نظام البواقي الصيني

و استخدامه في العمليات الحسابية على الأعداد الكبيرة

مسعود حيدر

نظام البواقي الصيني

تقديم الطالب: مسعود حيدر

المشرف : أ.كلوديا الجندي

العام الدراسي : 2016 – 2017

المقدمة :

التطابقات طريقة فريدة للتعبير عن بواقي القسمة طرحت لأول مرة من قبل الرياضي الألماني غاوس في بداية القرن التاسع عشر و شكلت التطابقات وسيلة فعالة لإثبات العديد من الخواص و القوانين في نظرية الأعداد.

للتطابقات استخدامات كثيرة ولاسيما في حساب بواقي القسمة و في التأريخ. و تستخدم بشكل كبير جداً في التشفير. و يمكن استخدامها في تطبيقات أخرى.

لدى استخدامنا في السابق للغات البرمجة من خلال دراستنا يمكننا أن نلاحظ أن لكل منها سعة تخزين معينة فيما يتعلق بالأعداد الصحيحة فمثلاً في لغة الc++ يمكن استخدام إما متحول صحيح من سعة 32 بت أو 64 بت و لهذه المتحولات حدود معينة لتخزين الأعداد فمثلاً متحول من سعة 64 يمكنه تخزين حتى الرقم $2^{64}-1$ فإذا ما أراد المبرمج القيام بالعمليات الحسابية على أعداد أكبر من ذلك فعليه اللجوء إلى خوارزميات تستفيد من العمليات الحسابية العادية لأيجاد نواتج عمليات حسابية على أعداد كبيرة.

تطرح التطابقات و نظام البواقي الصيني طريقة سهلة للقيام بالعمليات الحسابية على الأعداد الكبيرة. قد تكون هذه الطريقة غير تقليدية و لكنها فعالة في كثير من الأحيان إذ أنّها تقلل الحاجة للتعامل مع الأعداد الكبيرة بشكل كبير. فعند الدخل يقوم البرنامج بدل تخزين الرقم الكبير بتخزين باقي قسمته على عدة أعداد صغيرة و عند تنفيذ باقي التعليمات لا يحتاج المبرمج إلّا إلى التعامل مع هذه الأعداد الصغيرة في العمليات الحسابية المختلفة ثم يسترجع العدد الكبيرة بحل نظام البواقي الصيني المتشكل من باقي قسمة العدد المطلوب على الأعداد الصغيرة للقيام بعملية الخرج.

إن حل نظام بواقي صيني يلزم معرفة بالتطابقات الخطية و التي يمكن تحويلها إلى معادلات ديفونتية خطية يمكن الحصول على جميع حلولها باستخدام خوارزمية إقليدس الممدّدة. ففي بحثنا هذا سنبحث في التطابقات و نظام البواقي الصيني لفهم خوارزمية التعامل مع الأعداد الكبيرة و للوصول إلى الأجوبة عن إشكالية البحث المطروحة.

إشكالية البحث:

- لمً تعمل الخوارزمية المطروحة في المقدمة (أي ما هو إثبات أنها تعطي الجواب الصحيح) و كيف يتم تطبيقها ؟
- هل يمكن القيام بجميع العمليات (جمع - طرح - ضرب - قسمة - رفع إلى قوّة - مقارنة - التأكد من عدم تجاوز الحد المسموح) بوساطة هذه الخوارزمية ؟

((ملاحظة: في بداية كل من الفصل الأول و الثاني تم ذكر بعض المبرهنات و الخواص الأساسية المهمة في بقية البحث و للاختصار لم يتم ذكر برهانها و تم التركيز على باقي الأمور الأكثر أهمية في البحث. و للحصول على البرهان يمكن الرجوع إلى المصادر التي أخذت منها هذه المبرهنات و الخواص.))

الفهرس :

- المقدمة 2
- إشكالية البحث 2
- الفهرس 3
- الفصل الأول: خوارزمية إقليدس 4
  - أولاً: خوارزمية إقليدس لإيجاد القاسم المشترك الأكبر 4
  - ثانياً: عدد عمليات القسمة اللازمة في خوارزمية إقليدس 6
  - ثالثاً: خوارزمية إقليدس الممدّدة لحل المعادلات الديفونتية الخطية 8
- الفصل الثاني: التطابقات الخطية و نظام البواقي الصيني 12
  - أولاً: أساسيات في التطابقات 12
  - ثانياً: التطابقات الخطية 13
  - ثالثاً: البواقي الصينيّة 20
- العمليات الحسابية على الأعداد الكبيرة 26
  - أولاً: فكرة الخوارزمية و اختيار القياسات 26
  - ثانياً: خطوات الخوارزمية 29
  - ثالثاً: المقارنة و تجاوز الحد و القسمة باستخدام التطابقات 32
- الخاتمة 34
- المصادر و المراجع 35

الفصل الأول:

خوارزمية إقليدس

تعد خوارزمية إقليدس الطريقة الأكثر فاعلية لإيجاد القاسم المشترك الأكبر لعددين (أكبر عدد يقسم كليهما) و ذلك لسهولة تطبيقها و حاجتها لعدد قليل من العمليات الحسابية (تم إثبات لك لاحقاً في هذا الفصل). و بالإضافة لذلك تستعمل خوارزمية إقليدس الممددة لحل المعادلات الديفونية من الشكل

$$ax+by=c$$

و التي تستخدم لحل التطابقات الخطية.

