition (٢.٧.٢.٢)), we get :

, $f(2)=6$, $f(3)=2$, $f(4)=8$, and $f(5)=1$. $f(1)=10$

Hence

$$ev:\begin{cases} F_{11}[X]\to F_{11}^{\;5} \\ f(X)\ \to (10,6,2,8,1) \end{cases}$$

Example (II. ٤٣): Let us have $u=5$, $q=2$ and $0\leq i\leq 4$. Then it is required to find the Cyclotomic Coset.

Solution: From (Remark (٢.٧.٢.١)), we have $C_{0}=\{0\}$,

, since $1(2)^{0}\bmod 31=1$, $C_{1}=\{1,2,4,8,16\}=C_{2}=C_{4}=C_{8}=C_{16}$

$1(2)^{1}\bmod 31=2$, $1(2)^{2}\bmod 31=4$, $1(2)^{3}\bmod 31=8$, $1(2)^{4}\bmod 31=16$,

. And $C_{3}=\{3,6,12,24,17\}=C_{6}=C_{12}=C_{24}=C_{17}$, since $1(2)^{5}\bmod 31=1$

$3(2)^{0}\bmod 31=3$, $3(2)^{1}\bmod 31=6$, $3(2)^{2}\bmod 31=12$, $3(2)^{3}\bmod 31=24$

, $3(2)^{4}\bmod 31=17$. And also $C_{5}=\{5,10,20,9,18\}=C_{10}=C_{20}=C_{9}=C_{18}$.

$$C_{7}=\{7,14,28,25,19\}=C_{14}=C_{28}=C_{25}=C_{19}.$$

$$C_{11}=\{11,22,13,26,21\}=C_{22}=C_{13}=C_{26}=C_{21}.$$

$$C_{15}=\{15,30,29,27,23\}=C_{30}=C_{29}=C_{27}=C_{23}.$$

Example (II.٤٤): Let us have a field $GF(2^4)$, $f(x)=x^4+x+1$ be a primitive polynomial over $GF(2)$, λ is a root of $f(x)$, and λ is element in $GF(2^4)$. Then it is required to find the trace value of λ in $GF(2^4)$.

Solution: From the (Definition (٢.٧.٣.١)), then

$$Tr_2^{2^4}(x)=x^{2^0}+x^{2^1}+x^{2^2}+x^{2^3}$$

$$=x+x^2+x^4+x^8\ .$$

For λ, $Tr_2^{2^4}(\lambda)=\lambda+\lambda^2+\lambda^4+\lambda^8$

$=\lambda+\lambda^2+\lambda+1+\lambda^2+1$ (from Table (II.٤))

$=0.$ (from Remark (٢.٧.١)).

Example (II.٤٥): Let us have a field $GF(2^2)$, $f(x)=x^2+x+1$ be a primitive polynomial over $GF(2)$, λ is a root of $f(x)$, and λ is element in $GF(2^2)$. Then it is required to find the Trace value of λ in $GF(2^2)$.

Solution:

Let $Tr_2^{2^2}(x)=x+x^2$. For λ, $Tr_2^{2^2}(\lambda)=\lambda+\lambda^2$ (from Definition (٢.٧.٣.١))

$=\lambda+\lambda$ (from Theorem (٢.٧.١.٢))

$=0.$ (from Remark (٢.٧.١)).

Example (II.٤٦): Let us have a field $GF(3^2)$, $f(x)=x^2+x+2$ be a primitive polynomial over $GF(3)$, λ is a root of $f(x)$, and λ is element in $GF(3^2)$. Then it is required to find the Trace value of λ in $GF(3^2)$.

Solution:

Let $Tr_3^{3^2}(x)=x+x^3$. For λ,

(from Definition (٢.٧.٣.١)) $Tr_3^{3^2}(\lambda)=(\lambda+\lambda^3)\bmod 3$

$=(2\lambda+2+\lambda)\bmod 3$ (from table (II.٦) and from Theorem (٢.٧.١.٢))

$=(3\lambda+2)\bmod 3$ (from table (II.٦))

$=2.$

Example (II.٤٧): Let us have an element λ in $GF(2^4)$. Then it is required to find the Trace value of λ in $GF(2^4)$.

Solution: From (Definition (٢.٧.٣.١)) and (Remark (٢.٧.٣.١)), then

, $Tr_4^{2^4}(\lambda)=\lambda+\lambda^4=1$ and $Tr_2^{2^4}(\lambda)=\lambda+\lambda^2+\lambda^4+\lambda^8=0$.$Tr_{2^4}^{2^4}(\lambda)=\lambda$

Example (II.٤٨): Let us have an element $\lambda^7\in GF(2^4)$, $Tr_2^{2^4}(\lambda^7)\in GF(2)$.

Since $Tr_2^{2^4}(\lambda^7)=\lambda^7+\lambda^{7^2}+\lambda^{7^4}+\lambda^{7^8}$ (from Definition (٢.٧.٣.١))

$=\lambda^7+\lambda^{14}+\lambda^{28\bmod 15}+\lambda^{56\bmod 15}$

$=\lambda^7+\lambda^{14}+\lambda^{13}+\lambda^{11}$

$=1\in GF(2).$ (from table (II.٤)).

Example (II.٤٩): Let us have an element λ be a root of the primitive polynomial $f(x)=x^5+x^2+1$. Then it is required to find all the roots of the same primitive polynomial have the same trace value.

Solution:

The root λ and its conjugates (other roots of the same primitive polynomial), $\lambda^2,\lambda^4,\lambda^8$and λ^{16} are elements of $GF(2^5)$. The root powers is called a cyclotomic coset , all the roots of the same primitive polynomial have the same trace value. That is,

(from Definition (٢.٧.٣.١)) $x^{2^0}+x^{2^1}+x^{2^2}+x^{2^3}+x^{2^4}\ Tr_2^{2^5}(x)=$

$$=x+x^2+x^4+x^8+x^{16}\ .$$

For $x=\lambda$, $Tr_2^{2^5}(\lambda)=\lambda+\lambda^2+\lambda^4+\lambda^8+\lambda^{16}$

$=0.$ (from Table (II.٥)).

$$,\ Tr_2^{2^5}(\lambda^2)=\lambda^2+\lambda^{2^2}+\lambda^{2^4}+\lambda^{2^8}+\lambda^{2^{16}}\ x=\lambda^2$$

$$=\lambda^2+\lambda^4+\lambda^8+\lambda^{16}+\lambda^{32\bmod 31}$$

$$=\lambda^2+\lambda^4+\lambda^8+\lambda^{16}+\lambda$$

$$=0.$$

$$,\ Tr_2^{2^5}(\lambda^4)=\lambda^4+\lambda^{4^2}+\lambda^{4^4}+\lambda^{4^8}+\lambda^{4^{16}}\ x=\lambda^4$$

$$=\lambda^{4}+\lambda^{8}+\lambda^{16}+\lambda^{32 \bmod 31}+\lambda^{64 \bmod 31}$$

$$=\lambda^{4}+\lambda^{8}+\lambda^{16}+\lambda+\lambda^{2}$$

$$=0.$$

, $Tr_{2}^{2^5}(\lambda^{8})=\ \lambda^{8}+\lambda^{8^{2}}+\lambda^{8^{4}}+\lambda^{8^{8}}+\lambda^{8^{16}}\ x=\lambda^{8}$

$$=\lambda^{8}+\lambda^{16}+\lambda^{32 \bmod 31}+\lambda^{64 \bmod 31}+\lambda^{128 \bmod 31}$$

$=\lambda^{8}+\lambda^{16}+\lambda+\lambda^{2}+\lambda^{4}$,

$=0.$ (from Table (II.٥)).

, $Tr_{2}^{2^5}(\lambda^{16})=\ \lambda^{16}+\lambda+\lambda^{2}+\lambda^{4}+\lambda^{8}\ \ x=\lambda^{16}$

$=0.$ (from Table (II.٥)).

$$\lambda^{3}+\lambda^{3^{2}}+\lambda^{3^{4}}+\lambda^{3^{8}}+\lambda^{3^{16}}\,Tr_{2}^{2^5}(\lambda^{3})=$$

$$=\lambda^{3}+\lambda^{6}+\lambda^{12}+\lambda^{24}+\lambda^{17}$$

$=1.$ (from Table (II.٥)).

