Thm(2.1) : $n \ni n \in \mathbb{Z}^+$

$$n = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_k^{\alpha_k}$$

$P_1 < P_2 < \cdots < P_k$ اعداد اولية

$\alpha_i \in \mathbb{Z}^+ \cup \{0\}$

Ex(2.1) : 1999 عدد اولي

$$2000 = 2^4 \cdot 5^3$$

$$\begin{array}{c|l} 2 & 2000 \\ 2 & 1000 \\ 2 & 500 \\ & 250 \\ \vdots & \vdots \end{array}$$

Def (2.4) $n_1, n_2 \in \mathbb{Z}^+$

relatively prime $\Longleftrightarrow \gcd(n_1, n_2) = 1$

اولية نسبية

ex $\gcd(4, 15) = 1$

Thm(2.2): $a = \prod P_i^{\alpha_i}$, $b = \prod P_i^{B_i}$

$\gcd(a,b) = \prod P_i^{\epsilon}$, $\epsilon_i = \min(\alpha_i, B_i)$

$\operatorname{lcm}(a,b) = \prod P_i^{\delta_i}$, $\delta_i = \max(\alpha_i, B_i)$

Ex(2.2) $a = 240 = 2^4 \cdot 3 \cdot 5 = 2^4 \cdot 3^1 \cdot 5^1 \cdot 7^0$

$b = 560 = 2^4 \cdot 5 \cdot 7 = 2^4 \cdot 3^0 \cdot 5^1 \cdot 7^1$

$\gcd(a,b) = \gcd(240, 560) = 2^4 \cdot 3^0 \cdot 5^1 \cdot 7^0 = 80$

$\operatorname{lcm}(240, 560) = 2^4 \cdot 3^1 \cdot 5^1 \cdot 7^1 = 1680$

Thm(2.3): لايجاد العلاقة بين gcd , lcm

Euclidean Alg. ②

To find gcd(a,b)

always choose $a \geq b$

هناك اسلوبين لتطبيق الخوارزمية وسنطبقها معاً للتوضيح مع مثال

$r = a \bmod b$	$a = (q)b + (r)$
$r = 75 \bmod 45 = 30 \neq 0$	$75 = (1)45 + (30)$
مادام $r \neq 0$ نستمر	
$a = b,\ b = r$ ونجعل	
$r = 45 \bmod 30 = 15 \neq 0$	$45 = (1)30 + (15)$
نستمر	
$r = 30 \bmod 15 = 0$	$30 = (1)15 + (0)$
مادام $r = 0$ نتوقف	
$gcd = b$ فسيكون اخر	

$\therefore gcd(75, 45) = 15$

Def (2.5) يقال لـ a بانه متطابق congruent الى b mod. n

وتكتب $a \equiv b \pmod{n}$ اذا كان

n تقسم $a - b$ (يعني القسمة بدون باقي)

Ex (2.4)

$24 \bmod 5 = 4$, و $9 \bmod 5 = 4$

فنقول ان $24 \equiv 9 \pmod{5}$ متطابقان

$24 - 9 = 15 = 3 \cdot 5$ من مضاعفات 5

Def (3.5) المثال (3.1) تطبيق للتعريف (3.5) جداً.

$f(m) f(n) = f(mn)$, $\sqrt{n} \cdot \sqrt{m} = \sqrt{n \cdot m}$

تسمى دالة حسابية

Def (3.6) $\phi(n) = \sum_{\substack{1 \leq k < n \\ gcd(k,n)=1}} 1$ دالة اويلر تمثل عدد الاعداد التي تكون اولية نسبياً مع n الاصغر من n

Ex(3.3) تعديل ان يكون $\Pi(1)=1$ لتكون العلاقة في التعريف (3.7) صحيحة

Def(5.4) في هذا التعريف نعرف معنى Boolean Ring الذي لقيد على العمليات $\oplus$ ، + ، . و المتمم

Def(5.5): هذا التعريف يوضح Boolean Algebra الذي لقيد العلاقات $\wedge$ و $\vee$

Thm(5.1) Boolean algebra $\Longrightarrow$ Boolean Ring

اذن نحتاج لعرف عمليات Boolean Ring بدلالة عمليات Boolean algebra

Thm(5.2) Boolean Ring $\Longrightarrow$ Boolean algebra

اذن نحتاج نعرف عمليات Boolean Algebra بدلالة عمليات Boolean Ring

فكرة الموضوع هي كيفية تحويل الدوائر الالكترونية وهي معروفة على شكل Boolean Ring وتحويلها الى Boolean Algebra ومن ثم ليتم هنا اختزاله تبسيطا ثم ارجاعها الى Boolean Ring ثم دوائر الكترونية

المثال Q4 في الفديو $F(a,b,c)=(\overline{ab}\oplus 1)+\overline{a\overline{c}}\oplus\overline{c}+1+ab(ac\oplus b)+1$