أولاً: **خوارزمية إقليدس لإيجاد القاسم المشترك الأكبر**

" تعريف(1-1): القاسم المشترك الأكبر لعددين a و b ليسا معدومين معاً هو أكبر عدد بين قواسمهما المشتركة, و يرمز له ب $\gcd(a,b)$ أو للاختصار بالرمز (a,b).

مبرهنة (1-1) : إذا كان $d\mid a$ و $d\mid b$ فإن $d\mid(ax+by);x,y\in\mathbb{Z}$.

مبرهنة (1-2) : إذا كان لدينا عددين a و b ليسا معدومين معاً. فإن قاسمهما المشترك الأكبر هو أصغر عنصر موجب تماماً من المجموعة $\{ax+by;x,y\in\mathbb{Z}\}$.

انطلاقاً من المبرهنتين السابقتين يمكننا الوصول إلى المبرهنة التالية:

مبرهنة (1-3) : إذا كان $d\mid a$ و $d\mid b$ فإن $d\mid(a,b)$.

مبرهنة (1-4) : إذا كان $a\mid b$ و $b\mid a$ فإن $a=\pm b$." (Thomas H. Cormen, 2009)

و الآن يمكننا البدء ببرهان و شرح مبرهنة إقليدس, كما مرّ معنا في الدراسة الإعدادية سابقاً مبرهنة إقليدس تكون كما يلي:

لإيجاد القاسم المشترك الأكبر لعددين a و b حيث $a\geq b$ نسند : $r_0=a$ و $r_1=b$ و لكل $i>1$ يكون:

$$r_{i-2}=r_{i-1}\times q_{i-1}+r_i;0\leq r_i<r_{i-1}$$

أي أن r_i هو باقي قسمة r_{i-2} على r_{i-1} و تستمر الخوارزمية حتى الوصول لباقٍ r_{n+1} مساوٍ للصفر فيكون آخر باقي غير معدوم هو القاسم المشترك الأكبر لـ a و b أي $(a,b)=r_n$.

الآن سنتحدث عن برهان هذه الخوارزمية. تقوم الخوارزمية على مبرهنة أساسية و إثبات المبرهنة يعني إثبات خوارزمية إقليدس و هي:

مبرهنة (1-5): (مبرهنة إقليدس) : إذا كان $a = b \times q + r; 0 \le r < b$ أي أن q ناتج قسمة صحيحة لـ a على b و r هو باقي القسمة فإن $(a,b) = (b,r)$.

"البرهان: لإثبات ذلك سنثبت أن (a,b) و (b,r) يقسمان بعضهما. للتسهيل فلنسند :

$$d_1 = (a,b), d_2 = (b,r)$$

بما أن $d_2 \mid b$ و $d_2 \mid r$ و بما أن $a = b \times q + r$ أي أن a عبارة عن تركيب خطي لـ r و b فبحسب المبرهنة (1-1) : $d_2 \mid a$ و لكن $d_2 \mid b$ فبحسب المبرهنة (1-3) : $d_2 \mid (a,b)$ أي:

$$d_2 \mid d_1 \quad (1)$$

بما أن $d_1 \mid a$ و $d_1 \mid b$ و $r = a - b \times q$ أي أن r عبارة عن تركيب خطي لـ a و b فبحسب المبرهنة (1-1) : $d_1 \mid r$ و لكن $d_1 \mid b$ فبحسب المبرهنة (1-3) : $d_1 \mid (b,r)$ أي:

$$d_1 \mid d_2 \quad (2)$$

بالجمع بين (1) و (2) و بالاعتماد على المبرهنة (1-4) و أن القاسم المشترك الأكبر لعددين ليس عدداً سالباً نستنتج أن $d_1 = d_2$ أي أن:

$$(a,b) = (b,r)$$

و هو المطلوب." (Thomas H. Cormen,2009)

مثال: لإيجاد القاسم المشترك الأكبر للعددين 60 و 44 :

$$60 = 1 \times 44 + 16$$
$$44 = 2 \times 16 + 12$$
$$16 = 1 \times 12 + 4$$
$$12 = 3 \times 4 + 0$$

بما أن أخر باقي غير معدوم هو 4 فيكون $(60,44) = 4$.