Also, $Tr_{2}^{2^5}(\lambda^{6})=Tr_{2}^{2^5}(\lambda^{12})=Tr_{2}^{2^5}(\lambda^{24})=Tr_{2}^{2^5}(\lambda^{17})=1.$

$Tr_{2}^{2^5}(\lambda^{18})=1.\,Tr_{2}^{2^5}(\lambda^{9})=Tr_{2}^{2^5}(\lambda^{20})=Tr_{2}^{2^5}(\lambda^{10})=Tr_{2}^{2^5}(\lambda^{5})=$

$Tr_{2}^{2^5}(\lambda^{19})=0.\,Tr_{2}^{2^5}(\lambda^{25})=Tr_{2}^{2^5}(\lambda^{28})=Tr_{2}^{2^5}(\lambda^{14})=Tr_{2}^{2^5}(\lambda^{7})=$

$Tr_{2}^{2^5}(\lambda^{21})=1.\,Tr_{2}^{2^5}(\lambda^{26})=Tr_{2}^{2^5}(\lambda^{13})=Tr_{2}^{2^5}(\lambda^{22})=Tr_{2}^{2^5}(\lambda^{11})=$

$$Tr_2^{2^5}(\lambda^{23})=0. Tr_2^{2^5}(\lambda^{27})=Tr_2^{2^5}(\lambda^{29})=Tr_2^{2^5}(\lambda^{30})=Tr_2^{2^5}(\lambda^{15})=$$

$$Tr_2^{2^5}(\lambda^{0})=1.$$

Hence, all roots of an irreducible polynomial $f(x)$ over $GF(q)$ have the same trace.

Example (II. ٥٠): Let us have fields $GF(q)=GF(3)$, $GF(q^u)=GF(3^2)$, $a=1, b=2$ are in $GF(3)$, and $\psi=\lambda^3, \beta=\lambda^7$ are in $GF(3^2)$. Then it is required to find the $Tr(a\psi+b\beta)=aTr(\psi)+bTr(\beta)$.

Solution:

Let $Tr_3^{3^2}(1*\lambda^3+2*\lambda^7)=\sum_{i=0}^{1}(\lambda^3+2\lambda^7)^{3^i}$ (Definition (٢.٧.٣.١))

$=(\lambda^3+2\lambda^7)+(\lambda^3+2\lambda^7)^3$ (Definition (٢.٧.١.٣))

$=\lambda^3+2\lambda^7+\lambda^{9\text{mod}8}+2\lambda^{21\text{mod}8}$ (Lemma (٢.٧.١.١))

$=\lambda^3+2(1+\lambda)+2(2\lambda)$

$=\lambda+2+2\lambda+\lambda+4\lambda,$ (Theorem (٢.٧.١.٢))

$=(8\lambda+2)\text{mod}3$

$=2\lambda+2\ \text{mod}3$

$=2(3)+2\ \text{mod}3$

$=2.$

(Definition (٢.٧.٣.١)) $aTr_q^{q^u}(\psi)+bTr_q^{q^u}(\beta)=1\sum_{i=0}^{1}\psi^{q^i}+2\sum_{i=0}^{1}\beta^{q^i}$

$$=1(\psi+\psi^3)+2(\beta+\beta^3)$$

$$=(\lambda^3+\lambda^{3^3})+2(\lambda^7+\lambda^{7^3})$$

$$=\lambda^3+\lambda^{9\bmod 8}+2\lambda^7+2\lambda^{21\bmod 8}$$

$=\lambda+\lambda+2\ (1+\lambda)+2(2\lambda)$ (Theorem (٢.٧.١.٢))

$$=(8\lambda+2)\bmod 3$$

$$=(2\lambda+2)\bmod 3$$

$$=2(3)+2\bmod 3$$

$$=2.$$

Example ٥١: Let us have fields $GF(q)=GF(2)$, $GF(q^u)=\ GF(2^4)$, and the elements in $GF(2^4)$ are $\{0,1,\lambda,\lambda^2,\ldots\ldots\ldots,\lambda^{14}\}$.Then it is required to find $Tr_2^{2^4}(\lambda)=b$, $\forall\ \lambda$ in $GF(2^4)$ and b any element in $GF(2)$.

Solution:

From (Definition (٢.٧.٣.١)), we have $Tr_2^{2^4}(0)=0$, $Tr_2^{2^4}(1)=0$,

(from table (II.٤)) $\lambda+\lambda^2+\lambda^4+\lambda^8\ Tr_2^{2^4}(\lambda)=$

$=\lambda+\lambda^2+\lambda+1+\lambda+1$ (from Remark (٢.٧.١)).

$$=0.$$

$$\lambda^2+\lambda^{2^2}+\lambda^{2^4}+\lambda^{2^8}\,Tr_2^{2^4}(\lambda^2)=$$

$$=\lambda^2+\lambda^4+\lambda^8+\lambda^{16 \bmod 15}$$

$$=\lambda^2+\lambda+1+\lambda^2+1+\lambda$$

$$=0.$$

$$Tr_2^{2^4}(\lambda^3)=\lambda^3+\lambda^{3^2}+\lambda^{3^4}+\lambda^{3^8}$$

$$=\lambda^3+\lambda^6+\lambda^{12}+\lambda^{24 \bmod 15}$$

$$=\lambda^3+\lambda^3+\lambda^2+\lambda^3+\lambda^2+\lambda+1+\lambda^3+\lambda$$

$$=1.$$

$$\lambda^4+\lambda^{4^2}+\lambda^{4^4}+\lambda^{4^8}\,Tr_2^{2^4}(\lambda^4)=$$

$$=\lambda^4+\lambda^8+\lambda^{16 \bmod 15}+\lambda^{32 \bmod 15}$$

$$=\lambda^4+\lambda^8+\lambda+\lambda^2$$

$$=\lambda+1+\lambda^2+1+\lambda+\lambda^2$$

$$=0.$$

$$\lambda^5+\lambda^{5^2}+\lambda^{5^4}+\lambda^{5^8}\,Tr_2^{2^4}(\lambda^5)=$$

$$=\lambda^5+\lambda^{10}+\lambda^{20 \bmod 15}+\lambda^{40 \bmod 15}$$

$$=\lambda^5+\lambda^{10}+\lambda^5+\lambda^{10}$$

$$=0.$$

$$\lambda^{6}+\lambda^{12}+\lambda^{24}+\lambda^{48}\,Tr_{2}^{2^4}(\lambda^{6})=$$

$$=\lambda^{6}+\lambda^{12}+\lambda^{9}+\lambda^{3}$$

$$=1.$$

$$\lambda^{7}+\lambda^{14}+\lambda^{28}+\lambda^{56}\,Tr_{2}^{2^4}(\lambda^{7})=$$

$$=\lambda^{7}+\lambda^{14}+\lambda^{13}+\lambda^{11}$$

$$=1.$$

$$\lambda^{8}+\lambda^{16}+\lambda^{32}+\lambda^{64}\,Tr_{2}^{2^4}(\lambda^{8})=$$

$$=\lambda^{8}+\lambda+\lambda^{2}+\lambda^{4}$$

$$=0.$$

$$\lambda^{9}+\lambda^{18}+\lambda^{36}+\lambda^{72}\,Tr_{2}^{2^4}(\lambda^{9})=$$

$$=\lambda^{9}+\lambda^{3}+\lambda^{6}+\lambda^{12}$$

$$=1.$$

$$\lambda^{10}+\lambda^{20}+\lambda^{40}+\lambda^{80}\,Tr_{2}^{2^4}(\lambda^{10})=$$

$$=\lambda^{10}+\lambda^{5}+\lambda^{10}+\lambda^{5}$$

$$=0.$$

$$\lambda^{11}+\lambda^{22}+\lambda^{44}+\lambda^{88}\,Tr_{2}^{2^4}(\lambda^{11})=$$

$$=\lambda^{11}+\lambda^{7}+\lambda^{14}+\lambda^{13}$$

$$=1.$$

$$\lambda^{12}+\lambda^{24}+\lambda^{48}+\lambda^{96}\; Tr_2^{2^4}(\lambda^{12})=$$

$$=\lambda^{12}+\lambda^{9}+\lambda^{3}+\lambda^{6}$$

$$=1.$$

$$\lambda^{13}+\lambda^{26}+\lambda^{52}+\lambda^{104}\; Tr_2^{2^4}(\lambda^{13})=$$

$$=\lambda^{13}+\lambda^{11}+\lambda^{7}+\lambda^{14}$$

$$=1.$$

$$\lambda^{14}+\lambda^{28}+\lambda^{56}+\lambda^{112}\; Tr_2^{2^4}(\lambda^{14})=$$

$$=\lambda^{14}+\lambda^{13}+\lambda^{11}+\lambda^{7}$$

$$=1.$$

Example (II. ٥٢): Let us have the fields

. Then it is $GF(q)= GF(2)\subset GF(q^k)=GF(2^2)\subset GF(q^u)=GF(2^4)$

required to find the $Tr_2^{2^2}\ [Tr_{2^2}^{2^4}(x)]\ = Tr_2^{2^4}(x)$.

