مجلة تكريت للعلوم الصرفة، مجلد – ١٣، عدد – (٣) ٢٠٠٨

استخدام برامج الكومبيوتر في إيجاد القاسم المشترك الأعظم لعددين بالاعتماد على خوارزمية اقليدس

ليلى خالد خضير

قسم الرياضيات، كلية التربية، جامعة تكريت، تكريت، جمهورية العراق

(استلم 20 / 8 / ٢٠٠٧ ، قبل 10 / 1 / 2008)

الملخص:

تناولت في هذا البحث الطرق الرياضية في إيجاد القاسم المشترك الأعظم لعددين من خلال خوارزمية القسمة والتي اعتمدت على خوارزمية اقليدس لما فيه من أهمية في جانب علم الرياضيات و كذلك في علوم الحاسبات من خلال استخدامها في عمليات التشفير.

وقد تم اختيار خوارزمية اقليدس والتي هي من أكثر الخوارزميات شهرتا لإيجاد اكبر القوا سم المشتركة لأي عددين كاملين .وتناولت الخوارزمية لكونها طريقة رياضية تعنى أتباع الخطوة تلو الأخرى لحل مسائل رياضية ضمن عدد محدد من الخطوات وتكون التعليمات دقيقة بالنسبة لكل خطوة والكثير من الخوارزمية تنطوي على أعادة الخطوات نفسها عدة مرات والتي يمكن تنفذها من خلال برامج الكومبيوتر أضافة إلى سهولة استخدام برامج الكومبيوتر في إيجاد الحلول الدقيقة عند تنفيذ هذة الخوارزمية ،ولكون الحل اليدوي في الحسابات الرياضية يأخذ وقتا كبيرا ونسبة الخطأ كبيرة في النتائج التي نحصل عليها لذلك اتجهت إلى استخدام برامج الكومبيوتر لتسهيل عملية استخدام خوارزمية اقليدس في إيجاد القاسم المشترك الأعظم لعددين بصورة سهلة ومبسطة وسريعة وكذلك لإجراء عمليات توافقية بين النتائج التي تم استحصالها باستخدام الكومبيوتر لإعادة استخدامها مرة أخرى في مجال تشفير المعلومات أي أن هذة الخوارزمية والبرمجيات تصبح احد المحركات الرئيسية في عملية تشفير المعلومات.

المقدمة:

تعد ا لخوارزمية بصورة عامة هي طريقة رياضية تعني إتباع الخطوة تلو الأخرى لحل مسائل رياضية ضمن عدد محدد من الخطوات وتكون التعليمات دقيقة بالنسبة لكل خطوة والكثير من الخوارزمية تنطوي على إعادة الخطوات نفسها عدة مرات ويمكن تنفيذها بالحاسوب ولعل أكثر الخوارزميات شهرة هي خوارزمية اقليدس وتستعمل لإيجاد القوا سم المشتركة لأي عددين كاملين مثل (أ) و(ب) وتعد خوارزمية اقليدس من أقدم الخوارزميات والتي سميت باسم العلم الرياضي الشهير اقليدس والتي وجدت في كتابه السابع في الرياضيات الفيثاغورثية في الفترة مابين(٤٥٠-٥٠٠) ق.م حيث بحث الكتاب في الأعداد وقابلية القسمة.

وان النظرية التي وضعها حول إيجاد القاسم المشترك الأعظم لعددين (اكبر عدد يقسم كليهما) تسمى ألان بطريقة الكوريزم لاقليدس.لذلك سوف نتأول طرق إيجاد القاسم المشترك الأعظم لعددين من خلال خوارزمية القسمة المعرفة ومن تم اختص في خوارزمية اقليدس لما لها من أهمية كبيرة في الرياضيات ومميزات خاصة في إيجاد القاسم المشترك الأعظم وتصميم برنامج في الحاسوب لحل خوارزمية اقليدس وهذه خطوة جديدة في مجال الرياضيات.

١ . خوارزمية القسمة(Division Algorithm)

نظرية ١,١ – **خوارزمية القسمة(Division Algorithm)**

ليكن أ،ب عددين موجبين فانه يوجد عددان صحيحان وحيدان مثل ك ، ر حيث ٠ ≤ ر< ب حيث أ=ب ك + ر ألان علينا أن نبرهن أن ر، ك وحيدان.