"إن خوارزمية إقليدس يستحيل أن تكون لانهائية أي أننا سنصل حتماً إلى باقٍ مساوٍ للصفر و ذلك ببساطة لأن كل باقٍ أصغر تماماً من الباقي الذي يسبقه و أكبر أو يساوي الصفر فسنصل حتماً في النهاية لباقٍ يساوي الصفر فنكون بذلك وصلنا إلى القاسم المشترك الأكبر للعددين المطلوبين."
(Thomas H. Cormen, 2009)

و بهذا نكون أثبتا أننا لا يمكن أن نحتاج عدد لانهائي من عمليات القسمة في خوارزمية إقليدس و لكن في الحقيقة خوارزمية إقليدس أكثر فاعلية من ذلك بكثير كما سنثبت في هذا الفصل.

ثانياً: **عدد عمليات القسمة اللازمة في خوارزمية إقليدس.**

في هذا القسم سنبحث عن تقدير لأعلى حد ممكن من عمليات القسمة التي قد تحتاجها خوارزمية إقليدس. سنحتاج في هذا القسم من البحث لاستخدام متتالية فيبوناتشي المعرفة بالشكل التالي:

تعريف(1-2): أعداد فيبوناتشي: $1-1-2-3-5-8-13-21-34-55-89...$

تولد أعداد فيبوناتشي وفق القاعدة: $u_1 = u_2 = 1, u_n = u_{n-1} + u_{n-2}; n > 2$.

قبل استخدام أعداد فيبوناتشي لنضع حد أدنى لأعداد فيبوناتشي.

مبرهنة (1-6) : ليكن $n \geq 3$ عدد طبيعي و $\alpha = \frac{(1+\sqrt{5})}{2}$ فإن $u_n > \alpha^{n-2}$.

"البرهان: سنثبت المبرهنة بوساطة الاستقراء الرياضي . أولا نثبت المبرهنة عند $n = 3$:

$\alpha < 2 = u_3$ و بذلك المبرهنة محققة عند $n = 3$.

الآن نفرض أن لكل الأعداد الصحيحة k الأصغر أو تساوي n يتحقق $\alpha^{k-2} < u_k$

بملاحظة أن α حل للمعادلة $(x^2 - x - 1 = 0)$ يمكننا أن نجد أن $\alpha^2 = \alpha + 1$ أي:

$$\alpha^{n-1} = \alpha^2 \times \alpha^{n-3} = (\alpha + 1) \times \alpha^{n-3} = \alpha^{n-2} + \alpha^{n-3}$$

من فرض الاستقراء نجد :

$$\alpha^{n-2} < u_n$$
$$\alpha^{n-3} < u_{n-1}$$

بجمع المتراجحتين كل طرف إلى الطرف المقابل له نجد:

$$\alpha^{n-1} < u_{n+1}$$

و هو المطلوب." (Kenneth H. Rosen, 1984)

مبرهنة (1-7) : يلزم بالتحديد n عملية قسمة للوصول إلى أن $(u_{n+2}, u_{n+1}) = 1$.

"البرهان: بتطبيق خوارزمية إقليدس و الاستفادة من التعريف (1-2) لأعداد فيبوناتشي نجد:

$$u_{n+2} = 1 \times u_{n+1} + u_n$$
$$u_{n+1} = 1 \times u_n + u_{n-1}$$
.
.
.
$$u_4 = 1 \times u_3 + u_2$$
$$u_3 = 2 \times u_2$$

و بذلك نصل إلى أنه يلزم n عملية قسمة للوصول إلى أن $(u_{n+2}, u_{n+1}) = u_2 = 1$"

(Kenneth H. Rosen, 1984)

مبرهنة (1-8) : عدد عمليات القسمة اللازمة لإيجاد القاسم المشترك الأكبر لعددين باستخدام خوارزمية إقليدس لا يتجاوز 5 مرات عدد خانات العدد الأصغر بينهما.

"البرهان: لنطبق خوارزمية إقليدس لإيجاد القاسم المشترك الأكبر ل $r_0 = a$ و $r_1 = b$ علماً أن $a > b$:

$$r_0 = r_1 \times q_1 + r_2; 0 \le r_2 < r_1$$
$$r_1 = r_2 \times q_2 + r_3; 0 \le r_3 < r_2$$
.
.
.
$$r_{n-2} = r_{n-1} \times q_{n-1} + r_n; 0 \le r_n < r_{n-1}$$
$$r_{n-1} = r_n \times q_n$$

و بذلك استخدمنا n عملية قسمة. نعلم أن كل من القيم $q_1, q_2 \ldots q_{n-1}$ هي أكبر أو تساوي 1, و أن $q_n \ge 2$ و ذلك لأن $r_n < r_{n-1}$ و بذلك:

$$r_n \geq 1 = u_2$$
$$r_{n-1} \geq 2 \times r_n \geq 2 \times u_2 = u_3$$
$$r_{n-2} \geq r_{n-1} + r_n \geq u_3 + u_2 = u_4$$
$$r_{n-3} \geq r_{n-2} + r_{n-1} \geq u_4 + u_3 = u_5$$
$$\vdots$$
$$r_2 \geq r_3 + r_4 \geq u_{n-1} + u_{n-2} = u_n$$
$$b = r_1 \geq r_2 + r_3 \geq u_n + u_{n-1} = u_{n+1}$$