Solution:

Let $Tr_{2}^{2^2}\ [Tr_{2^2}^{2^4}(x)] = \sum_{j=0}^{2-1}\left(\sum_{i=0}^{\frac{4}{2}-1} x^{2^{2i}}\right)^{2^{j}}$ (Definition (٢.٧.٣.١))

$$= \sum_{j=0}^{1}\left(\sum_{i=0}^{1} x^{2i+j}\right)$$ (Definition (٢.٧.١.٣))

$$= \sum_{j=0}^{1}\ [x^{2^{2(0)+j}} + x^{2^{2+j}}]$$

$$= \sum_{j=0}^{1}\ [x^{2^{j}} + x^{2^{2+j}}]$$

$$= x^{2^0} + x^{2^{2+0}} + x^{2^1} + x^{2^{2+1}}$$

$$= x + x^4 + x^2 + x^8$$

$$= \sum_{i=0}^{3} x^{2^i}$$

$$= Tr_{2}^{2^4}(x).$$

Example (II.٥٣): Let us have the field $GF(q^u) = GF(2^2)$, where λ is an element in $GF(2^2)$ and let minimum polynomial of $m_{\lambda}(x) = \sum_{i=0}^{2} a_i x^{2-i}$. Then it is required to find the $a_1 = -\,Tr_{2}^{2^2}(\lambda)$.

Solution:

By Lemma (٢.٧.٢.١) we get,

$$m_\lambda(x)=\prod_{i=0}^{1}(x-\lambda^{2^i})$$

$$=(x-\lambda)(x-\lambda^2)$$

$$=x^2-(\lambda+\lambda^2)x+\lambda^3.$$

Then $a_1=-(\lambda+\lambda^2).$ (II.١١)

And $Tr_2^{2^2}(\lambda)=\lambda+\lambda^2$ (II.١٢)

From (II.١١) and (II.١٢), we have $a_1=-Tr_2^{2^2}(\lambda)$.

Example (II.٥٤): Let us have a field $GF(3^2)$ (vector space) over $GF(3)$, and the vector space $GF(3^2)^*$ consisting of all linear functionals on $GF(3^2)$. Then it is required to find the basis of $GF(3^2)^*$ over $GF(3)^*$.

Solution:

Firstly, find the elements in the dual space $GF(3^2)^*$.

Let $Tr:GF(3^2)\longrightarrow GF(3^2)$, $\forall x\in GF(3^2), Tr(x)=x+x^3.$

From Theorem (٢.٧.٣.١), $\dim GF(3^2)=\dim GF(3^2)^*$ and from (Remark (٢.٧.٣.١)) [$Tr_{3^2}^{3^2}(\lambda)=\lambda,\ \forall\lambda\in GF(3^2)$], that is,

$$Tr_{3^2}^{3^2}(1^*)=1^*,\dots\dots\dots\dots,Tr_{3^2}^{3^2}(\lambda^{7^*})=\lambda^{7^*}.Tr_{3^2}^{3^2}(0^*)=0^*,$$

Then $0^*,1^*,\lambda^*,\lambda^{2^*},\lambda^{3*},\lambda^{4^*},\dots\dots,\lambda^{7^*}$ are linear functionals on $GF(3^2)$.

Secondly, find the basis of $GF(3^2)^*$, let $\lambda+1=4^*$ and $\lambda+2=5^*$ are elements of $GF(3^2)^*$, since $(1^*,1^*)$ and $(1^*,2^*)$ are linear independent and both generate $GF(3^2)^*$.

Hence, $(1^*,1^*)$ and $(1^*,2^*)$ are basis of $GF(3^2)^*$ over $GF(3)^*$.

Example (II.٥٥) : Let us have a $Tr(x)$ be a linear mapping, $Tr:GF(3^2)\longrightarrow GF(3)$, x_i is a basis of $GF(3^2)$ over $GF(3)$ and $x_j{}^*$ is the basis of $GF(3^2)^*$ over $GF(3)^*$. Then it is required to find the dual basis of the basis of $GF(3^2)$ over $GF(3)$.

Solution:

Since $(1,1)$ and $(1,2)$ are basis of $GF(3^2)$ and $GF(3^2)^*$. Then from equation (٢.٧.٣.٤٦) we get :

$$Tr(4\cdot 4^*)=Tr((\lambda+1)(\lambda+1))$$

$$=Tr\,(\lambda^2+2\lambda+1)$$

$$=Tr\,(2\lambda+1+2\lambda+1) \qquad \text{(from table (II.٦))}$$

$$=Tr\,(4\lambda+2)$$

$$=Tr\,(2\lambda^2)$$

$$=[2\lambda^2+(2\lambda^2)^3]\mathrm{mod}3$$

$$=[2\lambda^2+2^3\lambda^{2^3}]\mathrm{mod}3$$

$=[2\lambda^{2}+2\lambda^{8}]\mathrm{mod}3$ (from Theorem (٢.٧.١.٢))

$=[2(2\lambda+1)+2(1)]\mathrm{mod}3$ (from table (II.٦))

$=(4\lambda+4)\mathrm{mod}3$

$=(\lambda+1)\mathrm{mod}3$

$=(3+1)\mathrm{mod}3$ (from table (II.٦))

$=1.$

Hence $Tr(4\cdot 4^{*})=1.$

$Tr(4\cdot 5^{*})=Tr((\lambda+1)(\lambda+2))$

$=Tr\ (\lambda^{2}+3\lambda+2)$

$=[(\lambda^{2}+3\lambda+2)+(\lambda^{2}+3\lambda+2)^{3}]\ \mathrm{mod}3$

$=[\lambda^{2}+3\lambda+2+(\lambda^{2})^{3}+(3\lambda)^{3}+(2)^{3}]\ \mathrm{mod}3$ (from Lemma (٢.٧.١.١))

$=(2\lambda+6)\mathrm{mod}3$

$=[2(3)+6]\mathrm{mod}3$ (from table (II.٦))

$=0.$

Also similarly, $Tr(5\cdot 4^{*})=0.$

$Tr(5\cdot 5^{*})=Tr((\lambda+2)(\lambda+2))$

$=Tr\ (\lambda^{2}+4\lambda+4)$

$=Tr\ (2\lambda+1+4\lambda+4)$

$$=Tr\,(6\lambda+5)$$

$$=[(6\lambda+5)+(6\lambda+5)^3]\mathrm{mod}3$$

$$=[6\lambda+5+(6\lambda)^3+(5)^3]\mathrm{mod}3$$ (from Lemma (٢.٧.١.١))

$$=[6\lambda+5+2^3]\mathrm{mod}3$$

$$=[6\lambda+5+2]\mathrm{mod}3$$ (from Theorem (٢.٧.١.٢))

$$=[6\lambda+7]\mathrm{mod}3$$

$$=[6(3)+7]\mathrm{mod}3$$

$$=1.$$

Hence, $\{4^*, 5^*\}$ are dual basis of the basis $\{4, 5\}$ of $GF(3^2)$ over $GF(3)$.

Example (II.٥٦): Let us have a polynomial $f(x)=x^2+4x+4$ over $GF(2^3)$. Then it is required to consider the polynomial $f(x)$ is square-free or not .

- The derivative of $f(x)$, $f^{(1)}(x)=2x+4$, the

$$GCD(f(x), f^{(1)}(x))=x+2=f_1(x).$$

- $f_2(x)=f(x)/f_1(x)=(x^2+4x+4)/(x+2)$

$$=(x+2)^2/(x+2)$$

$=x+2$, is the proper factor of $f(x)$.

- The derivative of $f^{(1)}(x)$, $f^{(2)}(x)=2$. Hence the degree of $f^{(2)}(x)$ is not positive integer, that is, the $\gcd(f_2(x), f^{(2)}(x))=(x+2, 2)=1.$

Example (II. ٥٧): Let us have a [٥, ٤] – code over a binary alphabet. From (Definition (٣.٢.١.١)) that is, we constructed a code with ١٦ codewords, each code being ٥ – tuple (block length ٥) and each component of ٥ – tuple being ٠ or ١ [٣].

Example (II. ٥٨): Let message blocks of three digits and by encoder transforms each message block into a code vector of six digits as follows:

Table II. ٩ : shows the Encoder of the Message Block .

Message	Encoder	Code vector
٠٠٠	⟷	٠٠٠٠٠٠
٠٠١	⟷	٠٠١١٠١
٠١٠	⟷	٠١٠٠١١
٠١١	⟷	٠١١١١٠
١٠٠	⟷	١٠٠١١٠
١٠١	⟷	١٠١٠١١
١١٠	⟷	١١٠١٠١
١١١	⟷	١١١٠٠٠

Since $k=3$, there are $2^3=8$ possible distinct messages. All codewords are distinct. The set of codewords a ٣-dimensional subspace of the vector space of all ٦-tuple. Therefore, it is a linear code [٣].

Example (II.٥٩): Let us have a code word $v = (1001011000\,1)$, then it is required to find the Hamming weight ($w(v)$) of v.

Solution: From (Definition (٣.٢.١.٣)) , then $w(v)$ =٥ [٣].

Example (II.٦٠): Let us have the alphabet $A=\{0,1\}$, the codewords $u = (1001011000\,1)$ and $v = (1100101010\,1)$. Then it is required to Hamming distance $d(u,v)$ between two code words u and v.

Solution: Let u - $v = (0101110010\,0)$. From (Definition (٣.٢.١.٤)),then $d(u,v)$=٥ [٣].