البرهان:

لنفرض العكس وانهما ليسا وحيدان

بل يوجد ك$_{١}$، ر$_{١}$ ، ك$_{٢}$ ، ر$_{٢}$ حيث ٠ ≤ر$_{١}$< ب ، ٠ ≤ر$_{٢}$< ب

∴ أ= ب ك$_{١}$ +ر$_{١}$

أ= ب ك$_{٢}$ +ر$_{٢}$ } ⇐ ب ك$_{١}$ +ر$_{١}$= ب ك$_{٢}$+ر$_{٢}$

ب ك$_{١}$+ ر$_{١}$–ب ك$_{٢}$–ر$_{٢}$ = صفر

ب(ك$_{١}$ –ك$_{٢}$) +(ر$_{١}$–ر$_{٢}$) = صفر

لكن ب تقسم الصفر وتقسم ب(ك$_{١}$–ك$_{٢}$)

∴ ب تقسم (ر$_{١}$–ر$_{٢}$)

∴ لكن ٠ ≤ر< ب ، ٠ ≤ ر$_{١}$< ب

∴ – ب < ر– ر$_{١}$ < ب والمضاعف الوحيد يبين – ب ،ب هو الصفر

∴ ر– ر$_{١}$ = صفر ⇐ ر= ر$_{١}$

∴ ب(ك – ك$_{١}$)+(ر– ر$_{١}$) = صفر

∴ ب(ك– ك$_{١}$)+ صفر= صفر

∴ ب(ك–ك$_{١}$) = صفر⇐ ك = ك$_{١}$ أي أن ر، ك وحيدين وهو المطلوب [١].

تعريف ٢,١

القاسم المشترك الأكبر(GCD - Greatest Common Divisor)

نقول بأن ء القاسم المشترك الأعظم للعددين أ،ب وتكتب بالشكل ء= (أ،ب) إذا وفقط تحقق الشرطان التاليان

١– ء|أ ،ء|ب

٢– إذا كان ج|أ ،ج|ب فأن ج≤ ء [١]

مثال (١) :

(٥،١٠)= ٥

(١٤،٨٤)=١٤

(٢٨،٣٥)=٧

مثال (٢) :

من المعلوم أن مجموعة عوامل العدد١٢ هي

ع$_{١٢}$={12,6,4,3,2,1 }

وان مجموعة عوامل العدد ٥٦ هي

ع$_{٥٦}$={56,28,14, 8,7,4,3,2,1}

ع$_{١٢}$ ∩ ع$_{٥٦}$ ={4,2,1 }

أن اكبر العوامل (القوا سم) المشتركة للعددين ١٢،٥٦ هو العدد (٤) لهذا فان العدد (٤) يسمى القاسم المشترك الأعظم للعدين١٢،٥٦ وسوف نرمز له بالرمز ١٢ Δ ٥٦=٤

والرمز Δ يقرأ دلتا وبشكل عام م ن=(ع م ∩ ع ن)

٢. طريقة خوارزمية القسمة لإيجاد القاسم المشترك الأعظم:

عند قسمة العدد ٩ على ٢ يكون الناتج ٤ والباقي ١ كما يمكن ملاحظة أن ٩=٢*٤+١

أي إن المقسوم =المقسوم عليه*الناتج+الباقي

وبشكل عام إذا كانت أ، ب∋ الإعداد الطبيعية فانه يوجد عددانء،ر ∋ ط بحيث أن أ=بء+ر

حيث ٠≤ر< ب تسمى هذة الخاصية بخوارزمية القسمة وتستعمل في إيجاد القاسم المشترك الأعظم وبالعمل بهذة الخاصية

إذا كان أ، ب ∋ ط فان أ=ب ء + ر حيث ٠ ≤ر < ب

إذا كان ر= صفرا نقف عند هذة الخطوة ويكون ب= أΔ ب

أما إذا كان ر ≠ صفرا فأننا نطبق خوارزمية القسمة مرة أخرى على ب،ر

فيكون ب=ر ء$_{١}$+ ر ١

حيث ٠≤ ر$_{١}$< ر

وهكذا تكرر العملية مثلا ك+٢ مرة ليصبح الباقي ر$_{ك+٢}$ =صفرا وعندها يكون ر$_{ك}$=أΔ ب [١]

مثال:

أوجد ٣٨Δ٣ باستعمال خوارزمية القسمة

الحل ٣٨=٣*١٢+٢

٣=٢*١+١

٢=1*2+0

٣٨Δ٣ =١

مثال:

أوجد ١٣٣Δ٤٩ باستعمال خوارزمية القسمة

الحل ١٣٣=٤٩*٢+٣٥

٤٩=٣٥*١+١٤

٣٥=14*2+7

١٤=٣*2+0

١٣٣Δ٤٩ =٧

٣. خوارزمية أقليدس (Euclidean Algorithm)

خوارزمية أقليدس هي خوارزمية تمكن من حساب القاسم المشترك الأكبر لعددين طبيعيين، و هي كالآتي:

القاسم المشترك الأكبر لعددين طبيعيين هو نفسه القاسم المشترك الأكبر للعدد الأصغر و باقي قسمة العدد الأكبر على العدد الأصغر

وليكن أ،ب عددان صحيحان(أ < صفر بإجراء خوارزمية القسمة بشكل متكرر)، نحصل على سلسلة من المعادلات

أ= ب ك +ر ، ٠≤ ر< ب

ب= رك$_{١}$+ر$_{١}$ ، ٠≤ ر$_{١}$< ر

ر= ر$_{١}$ ك$_{٢}$+ر$_{٢}$ ، ٠≤ ر$_{٢}$ < ر$_{١}$

ر$_{ن}$= ر$_{ن+١}$ك$_{ن+٢}$ +ر$_{ن+٢}$ ، ٠ ≤ ر$_{ن+٢}$ < ر$_{ن+١}$

فإذا كانت ن كبيرة جدا بحيث ن=ت فان رت−١=ر$_{ت}$ ك$_{ت+١}$ [١]

مثال ١

باستخدام خوارزمية أقليدس ، أوجد القاسم المشترك الأكبر للعددين(٧٤٦٩،٢٤٦٤)

7469=3×2464+77

2464=32×77+0

إذاً (٧٤٦٩،٢٤٦٤)=٧٧ [٣]

مثال ٢

باستخدام خوارزمية أقليدس ، أوجد القاسم المشترك الأكبر للعددين (٤٩٩٩،١١٠٩)

4999=4×1109+563

1109=1×563+546

563=1×546+17

546=32×17+2

17=8×2+1

2=2×1+0

إذاً[=(4999,1109) [٣]

٤. تصميم الخوارزمية(planning the algorithm)

اعتمدت الخوارزمية على مبدأين

٤,١المبدأ الأول:

عندما نقسم عددا اكبر على اصغر فان القاسم المشترك الأعظم لباقي القسمة والعدد الأصغر هو نفس القاسم المشترك الأعظم للعددين الأصليين فمثلا عندما نقسم العدد ٢٤ على ١٠ لإيجاد القاسم المشترك الأعظم للعددين فان باقي القسمة هو ٤ والقاسم المشترك الأعظم للعددين هو ٢ وكذلك القاسم المشترك الأعظم لباقي القسمة ٤و١٠ هو ٢ أيضا.

٤,٢المبدأ الثاني:

القاسم المشترك الأعظم لعدد ما والصفر هو ذلك العدد ،فمثلا القاسم المشترك الأعظم للعددين ١٠و٠هو ١٠.عندما نصمم الخوارزمية لإيجاد القاسم المشترك الأعظم لعدد سوف نبدأ بالعدد المطلوب أيجاد القاسم المشترك الأعظم لهما ونقسم الأكبر على الأصغر وحسب المبدأ الأول أن العدد الأصغر وباقي القسمة لهما نفس القاسم المشترك الأعظم للعددين الأصليين.

ومن اجل ذلك نقوم باستبدال العددين الأصليين بالعدد الأصغر وباقي القسمة ونكرر هذه العملية ،وفي كل تكرار نقسم العددين على الأصغر ثم

نستبدل العدد الأكبر بالاصغر والأصغر بباقي القسمة .ولا يهمنا عدد مرات التكرار هذه ، فالقاسم المشترك الأعظم للعددين الحاليين سيكون هو نفسه الذي للعددين اللذين بدأنا بهما.

نستنتج انه عندما نقسم عدد اكبر على عدد اصغر يكون باقي القسمة إما اصغر من القاسم المشترك أو من المقسوم ،وبعد تكرار كل خطوة سيكون اصغر العددين اقل من اصغر العددين في التكرار السابق.