و بذلك, حتى يكون هناك n عملية قسمة في خوارزمية إقليدس يجب أن يتحقق أن $b \geq u_{n+1}$. بحسب المبرهنة (6-1) $u_{n+1} > \alpha^{n-1}$ لكل $n > 2$. أي, $b > \alpha^{n-1}$. و الآن بما أن $\log_{10}(\alpha) > \frac{1}{5}$ نجد أن

$$\log_{10}(b) > (n-1) \times \log_{10}(\alpha) > \frac{n-1}{5}$$ أي : $5 \times \log_{10}(b) > n-1$.

لنقل أن العدد b له k خانة عشرية. أي $10^k > b$ فيكون $k > \log_{10}(b)$. أي $5 \times k > n-1$ و بما أن k و n أعداد صحيحة يمكننا أن نستنتج أن $5 \times k \geq n$. و هو المطلوب."
(Kenneth H. Rosen, 1984)

<u>ثالثاً</u>: خوارزمية إقليدس الممدّدة لحل المعادلات الديفونتية الخطية

سنتحدث في هذا القسم عن حل للمعادلات الديفونتية الخطية من الشكل $ax + by = c$ و التي ستفيدنا لاحقاً في حل التطابقات الخطية في الفصل الثاني.

من المبرهنة (1-1) بما أن القاسم المشترك الأكبر لعددين يقسمهما نجد أن $(a,b) \mid ax + by$ و بذلك نجد أنه إذا كان (a,b) لا يقسم c فليس للمعادلة حلول. أما إذا كان $(a,b) \mid c$ فيمكننا أن نبحث عن حلول للمعادلة $ax + by = (a,b)$ و من ثم نضرب طرفي المعادلة بـ $\frac{c}{(a,b)}$ للوصول للحلول المطلوبة.

تمثل خوارزمية إقليدس طريقة فعالة لحل هذه المعادلات و ذلك لأن خوارزمية إقليدس تتيح عند كل خطوة كتابة r_{i+2} كتركيب خطي من r_i و r_{i+1} فيمكننا من خلال المرور بخطوات الخوارزمية كتابة $r_n=(a,b)$ كتركيب خطي من $r_1=b$ و $r_0=a$ فنكون بذلك وصلنا للحلول المطلوبة.

"يمكن استخدام مثال لتوضيح طريقة حل المعادلات: فلنقم بحل $60x+22y=(60,22)$.

$$60=2\times 22+16$$
$$22=1\times 16+6$$
$$16=2\times 6+4$$
$$6=1\times 4+2$$
$$4=2\times 2+0$$

أولاً نعيد كتابة الخطوة الأولى لتصبح بالشكل: $16=a-2b$ حيث $b=22$ و $a=60$.

نعوض العدد 16 في الخطوة الثانية لنصل إلى :

$$b=1\times 16+6=1(a-2b)+6$$

أي:

$$6=b-(a-2b)=-a+3b$$

بالمتابعة نجد:

$$16=a-2b=2(-a+3b)+4=2\times 6+4$$
$$4=a-2b-2(-a+3b)=3a-8b$$
$$6=-a+3b=1(3a-8b)+2=1\times 4+2$$
$$2=-a+3b-3a+8b=-4a+11b$$

من الخطوة الأخيرة: $2=22\times 11+60\times -4$ أي أن الثنائية $(-4,11)$ حل للمعادلة."
(Joseph H.Silverman, 2012)

إن هذه الطريقة لحل المعادلات الديفونتية باستخدام خوارزمية إقليدس تتطلب الكثير من عمليات الاستبدال و التعويض و التي قد تجعل هذه الطريقة صعبة التطبيق برمجياً. لذلك سنعرض طريقة أخرى أكثر سهولة.

مبرهنة (1-9) : ليكن a و b عددين صحيحين فإن:

$$(a,b)=s_n a+t_n b$$

حيث n دليل العدد r_n الذي يمثل القاسم المشترك الأكبر ل a و b باستخدام خوارزمية إقليدس و كل من العددين s_n و t_n هو العنصر n من المتتاليتان المعرفتان بالشكل:

$$s_0 = 1, s_1 = 0, s_j = s_{j-2} - s_{j-1}q_{j-1}; j > 1$$

$$t_0 = 0, t_1 = 1, t_j = t_{j-2} - t_{j-1}q_{j-1}; j > 1$$

حيث q_j هي نواتج عمليات القسمة في خوارزمية إقليدس عند تطبيقها لإيجاد (a,b).

"البرهان: سوف نقوم بإثبات أن $r_j = s_j a + t_j b$ من أجل: $j = 0,1...n$ و بما أن $r_n = (a,b)$ نكون قد وصلنا للمطلوب.