Example (II.٦١): Let us have codewords u and v over the alphabet $A=\{0,1,2\}$ given by $u=(2\,1\,0\,0\,2)$, $v=(1\,2\,0\,0\,1)$. Then it is required to Hamming distance $d(u,v)$ between two code words u and v.

Solution: From (Definition (٣.٢.١.٤)), we have $d(x,y)=3$ [٣].

Example (II.٦٢): Let us have code words $u = (1001011000\,1)$ and $= (1100101010\,1)$. Then it is required to show that $d(u,v) = w(u+v)$ .v

Solution: Let $u+\ v\ = (0101110010\,0)$. From (Remark (٣.٢.١.١)), we have $d(u,v)$=٥ and $w(u+v)$=٥ [٣].

Example (II. ٦٣): Let us have a polynomial $g(x) = 1 + x + x^3$ and is a factor of $f(x) = x^7 + 1$ Then it is required to generate the code from $g(x)$.

Solution: Since $f(x)$ can be factor as

. Then from (Theorem (٣.٢.١.٣)), the $[7,4]-$ $x^7 + 1 = (1 + x + x^3)(1 + x + x^2 + x^4)$ code a generated by $g(x) = 1 + x + x^3$ has code polynomials or code vectors as shown in equation (٣.٢.١.٤٩). The minimum distance of this code is ٣. And the code has a single-error-correcting code [٣,١٥].

Example (II. ٦٤): Let us have a $[7,4]-$cyclic code with generator polynomial $g(x) = 1 + x + x^3$. Then it is required to generate the parity polynomial of the cyclic code .

Solution: Since $x^n + 1 = g(x)h(x)$, then from (Remark (٣.٢.١.٥)), we have $h(x) = (x^7 + 1)/(1 + x + x^3) = 1 + + x^2 + x^4$ [٣].

Example (II. ٦٥): Let us have a $[7,3]$ $RS-$code over $GF(2^3)$ and let $m(x) = 7x^2 + 2x + 5$, $\deg(m) < 3$. Then it is required to find the Reed Solomon Code.

Solution: From (Definition (٣.٢.٢.١)), we can compute

, $m(2) = 5,\ m(3) = 2,\ m(4) = 5,\ m(5) = 6,\ m(6) = 5,\ m(7) = 2 . m(1) = 6$

Thus, the code is $(6, 5, 2, 5, 6, 5, 2)$.

Example (II. ٦٦): Let us have a $[8,5]\,RS_5$ code over F_{11} is the following set of 8-tuples (codeword): $RS_5 = \{ev(m):\ m \in F_{11}[x], \deg(m) < 5\}$, and over F_{11}. Then it is required to find the Reed $m(x) = 7x^4 + 8x^3 + 10x^2 + 8x + 2$ Solomon Code.

Solution: From (Definition (٣.٢.٢.١)), we can compute

$$m(1) = 2,\ m(2) = 3,\ m(3) = 8,\ m(4) = 1,\ m(5) = 2,\ m(6) = 1, m(7) = 2, m(8) = 1.$$

Thus, the code is $RSC = (2\ 3\ 8\ 1\ 2\ 1\ 2\ 1)$.

Example (III. ١) : Let us have a square matrix A of dimension (٣ x ٣) over $GF(47^2)$, $A = \begin{bmatrix} 1291 & 776 & 1397 \\ 1969 & 1281 & 1685 \\ 157 & 1538 & 783 \end{bmatrix}$. Then it is required to generate a polynomial f over $GF(47^2)$ from the matrix A by using the Algorithm (٤.١.١- A).

Solution:

f = ١.٠e+٠٠٣ * [٠.٠٠١٠ ١.٠٦٣٠ ٠.٣٨٠٠ ٠]

Example (III. ٢): Let us have a square matrix A of dimension (٤ x ٤) over $GF(2^{15})$, $A = \begin{bmatrix} 12374 & 3415 & 3342 & 1235 \\ 3675 & 2340 & 3432 & 6712 \\ 2319 & 3210 & 24021 & 10419 \\ 28463 & 205 & 10523 & 32165 \end{bmatrix}$. Then it is required to generate a polynomial f over $GF(2^{15})$ from the matrix A by using the Algorithm (٤.١.١- A) :

Solution:

f = ١.٠e+٠٠٤ *[٠.٠٠٠١   ٢.٧٤٠٤   ٢.٤٣٨٤   ١.٠٠١٩   ٠.٦٩٧٦]

Example (III. ٣): Let us have a square matrix A of dimension (٤ x ٤) over F ,

$$A=\begin{bmatrix} -3 & -2 & -1 & -5 \\ -4 & -2 & -3 & -1 \\ -9 & -5 & -1 & -6 \\ -5 & -7 & -2 & -5 \end{bmatrix}$$

. Then it is required to generate a polynomial f over F from the matrix A by using the Algorithm (٤.١.١- A).

Solution:

f = ١   ١١   -٣٦   ١٤٦   -٣٢٠

Example (III. ٤): Let us have a square matrix A of dimension (٣ x ٣) over Q,

$$A=\begin{bmatrix} 3.2 & 4.7 & 5.3 \\ 3.3 & 6.6 & 9.8 \\ 2.1 & 4.5 & 8.3 \end{bmatrix}$$

. Then it is required to generate a polynomial f over Q from the matrix A by using the Algorithm (٤.١.١- A).

Solution:

f = ١.٠٠٠٠   -١٨.١٠٠٠   ٣١.٧٢٠٠   -٧.٤١٦٠

Example (III. ٥) : Let us have polynomials $f(x)=994x^2+501x+37$ and $g(x)=22x+17$ over $GF(2^{15})$. Then it is required to compute multiplication polynomial and division polynomial of polynomials f and g by using the Algorithm (٤.١.١- B).

Solution:

h = GF(٢^١٥) array. Primitive polynomial = X^١٥+X+١ (٣٢٧٧١ decimal)

Array elements = ١٣٩٣٢   ٩٩٠٠   ٧٢١١   ٦٢٩

quot = GF(٢^١٥) array. Primitive polynomial = X^١٥+X+١ (٣٢٧٧١ decimal)

Array elements = ٢٩٣٩٣   ١٥٦١٨

rem = GF(٢^١٥) array. Primitive polynomial = X^١٥+X+١ (٣٢٧٧١ decimal)

Array elements = ٠   ٠   ٢٧٩١٨.

Example (III. ٦) : Let us have polynomials $f(x)=2.5x^2+3.1x+5.4$ and $g(x)=1.1x^2+2.1x+4.2$ in $Q[x]$ over Q. Then it is required to

compute multiplication polynomial and division polynomial of polynomials f and g by using the Algorithm (٤.١.١- B).

Solution:

quot = ٢.٢٧٢٧

rem = ٠   -١.٦٧٢٧   -٤.١٤٥٥

Example (III. ٧): Let us have a polynomial $f(x)$ over $GF(101^7)$. Then it is required to evaluate of polynomial f at $x=10, 30, 56,90,1200$ by using the Algorithm (٤.١.٢- A).

Solution:

f = ١.٠e+٠١٣ *[٨.٩٨٥٨   ٠.٢١٠٦   ٧.٣٠٤٢   ٤.٠٦٨٦   ٨.٩١٨٠   ٥.٣٩٠٨]

```
v = ١.٠e+٠١٣ *[ ٣.٠٦٢٩   ٧.٤٤٠٣   ٨.٢٣٨٥   ٩.٧١١٢   ٣.٥١٨٤]
```

Example (III.٨): Let us have a polynomial $f(x) = 24x^2 + 33x + 9$ over $GF(2^{15})$. Then it is required to evaluate f at $x = 25, 50, 60$ by using the Algorithm (٤.١.٢- A).

Solution:

```
ev = GF(٢^١٥) array. Primitive polynomial = X^١٥+X+١ (٣٢٧٧١ decimal)

 Array elements = ٧٤٦٤      ٣٢٢٨٣      ٣٠٧٧٣.
```

Example (III. ٩) : Let us have the polynomial $f(x) = 37.34x^2 + 266.21x + 2.800$ over Q. Then it is required to evaluate the polynomial f at $x = 12.25, -56.7, 90.078$ using the Algorithm (٤.١.٢-A).

Solution:

```
ev =١.٠e+٠٠٥ *[٠.٠٨٨٧   ١.٠٤٩٥   ٣.٢٦٩٦].
```

Example (III. ١٠) : Let us have a polynomial $f(x)$ over $GF(101^3)$. Then it is required to find the roots of this polynomial over $GF(101^3)$ using the algorithm (٤.١.٢- B).

Solution:

```
f = Columns ١ through ٧

 ٤٧٠٢٩٩ ١٩٠٦٥  ٨٤٦٢٩٦  ٤٥٨١٧٨   ٦٣٤٠٨٠    ٨١٥٩٣٣  ٩٤٩٧٤٤

ev =Columns ١ through ٦
```

```
٧٢٣٩١     ٤٨٧٩٥٥     ٦٥٨١٨٧     ٣٢٦٧٤٧     ٣٧٧١٨٠     ٢٧٦٥٤١

Columns ٧ through ١٢

٣١٦٧٧٦     ٤١١٤٥١     ٥٩٩٣٣٤     ١٦٣٩٢٧     ٥٢٠٤٥٣     ٥٣٦٩٨٧
```

That is, $f(x)$ has no roots over $GF(101^3)$.