وإذا نفذنا تكرارات كافية يصبح العدد الأصغر اقل فاقل مع كل تكرار ثم في النهاية يصبح العدد الأصغر صفرا.

وباستخدام المبدأ الثاني يكون احد العددين صفرا ويكون العدد الأخر هو القاسم المشترك الأعظم للعددين ولذلك يكون العددين الحاليين صفرا ويكون العدد الأكبر هو القاسم المشترك الأعظم للعددين ولذلك يكون حسب المبدأ الأول هو أيضا القاسم المشترك الأعظم للعددين اللذين بدأنا بهما وهذه النتيجة التي نبحث عنها .

في الجدول (١) والذي يوضح كيف نقوم بحساب القاسم المشترك الأعظم للعددين ٥٥،٩٩ باستخدام خوارزمية اقليدس ، في الخطوة الأولى نقسم ٩٩ على ٥٥ لنحصل على باقي القسمة ٤٤ باستعمال المبدأ الأول فان القاسم المشترك الأعظم للعددين ٤٤، ٥٥ هو نفس القاسم المشترك الأعظم للعددين ٥٥،٩٩.

ثم نقسم ٥٥ على ٤٤ ونحصل على باقي القسمة ١١ وباستعمال المبدأ الأول فان القاسم المشترك الأعظم للعددين ٤٤،١١ وهو نفس القاسم المشترك الأعظم للعددين ٥٥، ٤٤ وكذلك هو القاسم المشترك للعددين ٩٩،٥٥. ثم نقسم ٤٤ على ١١ فنحصل على باقي القسمة صفرا. باستعمال المبدأ الثاني فان القاسم المشترك الأعظم للعددين ١١،٠هو ١١ وباستعمال المبدأ الأول فان العدد ١١ يكون هو القاسم المشترك الأعظم للعددين ٤٤،١١ وللعددين ٥٥،٤٤ وللعددين ٥٥،٩٩ ولهذا فان ١١ هو الجواب المطلوب والذي حصلنا عيه من سلسلة العمليات هذه.

جدول (١): (استعمال خوارزمية اقليدس للقاسم المشترك الأعظم لبيان ان القاسم المشترك الأعظم للعددين ٩٩ و٥٥ هو ١١)

خطوة ١	العدد الأكبر هو ٩٩		٩٩ / ٥٥
	العدد الأصغر هو ٥٥		٥٥
	باقي القسمة هو ٤٤		٤٤
خطوة ٢	العدد الأكبر هو ٥٥	١	٤٤/٥٥
	العدد الأصغر هو ٤٤		٤٤
	باقي القسمة هو ١١		١١
خطوة ٣	العدد الأكبر هو ٤٤	١	١١/٤٤
	العدد الأصغر هو ١١		٤٤
	باقي القسمة هو ٠		٠
خطوة ٤	العدد الأكبر هو ١١		
	العدد الأصغر هو ٠		

وحيث ان العدد الأصغر هو ٠ فقيمة العدد الأكبر ١١ ويكون العدد (١١) القاسم المشترك الأعظم للعددين٩٩و٥٥ .وتعقيب تنفيذ خوارزمية القاسم المشترك الأعظم صف العداد السابق لكل تعليمة يوضح محتويات larger و smaller و remainder قبل تنفيذ التعليمة وصف الأعداد التالي للتعليمة يوضح محتويات نفس المواقع بعد تنفيذ التعليمة ومقارنة الصفتين تكشف عن تأثير التعليمة كما في الجدول(٢) .

الجدول(٢): يوضح تعقيب تنفيذ خوارزمية القاسم المشترك الأعظم

الخطوات التتابعية	larger	smaller	remainder
	١٣٣	٤٩	
remainder‹— larger mod smaller	١٣٣	٤٩	٣٥
larger‹— smaller	٤٩	٤٩	٣٥
smaller‹— remainder	٤٩	٣٥	٣٥
remainder‹— larger mod smaller	٤٩	٣٥	١٤
larger‹— smaller	٣٥	٣٥	١٤
smaller‹— remainder	٣٥	١٤	١٤
Remainder ‹— larger mod smaller	٣٥	١٤	٧
larger‹— smaller	١٤	١٤	٧
smaller‹— remainder	١٤	٧	٧
Remainder ‹— larger mod smaller	١٤	٧	٠
larger‹— smaller	٧	٧	٠
smaller‹— remainder	٧	٠	٠