سنثبت أن $r_j = s_j a + t_j b$ بوساطة الاستقراء الرياضي:

من أجل $j = 0$: $a = r_0 = 1a + 0b = s_0 a + t_0 b$.
من أجل $j = 1$: $b = r_1 = 0a + 1b = s_1 a + t_1 b$.

فالمبرهنة محققة عند 0 و 1.

الآن فلنفرض أن $r_k = s_k a + t_k b$ لكل $k \le n$. المطلوب: $r_{n+1} = s_{n+1} a + t_{n+1} b$.

من أجل الخطوة k من خورازمية إقليدس نجد أن $r_{n+1} = r_{n-1} - r_n \times q_n$ باستخدام فرض الاستقراء نجد:

$$\begin{aligned} r_{n+1} &= (s_{n-1}a + t_{n-1}b) - (s_n a + t_n b)q_n \\ &= (s_{n-1} - s_n q_n)a + (t_{n-1} - t_n q_n)b \\ &= s_{n+1}a + t_{n+1}b \end{aligned}$$

و هو المطلوب." (Kenneth H. Rosen, 1984)

نلاحظ أنه يمكن أن يكون لنفس المعادلة أكثر من حل, مثل المعادلة $5x + 3y = 1$ لها الحل $(-1,2)$ و كذلك الحلول $(-4,7),(-7,12)...$ في الحقيقة إن للمعادلة $ax + by = (a,b)$ عدد لانهائي من الحلول و سنتحدث الآن عن إيجاد صيغة لجميع هذه الحلول.

مبرهنة (1-10) : للمعادلة $ax + by = (a,b)$ عدد لانهائي من الحلول. يمكن إيجاد حل لها (x_1, y_1) باستخدام خوارزمية إقليدس الممدّدة و من ثم يمكن الحصول على جميع الحلول الأخرى بالصيغة:

$$\left\{x_1+\frac{b}{(a,b)}k, \mathrm{y}_1-\frac{a}{(a,b)}k\right\}; k\in\mathbb{Z}$$

"البرهان: في البداية لندرس الحالة عندما $(a,b)=1$ عندها إذا كان (x_1,y_1) حلاً للمعادلة (يمكن إيجاد هذا الحل بخوارزمية إقليدس الممدّدة المذكورة سابقاً في هذا الفصل), فإن المطلوب هو إثبات أن جميع الحلول الأخرى يمكن الحصول عليها من الصيغة:

$$x=x_1+kb, y=y_1-ka$$

أولاً لنبرهن أن هذه الصيغة تعطي حلول للمعادلة:

$$a(x_1+kb)+b(y_1-ka)=ax_1+kab+by_1-kab$$
$$=ax_1+by_1=1$$

بعد ذلك علينا أن نبرهن أن جميع حلول المعادلة يمكن التعبير عنها بالصيغة السابقة.

ليكن لدينا حلين للمعادلة و هما (x_1,y_1) و (x_2,y_2) أي:

$$ax_1+by_1=1, ax_2+by_2=1$$

نضرب المعادلة الأولى ب y_2 و المعادلة الثانية ب y_1 و نطرح المعادلتين من بعضهما. بعد التبسيط نجد:

$$ax_1y_2-ax_2y_1=y_2-y_1$$

و بالمثل نضرب المعادلة الأولى ب x_2 و الثانية ب x_1 و نطرح و نبسط فنصل إلى:

$$by_1x_2-by_2x_1=x_2-x_1$$

لنسند $k=x_2y_1-x_1y_2$. نعوض k في النتيجتين السابقتين لنجد:

$$x_2=x_1+kb, y_2=y_1-ka$$

هذا يعني أن الحل الثاني تم الحصول عليه من الحل الأول بالقاعدة السابقة أي أن القاعدة صحيحة عند $(a,b)=1$. و لكن ماذا إن كان $(a,b)>1$!!

لنسند $g=(a,b)$. من خوارزمية إقليدس الممدّدة (المذكورة في هذا الفصل) يمكن الحصول على حل (x_1,y_1) للمعادلة $ax+by=g$ و لكن g يقسم كل من a و b فيكون (x_1,y_1) حل للمعادلة:

$$\frac{a}{g}x+\frac{b}{g}y=1$$

و هذه المعادلة الأبسط حلولها كما رأينا سابقاً هي:

$$\left\{x_1+\frac{b}{(a,b)}k, y_1-\frac{a}{(a,b)}k\right\}; k\in\mathbb{Z}$$

و هو المطلوب." (Joseph H.Silverman, 2012)

الفصل الثاني:

التطابقات الخطية و نظام البواقي الصيني

تلزم التطابقات الخطية لحل نظام بواقي صيني. و سنناقش في هذا الفصل حل التطابقات الخطية بالاعتماد على طرق حل المعادلات الديفونتية الخطية التي ناقشناها في الفصل الماضي بالإضافة إلى طرق لحلها باستخدام مبرهنة أويلر. و ثم سنناقش كيفية حل نظم البواقي الصينية بالاعتماد على التطابقات الخطية.