Example (III. ١١): Let us have a polynomial $f(x)=22x^3+15x^2+20x+1$ over $GF(2^{14})$. Then it is required to find the roots of this polynomial over $GF(2^{14})$ by using the Algorithm (٤.١.٢- B).

Solution:

gfpolynomial = GF(٢^١٤) array. Primitive polynomial = X^١٤+X^١٠+X^٦+X+١ (١٧٤٧٥ decimal).

Array elements = ٢٢   ١٥   ٢٠   ١

r = GF(٢^١٤) array. Primitive polynomial = X^١٤+X^١٠+X^٦+X+١ (١٧٤٧٥ decimal)

Array elements =

That is, $f(x)$ has no roots over $GF(2^{14})$.

Example (III. ١٢) : Let us have a polynomial $f(x)=5x^2+4x+2$ over F. Then it is required to find the roots of this polynomial over F by using the Algorithm (٤.١.٢- B).

Solution:

r =-٠.٤٠٠٠ + ٠.٤٨٩٩i

r = - ٠.٤٠٠٠ - ٠.٤٨٩٩i .

Example (III. ١٣) : Let us have a field $GF(97^{14})$. It is required to generate a monic polynomial $f(x)$ of degree ٥ over $GF(97^{14})$ by using the Algorithm (٤.١.٢- D).

Solution:

```
p =  ١.٠e+٠٢٧ * [٠.٠٠٠٠   ٠.٣٧٧٩   ٢.٣٠٣٧   ٥.٣٠٨٦   ٠.٠٦٤٤   ٠.٩٠٦٧]
```

Example (III. ١٤) : Let us have a field $GF(2^{15})$. Then it is required to generate a monic polynomial $f(x)$ of degree ٦ over $GF(2^{15})$ by using the Algorithm (٤.١.٢- D).

Solution:

```
 f = Columns ١ through ٧

  ١    ٦٦٤٥    ٦٥١٢    ١٩٧٨٥    ٨٩١٩    ٦٥١٥    ٥٠١.
```

Example (III. ١٥): Let us have a field $GF(11^2)$. Then it is required to generate a default primitive polynomial over $GF(11^2)$ by using the Algorithm (٤.١.٢-E).

Solution:

```
defpoly = ٧    ١    ١.
```

Example (III. ١٦) : Let us have a field $GF(2^{16})$. Then it is required to generate a default primitive polynomial over $GF(2^{16})$ by using the Algorithm (٤.١.٢-E).

Solution:

Primitive polynomial(s) = X^١٦+X^٥+X^٣+X^٢+١

defaultprimpoly = ٦٥٥٨١.

Example (III. ١٧) : Let us have a field $GF(11^{2})$. It is required to generate all the primitive polynomials over $GF(11^{2})$ by using the Algorithm (٤.١.٢- F).

Solution:

allpol = [٧ ١ ١], [٨ ١ ١], [٦ ٢ ١], [٦ ٣ ١], [٨ ٣ ١], [٢ ٤ ١],

[٧ ٤ ١], [٢ ٥ ١], [٢ ٦ ١], [٢ ٧ ١], [٧ ٧ ١], [٦ ٨ ١], [٨ ٨ ١],

[٦ ٩ ١], [٧ ١٠ ١], [٨ ١٠ ١].

Example (III. ١٨): Let us have a field $GF(2^{16})$. Then it is required to generate a primitive polynomial over $GF(2^{16})$ by using the Algorithm (٤.١.٢- F).

Solution:

Primitive polynomial(s) = X^١٦+X^٥+X^٣+X^٢+١

defaultprimpoly = ٦٥٥٨١.

Example (III. ١٩): Check the polynomial $f(x)=31+23x+11x^2$ over $GF(97)$ is primitive or not by using the algorithm (٤.١.٢- G).

Solution:

ck = ٠

Example (III. ٢٠): Check the polynomials $f_1(x)=1+x$, $f_2(x)=2+x$ and $f_3(x)=2x$ over $GF(3^2)$ is primitive or not by using the algorithm (٤.١.٢- G).

Solution:

p١ = [١ ١], ck = ١

p٢ = [٢ ١], ck = ٠

p٣ = [٠ ٢], ck = -١

That is, $p_1(x)=1+x$ is a primitive polynomial, $p_2(x)=2+x$ is irreducible but not a primitive polynomial for $GF(3^2)$ and $p_3(x)=2x$

is not an irreducible polynomial .

Example (III. ٢١): Let us have a polynomial $f(x)=x^{16}+x^5+x^3+x^2+1$ (decimal ٦٥٥٣٦) over $GF(2^{16})$. Then it is required to check a polynomial $f(x)$ is primitive or not.

Solution:

ck١ = ٠. Then $f(x)$ is not primitive.

Example (III. ٢٢): Let us have a field $GF(11^2)$. It is required to generate a minimal polynomial of the element λ^9 in $GF(11^2)$ by using the algorithm (٤.١.٢- l).

Solution:

p = ٨ ٧ ١

Example (III. ٢٣): Let $GF(11^2)$ be an extension field, generate the minimal polynomial of an element λ^6 in $GF(11^2)$ based on the primitive polynomial over $GF(11^2)$ by using the algorithm (٤.١.٢- l).

Solution:

prim_ poly = ٧ ١ ١

pol = ٤ ٠ ١.

Example (III. ٢٤): Let us have data points $(1, 4)$, $(4, 2)$, $(6, 1)$,$(8, 9)$, $(43,10)$, $(67,20)$ and $(90, 45)$ over $GF(101^2)$. It is required to generate a unique polynomial of degree $k=6$ that length $n=7$ by using the algorithm (٤.١.٢- k).

Solution:

s١ =٢٠٧٣٦*(z-٤)*(z-٦)*(z-٨)*(z-٤٣)*(z-٦٧)*(z-٩٠)+٩٦٨٠*(z-١)*(z-٦)*(z-

٨)   *(z-٤٣)*(z-٦٧)*(z-٩٠)+٤٩٢١*(z-١)*(z-٤)*(z-٨)*(z-٤٣)*(z-٦٧)*(z-٩٠)   +
٨٥٥٩٩*(z-١)*(z-٤)*(z-٦)*(z-٤٣)*(z-٦٧)*(z-٩٠)+٧٠٩٦٠*(z-١)*(z-٤)*(z-٦)*(z-٨)*(z-
٦٧)*(z-٩٠)+١٠٨٤٠*(z-١)*(z-٤)*(z-٦)*(z-٨)*(z-٤٣)*(z-٩٠)+   ٣١٤١٩٠*(z-١)*(z-
٤)*(z-٦)*(z-٨)*(z-٤٣)*(z-٦٧)

r =١٦٩٢٦*z^٦-٨٠٣٧٨٣٦٠*z^٥+٤١٧٥٤٢٣٨٤٠*z^٤-٨٤٠١٣٣٤٣١٨٠ *

z^٣+٦٥٣٤٧٣٣٤٧٣١٤*z^٢-٢٠٢٦٧٠٨١٦٤٣٨٠*z+١٩٩٠٣٠٤٩٩٢٠٨٠

poll = ٨   ٦٦   ١٠   ١٠٠   ٧٣   ٩٠   ٦٠

rr = ٨*x^٦+٦٦*x^٥+١٠*x^٤+١٠٠*x^٣+٧٣*x^٢+٩٠*x+٦٠.

Example (III. ٢٥): Let us have a $[34,26]$ $RS-$code over $GF(97^2)$ and $m(x)$ be a message , $\deg(m)<26$. Then it is required to compute the Reed Solomon code by using the algorithm (٤.١.٣- A).

Solution:

m= Columns ١ through ٦

```
    ٩٢٧٥      ٥٧٢٦      ٧٩١٤      ٦٦٠٨      ٧٣٥٤      ٥١٣٣
```

Columns ٧ through ١٢

```
    ٤٦٦٤      ٨٨٨٠      ٣١٢٩      ٣٥٢٥      ٩٢٨٧       ٦٣٢
```

Columns ١٣ through ١٨

```
    ٥٣٢٩      ٧٥٩٠      ٢٧١٥      ٤٢٠٥      ٤٧٧١      ١٣٤٨
```

Columns ١٩ through ٢٤

```
    ٨١٤٨      ٢٦٢٠      ٧٧٤٣      ٥٩٣٦      ٧٤٠١      ٥٢٠٩

  Columns ٢٥ through ٢٦

    ٧٨٣٥      ٣٥٣٤

C =  ١.٠e+٠٢٦ *

  Columns ١ through ٨

   ٠.٠٠٠٠   ٠.٠٠٠٠   ٠.٠٠٠٠        ٠        ٠        ٠        ٠        ٠

  Columns ٩ through ١٦

        ٠        ٠        ٠        ٠        ٠   ٠.٠٠٠٠        ٠  -٠.٠٠٠٠

  Columns ١٧ through ٢٤

        ٠        ٠        ٠        ٠        ٠   ٠.٠٠٠٠        ٠        ٠

  Columns ٢٥ through ٣٢

  -٠.٠٠١٥        ٠        ٠        ٠  -٠.٠٤٨٤        ٠        ٠        ٠

  Columns ٣٣ through ٣٤

   ١.٥٤٧٤        ٠
```

Example (III. ٢٦): Let us have a $[31,3]$ $RS-$code over $GF(2^5)$. It is required to generate the generator polynomial of the code by using the algorithm (٤.١.٣-C).