ويتم الاستفادة من الجدول (6.1) في تبسيط الدوائر الالكترونية

حيث ان $a+a=a$ و $a\oplus a=0$ و $\overline{a}=a\oplus 1$

$$F(a,b,c)=(ab\oplus\cancel{1}\oplus\cancel{1})+(ac\oplus\cancel{1}\oplus c\oplus\cancel{1})+1+ab(ac\oplus 1\oplus b)+1$$
$$= ab+(ac\oplus c)+ab(ac\oplus b\oplus 1)+1$$

وهكذا يتم تبسيطها ويمكن رسمها حسب المخطط في البند (6)

ويمكن اثبات تكافؤ عملية التبسيط باستخدام truth table وكما في الفديو

Def (8.1) كل متعددة حدود يقال لها irreducible غير قابلة للاختزال على الحقل GF(P) اذا لا يمكن تجزئتها الى حاصل ضرب متعددة اخرى وعكس ذلك تسمى reducible قابلة للتجزئة

Ex(8.1) قد تكون متعددة الحدود قابلة للاختزال في حقل وغير قابلة الاختزال في حقل اخر

Ex(8.2) يوضح كيفية تحويل متعددة الحدود الى ارقام ثنائية اذا كانت تنتمي الى الحقل GF(2) فيمكن جمعها او ضربها على الحقل GF(2)

8.4 No. of Primitive poly.

سؤال مهم

سؤال احد الطلبة عن كيفية اختيار متعددة الحدود اذا كانت قابلة او غير قابلة للاختزال ؟

ملاحظة متعددة الحدود $f(x)$ ~~…~~ غير القابلة للاختزال من الدرجة n تقسم متعددة الحدود $p(x) = x^{2^n-1}+1$

مثال هل ان $f(x)=x^3+x+1$ قابلة ام غير قابلة للاختزال ، $n=3$

الحل نقسم قسمة طويلة $1+x+x^3 \,\big)\, x^7+1$

بعد التقسيم نجد الباقي = 0

$\therefore$ $f(x)$ غير قابلة للاختزال

HW check $f(x)=x^4+x^2+1$ ~~HW End~~

Thm Every primitive poly. is irreducible poly. مهمة
ولكن العكس غير صحيح

Thm $f(x)$ is ~~…~~ primitive poly iff irreducible poly when 2^n-1 is prime

للايجاد عدد irreducible يُرمز $\varphi_2(n)$ وعدد primitive يُرمز $\lambda_2(n)$

10. Linear Equation

Ex(10.1) لسنا بصدد طريقة الحل وانما
تريدان توضيح بالمثال انه يمكن ان يكون له اكثر من حل
خصوصا اذا كان عدد المتغيرات n اكبر من عدد المعادلات m

10.5 Determinant: المحدد
يمكن استخدام اكثر من طريقة ويمكن
طريقة adjoint هي الطريقة الاكثر عموما

10.8.2 استخدام طريقة inverse لايجاد
حل المنظومة.
س/ اعد الطلبة بأن كم اي طريقة يمكن استخدامها
لايجاد المعكوس. هناك اكثر من طريقة:

① $[A|I] \equiv [I|A^{-1}]$
استخدام العمليات الاولية لتحويل $A \longrightarrow I$
فان I تتحول الى A^{-1}

② Since $A \cdot B = I$ حيث انه $B = A^{-1}$
مثلا $A = \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ حلو كان
يمكن نعمل نظام رياضي لحل المسألة

③ $A = \begin{bmatrix} 2 & 5 \\ 1 & 5 \end{bmatrix} \Rightarrow |A| = 5$

$A^{-1} = \frac{1}{5} \begin{bmatrix} 5 & -5 \\ -1 & 2 \end{bmatrix}$ حيث يتم ابدال عناصر القطر الرئيسي مع
بعضها وابدال اشارة عناصر
القطر الثانوي

مثلاً متعددة حدود في الحقل $GF(2^5)$

هي $f(x)=x^4+x^3+x+1$ فعندما نحولها الى ثنائي تكون

$(1,1,0,1,1)$ تمثيل خماسي للثنائي $GF(2^5)$

ومثلاً $g(x)=x^3+x+1$ تكتب $(0,1,0,1,1)$

وهكذا عند الجمع

$$
\begin{array}{ccccc}
1&1&0&1&1\\
0&1&0&1&1\\
\hline
1&0&0&0&0
\end{array}
$$

بما ان $1\oplus1=0$ خاسر

فان متعددة الحدود الناتجة هي x^4

عند الضرب

$$
\begin{array}{cccccccc}
&&&\cancel{0}&1&0&1&1\\
&&&0&0&0&0&0\\
&&1&1&0&1&1&\\
&1&\cancel{1}&0&1&1&&\\
\hline
1&1&1&1&0&1&0&1\\
x^7&x^6&x^5&x^4&x^3&x^2&x&1
\end{array}
\Rightarrow x^7+x^6+x^5+x^4+x^2+1 \Rightarrow
$$

x^4+x^2+1 وتحذف البقية لانها خارج الحقل $GF(2^5)$