أولاً: أساسيات في التطابقات

سنذكر في البداية عدد من الخواص الأساسية والتعاريف في التطابقات و التي سنحتاجها في بحثنا.

"تعريف(2-1): نقول عن عددين صحيحين a و b أنهما متطابقان في القياس m إذا كان $m|(a-b)$ و رمزه:

$$a \equiv b(\mathrm{mod}\, m)$$

أما إذا كان m لا يقسم $a-b$ فإن a و b غير متطابقان بالقياس m و نرمز لذلك ب:

$$a \neq b(\mathrm{mod}\, m)$$

يفيد في كثير من الأحيان تحويل التطابق إلى مساواة لذلك تفيدنا الخاصة التالية:

إذا كان $a \equiv b(\mathrm{mod}\, m)$ فيوجد عدد صحيح k بحيث $a = km + b$.

للتطابقات خواص كثيرة أخرى مفيدة سنذكر بعضاً منها. ليكن m عدد صحيح موجب فإن:

- إذا كان a عدد صحيح فإن $a \equiv a(\mathrm{mod}\, m)$
- إذا كان a و b عددان صحيحان فإن $a \equiv b(\mathrm{mod}\, m)$ يكافئ $b \equiv a(\mathrm{mod}\, m)$
- إذا كان a و b و c أعداد صحيحة و كان $a \equiv b(\mathrm{mod}\, m)$ و $b \equiv c(\mathrm{mod}\, m)$ فإن $a \equiv c(\mathrm{mod}\, m)$.
- إذا كان a و b و c أعداد صحيحة و كان $a \equiv b(\mathrm{mod}\, m)$ فإن:
  - $a + c \equiv b + c(\mathrm{mod}\, m)$ ✓
  - $a - c \equiv b - c(\mathrm{mod}\, m)$ ✓
  - $ac \equiv bc(\mathrm{mod}\, m)$ ✓
- إذا كان a و b و c أعداد صحيحة و كان $d = (c, m)$ و $ac \equiv bc(\mathrm{mod}\, m)$ فإن

$$a \equiv b(\mathrm{mod}\, \frac{m}{d})$$

تعريف(2-2): نظام كامل من البواقي بالقياس m *(complete system of residues modulo m)* هو مجموعة من m عدد بحيث كل عدد صحيح يطابق بالقياس m أحد هذه الأعداد.

مبرهنة (2-1): إذا كان $r_1, r_2, r_3 ... r_m$ نظام كامل من البواقي بالقياس m و إذا كان $(a, m) = 1$ فإن:

$$ar_1 + b, ar_2 + b ... ar_m + b$$

يشكل أيضاً نظام كامل من البواقي بالقياس m." (Kenneth H. Rosen, 1984)

"تعريف(2-3): التابع $\phi(n)$ لأويلر *(Euler's phi function)*: لكل عدد صحيح n التابع $\phi(n)$ يساوي عدد الأعداد من 1 إلى n التي تكون أولية فيما بينها مع n". (Oystein Ore, 1948)

ثانياً: **التطابقات الخطية**

التطابقات الخطية تكون من الشكل:

$$ax \equiv b (\mathrm{mod}\, m)$$

و نعني بحل التطابق الخطي إيجاد جميع الحلول التي تحقق التطابق. يجدر بالذكر أنه إذا وجد حل للتطابق فهناك عدد لانهائي من الحلول للتطابق في مجموعة الأعداد الصحيحة مثلاً التطابق:

$$7x \equiv 3 (\mathrm{mod} 12)$$

له حل عند: $\mathrm{x} \equiv 9 (\mathrm{mod} 12)$

فللتطابق أيضاً الحلول : $(9, 21, 33...)$

نلاحظ أن جميع هذه الحلول متطابقة بالقياس m فنعتبر عند دراستها أنها حل واحد. و نهتم عند دراسة التطابقات الخطية بإيجاد الحلول المختلفة أي الحلول غير المتطابقة بالقياس m. أي أن x_1 و x_2 حلان مختلفان للتطابق إذا كان $x_1 \neq x_2 (\mathrm{mod}\, m)$.

قبل البدء بمناقشة طريقة حل التطابقات الخطية لنطلع على بعض الأمثلة المحلولة تجريبياً.

التطابق $(7x \equiv 3 (\mathrm{mod} 12))$ له حل واحد عند $(x \equiv 9 (\mathrm{mod} 12))$.
التطابق $(4x \equiv 2 (\mathrm{mod} 8))$ ليس له حلول (بتجريب جميع الأعداد من 0 إلى 7).
التطابق $(6x \equiv 9 (\mathrm{mod} 15))$ له ثلاثة حلول و هي $(x \equiv 4 (\mathrm{mod} 15))$ و $(x \equiv 9 (\mathrm{mod} 15))$ و $(x \equiv 14 (\mathrm{mod} 15))$.