Solution:

Primitive polynomial(s) = X^٥+X^٢+١

```
pr = ٣٧

genpoly٢ = GF(٢^٥) array. Primitive polynomial = X^٥+X^٢+١
 (٣٧ decimal)

 Array elements = Columns ١ through ١٥

   ١   ٢٦   ١٤   ٢٩   ٩   ٢٧   ٢٠   ١٨   ١٤   ٢٨   ١٨   ١٥   ٧  ٦   ٢٨

  Columns ١٦ through ٢٩

   ١٩   ٢٠   ١٩   ٢١   ٨   ١   ٢٧   ٢١   ٩   ٢٦   ١٥   ٦   ٢٩   ٨
```

Example (III. ٢٧): Let us have a message word [٤ ٠ ٦] over $GF(2^3)$ using a $[7, 3]$ RS encoder. And corrupts the code by introducing two errors [٣ ٤ ٠ ٠ ٠ ٠ ٠] in the code word. It is required to compute the decoding Reed Solomon code and recover the message by using the Algorithm (٤.١.٣-D).

Solution:

```
code = GF(٢^٣) array. Primitive polynomial = X^٣+X+١ (١١ decimal)

Array elements =  ٤    ٠    ٦    ٤    ٢    ٢    ٠

 noisycode = GF(٢^٣) array. Primitive polynomial = X^٣+X+١ (١١ decimal)

Array elements =  ٧    ٤    ٦    ٤    ٢    ٢    ٠


dec = GF(٢^٣) array. Primitive polynomial =X^٣+X+١ (١١ decimal)

 Array elements =  ٤    ٠    ٦

cnumerr =
```

٢

Note that, the $DRSC$ can correct at most two errors in each word, since $t=(n-k)/2=2$.

Example (III. ٢٨): Let us have a message word [٥ ١ ١] over $GF(2^3)$ using a $[7,3]\,RS$ encoder. It corrupts the code by introducing three errors [٥ ٦ ٧ ٠ ٠ ٠ ٠] in the code word. It is required to compute the decoding Reed Solomon code and recover the message by using the Algorithm (٤.١.٣-D).

Solution:

code = GF(٢^٣) array. Primitive polynomial = X^٣+X+١ (١١ decimal)

Array elements = ٥ ١ ١ ٤ ٥ ٤ ٠

noisycode = GF(٢^٣) array. Primitive polynomial = D^٣+D+١ (١١ decimal)

Array elements = ٠ ٧ ٦ ٤ ٥ ٤ ٠

dec = GF(٢^٣) array. Primitive polynomial = X^٣+X+١ (١١ decimal)

Array elements = ٠ ٧ ٦

cnumerr = -١

Note that, the $DRSC$ cannot recover the message word.

Example (III. ٢٩): Let us have $GF(q)=GF(11)$, $n=8$, $k=3$, $w=1$, $W=3$, the cipher text $y=(7,10,1,10,0,3,7,1)$ and the public key $Z=(9,6,9,6,5,9,10,8)$. Then it is required to recover the message by using the algorithm (٤.١.٤- D).

Solution:

mat٣ =

```
[  ٧-٩*L,  ٧-٩*L   ]
[ ١٠-٦*L, ٢٠-١٢*L]
[  ١-٩*L,  ٣-٢٧*L  ]
[ ١٠-٦*L, ٤٠-٢٤*L]
[   -٥*L,  -٢٥*L   ]
[  ٣-٩*L, ١٨-٥٤*L ]
[ ٧-١٠*L, ٤٩-٧٠*L]
[  ١-٨*L,  ٨-٦٤*L  ]
```

mat٩ =

```
[  ٧-٩*L,  ٧-٩*L,     ١٠,     ١٠,     ١٠,    ١٠]
[ ١٠-٦*L, ٢٠-١٢*L,   ١٠,      ٩,      ٧,      ٣]
[  ١-٩*L,  ٣-٢٧*L,    ١٠,      ٨,      ٢,      ٦]
[ ١٠-٦*L, ٤٠-٢٤*L,   ١٠,      ٧,      ٦,      ٢]
[   -٥*L,  -٢٥*L,      ١٠,      ٦,      ٨,      ٧]
[  ٣-٩*L, ١٨-٥٤*L,   ١٠,      ٥,      ٨,      ٤]
[ ٧-١٠*L, ٤٩-٧٠*L,   ١٠,      ٤,      ٦,      ٩]
[  ١-٨*L,  ٨-٦٤*L,    ١٠,      ٣,      ٢,      ٥]
```

```
 MM =


[ ٧-٩*conj(L), ٧-٩*conj(L), ١٠,    ١٠,    ١٠,     ١٠]

[١٠-٦*conj(L),   ٩-conj(L),  ١٠,     ٩,     ٧,      ٣]

[ ١-٩*conj(L), ٣-٥*conj(L),  ١٠,     ٨,     ٢,      ٦]

[١٠-٦*conj(L), ٧-٢*conj(L),  ١٠,     ٧,     ٦,      ٢]

[  -٥*conj(L),  -٣*conj(L),   ١٠,     ٦,     ٨,      ٧]

[ ٣-٩*conj(L),٧-١٠*conj(L),  ١٠,     ٥,     ٨,      ٤]

[٧-١٠*conj(L), ٥-٤*conj(L),  ١٠,     ٤,     ٦,      ٩]

[ ١-٨*conj(L), ٨-٩*conj(L),  ١٠,     ٣,     ٢,      ٥]


d = -٣٦٢٤٠+٥٧٧٠٠*conj(L)+٣٣٨٠*conj(L)^٢


f =  ٣    ٥    ٥


ev =  ٢    ٥    ٣    ٧    ٦    ٠    ٠    ٦
```

That is, f(x) have ٦, ٧ roots.

L=٧ is a primitive element over GF(١١).

```
mat٩ =

   ١٠   ١٠   ١٠   ١٠   ١٠   ١٠

    ١    ٢   ١٠    ٩    ٧    ٣

    ٤    ١   ١٠    ٨    ٢    ٦
```

١	٤	١٠	٧	٦	٢
٩	١	١٠	٦	٨	٧
٦	٣	١٠	٥	٨	٤
٣	١٠	١٠	٤	٦	٩
٠	٠	١٠	٣	٢	٥

V= ٨ ٧

N= ٥ ١ ١

message = ٢ ٨.

Example (III. ٣٠) : Let us have a field $GF(q^u) = GF(11^2)$, and $n=11$, $k=5$, $u=2$, $w=1$, $y=(2,2,6,6,6,3,7,0,3,5,1)$, $Z_1=(2,5,0,4,9,0,4,0,5,4,6)$ and $Z_2=(5,6,9,10,6,8,2,9,4,5,1)$. It is required to recover the message from the cipher text y and public keys Z_1, Z_2 by using the algorithm (٤.١.٥- D).

Solution:

v = [a+b, a+٢*b, a+٣*b, a+٤*b, a+٥*b, a+٦*b, a+٧*b, a+٨*b,

a+٩*b, a+١٠*b, a+١١*b]

F = [٢*a+٢*b, ٢*a+٤*b, ٦*a+١٨*b, ٦*a+٢٤*b, ٦*a+٣٠*b, ٣*a+١٨*b,

٧*a+٤٩*b, ٠, ٣*a+٢٧*b, ٥*a+٥٠*b, a+١١*b]