وبذالك يمكن تلخيص الخوارزمية التي توصلنا إليها كالأتي :

أولا نحتاج إلى استعمال علاقتين خاصتين وهما علاقة (mod) و(‹—)وهما من العلاقات الرياضية وحيث أن علاقة (mod) تمثل باقي القسمة مثل(٢ =٤ mod ٦) وكذلك علاقة (‹—) تعنيان القيمة على اليمين تنقل إلى اليسار فان ٥ ‹—— larger تعني أن ٥ يكتب في larger مستبدلا أي عدد كان موجودا سابقا هناك ، larger ‹— smaller تعني أن العدد في smaller يستنسخ إلى داخلlarger مستبدلا أي عدد كان موجودا سابقا في larger .وتعد التعليمات من النوع ٥ ‹——larger تعليمات إلزامية(imperative statement) متى تأمرنا بالقيام بفعل ما وعادة تشير إلى هذه التعليمات الإلزامية كتعليمات فقط وذلك للاختصار . [٢]

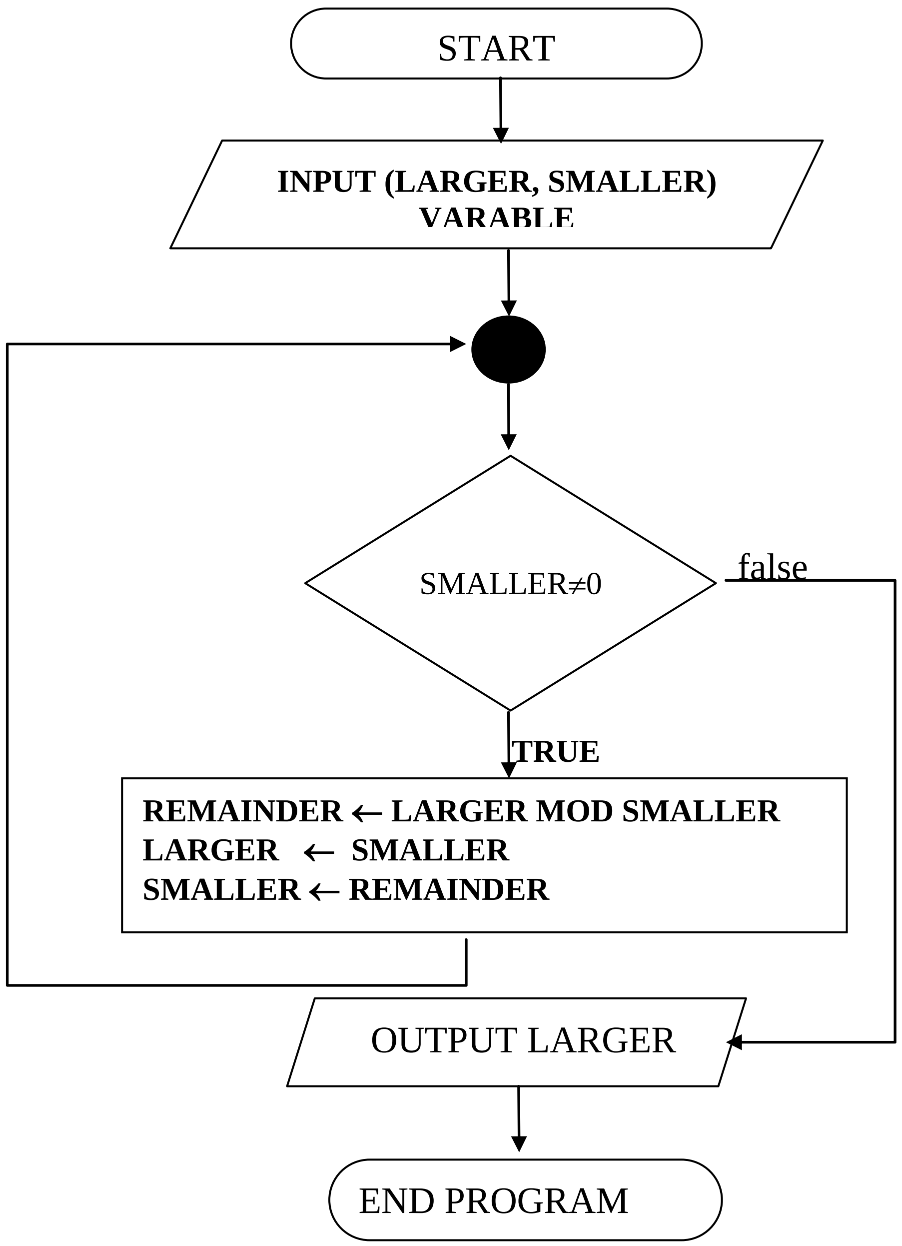
وأيضا الإشارة إلى أن بيانات الإدخال ستكون العددين الذين نريد إيجاد القاسم المشترك الأعظم لهما وحيث نضع larger وsmaller و input لإدخال القيم.