و الآن لنبدأ بطريقة حل التطابقات الخطية. "من تعريف التطابق نجد من $(ax \equiv b (\mathrm{mod}\, m))$ أنه يوجد عدد y يحقق :

$$ax - b = my$$

$$ax - my = b$$

و بذلك نكون حولنا التطابق الخطي إلى معادلة ديفونتية خطية. أي أن حلول التطابق الخطي المذكور أولاً يكافئ حل المعادلة الديفونتية التي توصلنا إليها. فيمكننا نقل ما توصلنا إليه سابقاً عن المعادلات الديفونتية إلى التطابقات الخطية.

نعلم مما مرّ معنا سابقاً من المعادلات الديفونتية أن معادلة من الشكل $ax + by = c$ لها حلول فقط إذا كان القاسم المشترك الأكبر لأمثال x و y (أي a و b) يقسم c. لذلك يمكننا أن نصل إلى المبرهنة التالية:

مبرهنة (2-2) : تطابق خطي من الشكل:

$$ax \equiv b(\mathrm{mod}\, m)$$

له حلول فقط إذا كان: $(a,m) \mid b$ " (Oystein Ore, 1948)

و الآن لنفرض أن $d = (a,m) \mid b$ أي أن للتطابق حلول. كيف يمكننا الوصول إلى هذه الحلول ؟

نعلم ممّا مرّ معنا في الفصل السابق أن المعادلة من الشكل:

$$ax - my = b$$

يمكن إيجاد حلها الأول (x_1, y_1) باستخدام خوارزمية إقليدس الممدّدة, و من ثم جميع هذه الحلول يمكن الوصول لها بحسب المبرهنة (1-10) من الصيغة:

$$x = x_1 + \frac{m}{d}k, y = y_1 + \frac{a}{d}k$$

((ملاحظة:كما نعلم k هو أي عدد صحيح موجب أو سالب فاستبدلناه من صيغة المبرهنة(1-10) ب $-k$))

فنكون بذلك حصلنا على جميع حلول التطابق في الأعداد الصحيحة و هي $(x_1 + \frac{m}{d}k)$

و لكن السؤال هو هل هذه الحلول كلها متطابقة ؟

"لنعلم كم حل لدينا غير متطابق في القياس m نناقش حالة أن حلين $x = x_1 + \frac{m}{d}k$ و

$x' = x_1 + \frac{m}{d}k'$ متطابقين في القياس m عندها:

$$x_1 + \frac{m}{d}k \equiv x_1 + \frac{m}{d}k' (\mathrm{mod}\, m)$$

بطرح x_1 من طرفي التطابق:

$$\frac{m}{d}k \equiv \frac{m}{d}k' (\mathrm{mod}\, m)$$

بما أن $\frac{m}{d} \mid m$ فإن $(m, \frac{m}{d}) = \frac{m}{d}$ فبحسب خواص التطابق نجد:

$$k \equiv k' (\mathrm{mod}\, d)$$

بذلك نرى أننا نحصل على مجموعة الحلول غير المتطابقة للتطابق الخطي بأخذ $x = x_1 + \frac{m}{d}k$ حيث k تمر بنظام كامل من البواقي بالقياس d *(complete system of residues modulo d)*. أبسط طريقة للحصول على هذا النظام تكون ب: $k = 0,1,2...d-1$ و بذلك يكون لدينا d حل غير متطابق." (Kenneth H. Rosen, 1984)

"كما يجدر بالذكر أنه من الحل $x = x_1 + \frac{m}{d}k$ يمكن أن نصل إلى أن:

$$x \equiv x_1 (\mathrm{mod}\, \frac{m}{d})$$

أي أن جميع حلول التطابق متطابقة بالقياس $\frac{m}{d}$." (Oystein Ore, 1948)

بما سبق يمكننا وضع المبرهنة:

مبرهنة (2-3): التطابق الخطي $ax \equiv b (\mathrm{mod}\, m)$ له $d = (a, m)$ حل مختلف تعطى ب:

$$x = x_1 + \frac{m}{d}k; k = 0,1,2...d-1$$

و ذلك في حال كان $d \mid b$.

و الآن لنعطي مثال عن حل لتطابق خطي. ليكن التطابق :

$$9x \equiv 12 (\mathrm{mod} 15)$$

بما أن $(9,15) = 3 | 12$ نجد أن لدينا بالتحديد 3 حلول غير متطابقة بالقياس 15.
للحصول في البداية على الحل الأول نبحث عن حلول للمعادلة الديفونتية:

$$9x - 15y = 12$$

بتطبيق خوارزمية إقليدس الممدة نحصل على الحل $x_0 = 8$ و باقي الحلول تعطى ب:

$$x = 8 + \frac{15}{3} k = 8 + 5k$$

بوضع $k = 0,1,2$ نحصل على الحلول غير المتطابقة $x \equiv 8,13,3 (\mathrm{mod} 15)$.