R =[٢*c+٢*d+٥*e+٥*f, ٥*c+١٠*d+٦*e+١٢*f, ٩*e+٢٧*f,

```
 ٤*c+١٦*d+١٠*e+٤٠*f,      ٩*c+٤٥*d+٦*e+٣٠*f,                    ٨*e+٤٨*f,

٤*c+٢٨*d+٢*e+١٤*f,              ٩*e+٧٢*f,              ٥*c+٤٥*d+٤*e+٣٦*f,

٤*c+٤٠*d+٥*e+٥٠*f,      ٦*c+٦٦*d+e+١١*f]

N =[   n١+n٢+n٣+n٤,          n١+٢*n٢+٤*n٣+٨*n٤,     n١+٣*n٢+٩*n٣+٢٧*n٤,
n١+٤*n٢+١٦*n٣+٦٤*n٤,                             n١+٥*n٢+٢٥*n٣+١٢٥*n٤,
n١+٦*n٢+٣٦*n٣+٢١٦*n٤,                            n١+٧*n٢+٤٩*n٣+٣٤٣*n٤,
n١+٨*n٢+٦٤*n٣+٥١٢*n٤,                            n١+٩*n٢+٨١*n٣+٧٢٩*n٤,
n١+١٠*n٢+١٠٠*n٣+١٠٠٠*n٤, n١+١١*n٢+١٢١*n٣+١٣٣١*n٤]



matofanalysis =



[  conj(٢*a+٢*b-٢*c-٢*d-٥*e-٥*f-n١-n٢-n٣-n٤)                  ]

[  conj(٢*a+٤*b-٥*c-١٠*d-٦*e-١٢*f-n١-٢*n٢-٤*n٣-٨*n٤)          ]

[  conj(٦*a+١٨*b-٩*e-٢٧*f-n١-٣*n٢-٩*n٣-٢٧*n٤)                 ]

[  conj(٦*a+٢٤*b-٤*c-١٦*d-١٠*e-٤٠*f-n١-٤*n٢-١٦*n٣-٦٤*n٤)    ]

[  conj(٦*a+٣٠*b-٩*c-٤٥*d-٦*e-٣٠*f-n١-٥*n٢-٢٥*n٣-١٢٥*n٤)    ]

[  conj(٣*a+١٨*b-٨*e-٤٨*f-n١-٦*n٢-٣٦*n٣-٢١٦*n٤)              ]

[  conj(٧*a+٤٩*b-٤*c-٢٨*d-٢*e-١٤*f-n١-٧*n٢-٤٩*n٣-٣٤٣*n٤)    ]

[  conj(-٩*e-٧٢*f-n١-٨*n٢-٦٤*n٣-٥١٢*n٤)                       ]

[  conj(٣*a+٢٧*b-٥*c-٤٥*d-٤*e-٣٦*f-n١-٩*n٢-٨١*n٣-٧٢٩*n٤)    ]

[  conj(٥*a+٥٠*b-٤*c-٤٠*d-٥*e-٥٠*f-n١-١٠*n٢-١٠٠*n٣-١٠٠٠*n٤)]

[  conj(a+١١*b-٦*c-٦٦*d-e-١١*f-n١-١١*n٢-١٢١*n٣-١٣٣١*n٤)     ]


    V=  ٣    ٥
```

R١= ٢   ٧

R٢= ٩   ٤

N= ٤   ٦   ١٠   ١

message = ٥   ١   ٩.

١. ١ Introduction:

Cryptography is one of the oldest fields of technical study we can find records of, and is went back at least ٤,٠٠٠ years. It is quite noteworthy that of all the cryptosystems developed in those ٤,٠٠٠ years of effort, only ٣ systems in widespread serious use remain hard enough to break to be of real value. One of them takes too much space for most practical uses, another is too slow for most practical uses, and the third is widely believed to contain serious weaknesses. There are many notable personalities who participated in the evolution of Cryptography. For example, " ***Julius Caesar (١٠٠-٤٤ BC)*** " [٢١] , used a simple substitution with the normal alphabet in government communications", and later [٢١].

The Cryptographic is a term which refers to the design of cryptosystems and cryptanalysis. This science is divided into three parts; the cryptosystem designing part which is specialized in designing and constructing cryptosystems, the cryptanalysis part which is specialized in finding techniques and methods of transforming the cipher text to plain text, and the evaluation of the algorithms part which is specialized in calculating the complexities of these algorithms [٨, ٢٠].

In modern cryptography, the development in ١٩٧٦ was perhaps even more important, for it fundamentally changed the way crypto systems might work.. The problems of authentication large network privacy protection were addressed theoretically in ١٩٧٦ by Whitfield Diffie and Martin Hellman when they published their concepts for a method of exchanging secret messages without exchanging secret keys. The idea came to fruition in ١٩٧٧ with the invention of the RSA Public Key Cryptosystem by Ronald Rivest, Adi Shamir, and Len Adleman, then professors at the Massachusetts Institute of Technology. Rather than using the same key to both encrypt and decrypt the data, the RSA system uses a matched pair of encryption and decryption keys. Each key performs a one-way transformation upon the data. Public key is made publicly available by its owner, while the RSA Private Key is kept secret. To send a private message, an author scrambles the each key is the inverse function of the other; what one does, only the other can undo the RSA message with the intended recipient's public key. Once so encrypted, the message can only be decoded with the recipient's private key [٢١].

Inversely, the user can also scramble data using their private key; in other words, RSA keys work in either direction. This provides the basis for the "digital signature " for if the user can unscramble a message with someone's Public Key, the other user must have used their Private Key to scramble it in the first place. Since only the owner can utilize their own private key, the scrambled message becomes a kind of electronic signature which is a document that nobody else can produce [٢١].It is an important goal in cryptology to find difficult problems to design cryptographic primitives, and it is a major area of research to establish these primitives and demonstrate their security through reductions to those new hard problems [٣٠].

The problem decoding of Reed-Solomon Codes is quite old and has received much interest from coding theorists since the introduction of these codes [٣٠]. The goal of decoding is to retrieve a word of the Reed-Solomon Code from a corrupted word, that is, a word containing a small number of errors. More recently, important progress has been done to extend the number of errors which can be corrected [٢٢]. Thus the problem of decoding Reed-Solomon error – correcting codes is easy when the number of errors is small.

On the other hand, this problem has an equivalent formulation under the name ***Polynomial Reconstruction (PR)***, is an important problem in cryptography application. The ***PRP*** has been introduced in ١٩٩٩ as a new hard problem. Several cryptographic primitives established on this problem have been constructed. Then it has been studied from the point of view of robustness, and several important properties have been discovered and proved. Furthermore many researchers constructed asymmetric cipher based on the ***PRP*** [٣٠]. The (Figure ١.١) shows the development directions of cryptosystems .

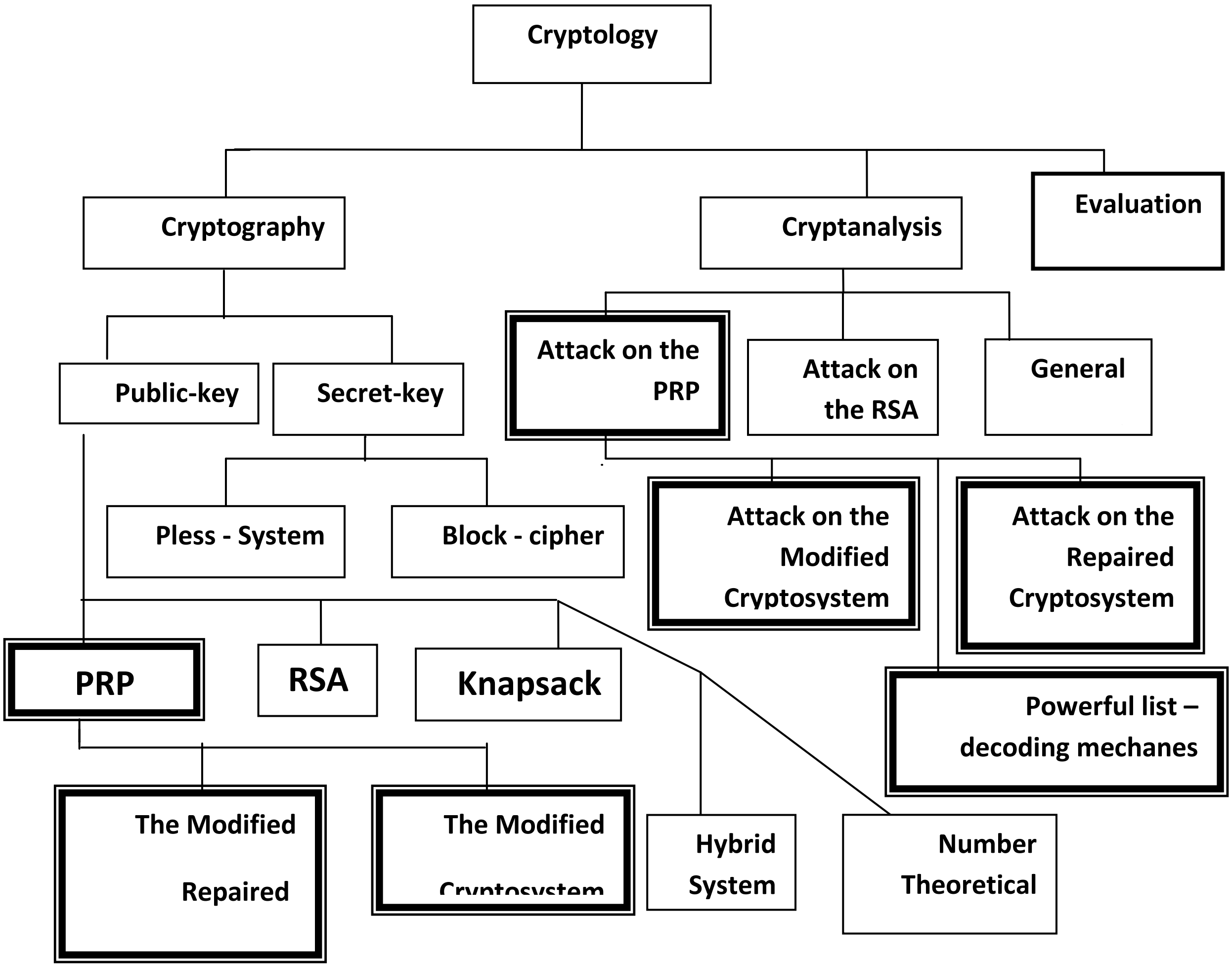

Figure ١- ١: shows the Directions of Development Cryptography.