ولمتابعة عمل البرنامج فان المخطط الانسيابي لخوارزمية القاسم المشترك الأعظم الذي يعرض بالشكل (١) وهو يمثل المخطط الانسيابي لخوارزمية القاسم المشترك الأعظم وأكثر الأشياء تشوقا في هذا المخطط الانسيابي

هو طريقة تمثيل التكراري لاحظ الدوارة (loop)التي تبدأ عند دائرة التجميع وتمر خلال شكل القرار ثم تمر خلال شكل المعالجة الذي يحتوي على التعليمات التي تكرر وتنهى بالعودة إلى دائرة التجميع.

لنتبع طريقنا خلال هذة الدائرة الدوارة فنبدأ عند دائرة التجميع وتتوجه إلى شكل القرار وهناك نتظر المستطيل smaller ونرى فيما إذا كان العدد الذي فيه مساويا للصفر .فإذا كان smallerلا يساوي صفرا فإننا نتبع الممر ذا العلاقة الصائبة(TRUE)ونفذ التعليمات المكررة ونعود إلى دائرة التجميع ثم نصل إلى شكل القرار مرة أخرى وهنا لابد من فحص الشرط ٠ ≠ smaller مرة أخرى .فإذا كان يزال محققا نذهب خلال الدوارة مرة أخرى.[٢]

ويستمر هذا طالما نجد أن ٠ ≠ smaller عندما نأتي إلى شكل القرار أخيرا يأتي الوقت الذي نصل فيه غلى شكل القرار ونجد إن ٠ ≠ smaller غير محقق حينئذ نأخذ الممر ذا العلاقة الخاطئة (FALSE) والذي يقودنا إلى شكل الإخراج ومن هناك إلى نقطة التوقف وقد تم بناء برنامج بلغة Gwbasic ويتمثل في شكل(٢) وبرنامج بلغة VB يتمثل بشكل(٣).



شكل(١): المخطط الانسيابي للبرنامج الذي يعمل على حساب القاسم المشترك الأعظم

```
   Input "ادخل العدد الكبير" :L
10 Input ""ادخل العدد الصغير" :S
   If S=0 then  Print "لايقبل القسمة على صفرا" ; go to 10
20   R = L mod S
     if s=0  then go to 50
     L=S
     S=r
     Go to 20
50  Print "القاسم المشترك الاعظم" ; L"
     end.
```

شكل(٢): يمثل برنامج بلغة basic

```
ضع خانتي نص Text1 + Text2 ثم أضف زر 1command1
Function PGDCDET(A As Long, B As Long)
Dim r As Long
r = A - (A \ B) * B
If r = 0 Then
PGDCDET = B
ElseIf B \ r = B / r Then
PGDCDET = r
Else
PGDCDET = PGDCDET(B, r)
End If
End Function
command1 للزر click في الحدث وإضافة هذا الكود
Dim X as integer
Dim Y as integer
Dim N as integer
Dim M as integer
X = cint(text1.text)
Y = cint(text2.text)
If Abs(x) > Abs(y) Then
N = Abs(X)
M = Abs(Y)
Else
N = Abs(Y)
M = Abs(X)
End If
Print PGDCDET(N, M)
```

شكل(٣): برنامج بلغة VB يعمل على خوارزمية اقليدس

المصادر:

[١] عوض . د.عدنان محمد . بنية الأعداد ونظرية الأعداد

[٢] جراهام.نيل . مقدمة في علوم الحاسبات.طريقة مهيكلة

[٣] (شـــــبكة الرياضـــــيات الرمـــــز)
http://www.mathramz.com/math/greatest_common_divisor