١. ٢ Literature Review

- ***WEN BAO HAN*** in ١٩٩٦ [١٨], presented study about a primitive polynomial, and proved that there always exists a primitive polynomial of degree n, $(n \geq 7)$ over a finite field F_q (q an odd prime).

- ***Erich Kaltofen*** and ***Victor Shoup*** in ١٩٩٨ [١٩], presented probabilistic algorithms for factoring univariate polynomials over finite fields. The algorithms factor a polynomial of degree n over finite field of constant cardinality in time $O(n^{1.815})$. These algorithms rely on fast matrix multiplication techniques. More generally, to factor a polynomial of degree n over finite field F_q with q elements; the algorithms use $O(n^{1.815}\log q)$ arithmetic operations in F_q.

- ***Erich Kaltofen*** and ***Michael Monagan*** (Mathematicians) in ١٩٩٩ [٢٣], studied generic setting of the modular ***GCD*** algorithm. They developed the algorithm for multivariate polynomials over Euclidean domains. They applied this generic algorithm to a ***GCD*** problem in $Z/(p)[t][x]$ where p is small prime number that yields an improved asymptotic performance over the usual approach, and a very practical algorithm for polynomials over small finite fields.

- ***Jean–Sebastian Coron*** [٢٦], presented a much simpler algorithm for finding small roots of bivariate integer polynomial equations that the same coppersmith problem is proposed at ***Euro crypto*** ٩٦ conference. A simplification is analogous to the simplification brought by ***Howgrave-Graham*** to Coppersmith's algorithm for finding small roots of univariate modular polynomial equations.

- *Don Copporsmith* in ٢٠٠١ [٢٥], presented a brief survey of recent results and ideas concerning the problem of finding a small root of a univariate polynomial mod n , and the companion problem of finding a small solution to abivariate equation over Z .

- ***Philippe Flajolet, Xavier Gourdon*** and ***Daniel Panario*** in ٢٠٠١ [٢٤], presented a factoring polynomials over finite fields. The framework is based on generating functions for describing parameters of interest and on (singularity analysis) for extracting asymptotic values.

- *Helmut Meyn* and ***Werner Gotz*** [٤٠], provided the reciprocal polynomials; the reciprocal $f^{*}(x)$ of a polynomial $f(x)$ of degree n is defined by $f^{*}(x)=x^{n}f(1/n)$. A polynomial is called self – reciprocal if it coincides with its reciprocal. They presented two folds : first they wanted to give attention to the fact that the product of all self – reciprocal irreducible monic (srim) polynomials of a fixed degree has structural properties which are very similar to those of the product of all irreducible monic polynomials of a fixed degree over finite field F_q. The second and central point is a short proof of a criterion for the irreducibility of self -reciprocal polynomials over F_2. Any polynomial $f(x)$ of degree n may be transformed into self -reciprocal polynomial f^{Q} of degree $2n$ given $f^{Q}=x^{n}f(x+x^{-1})$. The criterion states that the self-reciprocal polynomial f^{Q} is irreducible iff the irreducible polynomial f satisfies $f^{(1)}(0)=1.$

- ***Jean – Sebastien Coron*** and ***Alexander May*** (Computer Science, Electrical Engineering and Mathematics) [٣٨], they addressed one of the most fundamental problems concerning the RSA cryptosystem: does the knowledge of the Rivest, Shamir and Addelma (RSA) public and secret key pair (e,d) yield the factorization of $n=pq$ in polynomial time ? It is well –known that there is a probabilistic polynomial time algorithm that on input (n,e,d) outputs the factors p and q. They presented the first deterministic polynomial time algorithm that factors n provided that $e,d<\Phi(n)$. The approach is an application of Coppersmith's technique for finding small roots of univariate modular polynomials.

- ***Xavier-Francois Roblot*** in ٢٠٠٢ [٢٧], described two new factorization algorithms for polynomials. The first factorizes polynomials modulo the prime ideal of a number field, it generalizes the algorithm of ***Berlekamp*** over finite field. The second factorizes polynomials over a number field.

- ***D . Augot*** and ***M . Finiasz*** in ٢٠٠٣ [٣٠], constructed public key encryption scheme based on the hardness of the problem of polynomial reconstruction. The scheme presented is the first public key encryption scheme based on this polynomial reconstruction problem. They also presented some attacks, discussed their performances and stated the size of the parameters required to reach the desired security level.

- ***Jean-Sebastien Coron*** in ٢٠٠٣ [٣١], described a cryptanalysis of a public-key encryption scheme based on PRP. Given the public key and a cipher text, he recovered the corresponding plain text in polynomial time. Therefore, the scheme is not one-way. The technique is a variant of the Berlekamp –Welch algorithm.

- ***D. Augot - M. Finiasz*** and ***P. Loidreau*** in ٢٠٠٣ [٣٢], presented a modification of the ***Augot–Finiasz*** cryptosystem that presented at ***Euro crypt*** ٢٠٠٣ conference. The modification of the scheme is based on the ***Trace Opertor*** which appears to resist the ***Coron's*** attack. Furthermore, they proposed parameters thwarting the state of art attacks.

- ***Jean-Sebastien Coron*** in ٢٠٠٣ [٣٣], described a cryptanalysis of the repaired scheme. Given the public-key and a cipher text, he recovered the corresponding plain text in polynomial time. The technique is a variant of the ***Berlekamp – Welch*** algorithm.

- ***Aggelos Kiayias*** (Computer Science and Engineering) and ***Moti Yung*** (Computer Science) in ٢٠٠٣ [٣٥], employed the powerful list– decoding mechanisms to attack the ***Augot*** and ***Finicisz*** cryptosystem. They presented a coding theoretic public key cryptosystem that suggested approach for designing based on the Polynomial Reconstruction Problem. Their cryptosystem is an instauration of this approach under a specific choice of parameters which give the state of the art of coding theory.

- ***Aggelos Kiayias*** and ***Moti Yung*** [٣٦], studied the optimal parameter setting of the Augot and Finiasz cryptosystem and analyzed it from a probabilistic point of view. They first showed that a small modification of the parameters of this scheme foiled the worst case analysis (Coron’s attacks). However, they gave an alternative probabilistic analysis showing that the attack works almost always. They presented a novel analysis of optimal parameter selection for their cryptosystem . And showed that in the optimal setting of parameter selection, the Augot and Finiasz cryptosystem actually thwarts Coron’s attack. They presented a stronger cipher text – only attack based on the Sudan and Guru swami – Sudan’s list –decoding algorithms that breaks the optimal parameter setting of this cryptosystem. They concluded that the Augot and Finiasz’s setting of this cryptosystem. They concluded that the Augot and Finiasz’s cryptosystem, regardless of exact choice of parameters, and succumbs to a polynomial – time cipher text – only attack.

- ***Fangguo Zhang*** (Information and Communication)***, Shengli Liu*** (Computer Scinence and Engineering), and ***Kwangjo Kim*** (Information and Communication) [٣٩], showed that public key cryptosystem. The complexity of their attack is polynomial time. In other word, the underlying problem of zheng’s public- key cryptosystem is not hard problem.

- ***Jose Luis Diaz – Barrero*** and ***Juan Jose Egozcue*** in ٢٠٠٤, [٣٤] gave a computed characterization and classification of polynomials using reflection coefficients of polynomial instead of zeros and coefficients.

- Shuhong Gao (Mathemaical Sciences), ***Erich Kaltofen*** (Mathematics) and ***Alan G. B. Lauder*** (Mathematics Institute) in ٢٠٠٤ [٤٢], presented a deterministic polynomial time algorithm for finding the distinct - degree factorization of multivariate polynomials over finite fields in deterministic polynomial time.

١.٣ The Overview of the Research:

In the addition to the introduction chapter, the research includes four chapters:

- Chapter two includes definitions , theorems, the arithmetic operations of polynomials over field F, the greatest common divisor (GCD) of the polynomial over F, finding the roots of polynomial over F, the factorization of polynomials over F, polynomial interpolation methods and finite field.

- Chapter three includes the coding system in cryptography, Augot's Modified Original Cryptosystem, Augot's modified repaired cryptosystem, and cryptanalysis of public key cryptosystem based on PRP.

- Chapter four includes the Implementation Algorithms of the PKC based on PRP and Case Studies .

- Chapter five includes conclusions and suggestions for future works.