"الآن سنناقش حالة خاصة من التطابقات الخطية, و هي تطابقات من الشكل ($ax \equiv 1 (\mathrm{mod} m)$). من المبرهنة (2-2) و المبرهنة (2-3) نجد أن التطابق السابق له حل فقط في حال $(a,m) = 1$ و في حال تحقق ذلك فالحلول كلها تكون متطابقة بالقياس m. لكل عدد a يحقق $(a,m) = 1$ يدعى حل التطابق $ax \equiv 1 (\mathrm{mod} m)$ مقلوب a بالقياس m.

عندما يكون لدينا مقلوب ل a بالقياس m يمكننا استخدامه لحل أي تطابق من الشكل $ax \equiv b (\mathrm{mod} m)$. لنوضح ذلك ليكن a' مقلوب a بالقياس m أي أن ($a'a \equiv 1 (\mathrm{mod} m)$) إذاً إذا كان $ax \equiv b (\mathrm{mod} m)$ فبضرب طرفي التطابق ب a' نجد $a'(ax) \equiv a'(b) (\mathrm{mod} m)$ و منه $x \equiv a'b (\mathrm{mod} m)$. (Kenneth H. Rosen, 1984)"

لنعطي مثال عن ذلك, لنقم بحل التطابق التالي:

$$7x \equiv 22 \mod 31$$

بما أن العددان 7 و 31 أوليان فيما بينهما فيمكن إيجاد مقلوب للعدد 7 بالقياس 31. نقوم بحل التطابق:

$$7y \equiv 1 (\mathrm{mod} 31)$$

بحل التطابق السابق نصل إلى أن $y \equiv 9 (\mathrm{mod} 31)$

أي أن 9 مقلوب 7 بالقياس 31 فبضرب طرفي التطابق الأول ب 9 نجد:

$$9 \times 7x \equiv 9 \times 22 (\mathrm{mod} 31)$$

أي: $x \equiv 198 \equiv 12 (\mathrm{mod} 31)$

إذاً كما رأينا يمكننا حل التطابقات الخطية من الشكل $ax \equiv b(\mathrm{mod}\, m)$ عندما a و m أوليان فيما بينهما باستخدام مقلوب a بالقياس m. و هذا المقلوب يمكن حسابه إما بالطريقة التي تحدثنا عنها سابقاً (تحويل التطابق إلى معادلة ديفونتية خطية) أو باستخدام المبرهنة التالية:

مبرهنة (2-4) : ((مبرهنة أويلر)) : لكل عدد a أولي فيما بينه مع m يتحقق:

$$a^{\phi(m)} \equiv 1(\mathrm{mod}\, m)$$

"البرهان: لنقم بأخذ مجموعة الأعداد الأصغر من m الأولية فيما بينها مع m و لتكن كالتالي:

$$S = \left\{ r_1, r_2 \ldots r_{\phi(\mathrm{m})} \right\}$$

نضرب كل عدد من المجموعة السابقة ب a و نقسم على m لنحصل على:

$$ar_i = q_i m + r_i'; 0 \le r_i' < m$$

إن كل من a و r_i أوليان فيما بينهما مع m فـ ar_i أولي فيما بينه مع m فبحسب المبرهنة (1-5)(مبرهنة إقليدس) فإن r_i' أولي فيما بينه مع m. بذلك نجد أن كل من r_i' هو عنصر من المجموعة S.

نكتب العلاقة $ar_i = q_i m + r_i'$ بالشكل:

$$ar_i \equiv r_i' (\mathrm{mod}\, m)$$

إن عددين r_i و r_j مختلفين من S لا يمكن أن ينتج عنهما نفس العدد r_i' لأنه في حال ذلك سيكون :

$$ar_i \equiv ar_j (\mathrm{mod}\, m)$$

و ذلك بحسب خواص التطابق يؤدي إلى:

$$r_i \equiv r_j (\mathrm{mod}\, m)$$

و بما أن كل من r_i و r_j أصغر من m هذا يؤدي إلى $r_i = r_j$ و هذا تناقض. بذلك نجد أن كل من r_i و r_i' هما عناصر المجموعة S و لكن بترتيب مختلف.

من العلاقة $ar_i \equiv r_i' (\mathrm{mod}\, m)$ بضرب ال $\phi(m)$ تطابق (كل حد إلى حد) نجد:

$$a^{\phi(m)} r_1 r_2 ... r_{\phi(m)} \equiv r_1' r_2' ... r_{\phi(m)}' (\mathrm{mod}\, m)$$

بما أن $r_1, r_2 ... r_{\phi(m)}$ و $r_1', r_2' ... r_{\phi(m)}'$ عناصر لنفس المجموعة و لكن بغير ترتيب فإن جداءي كل مجموعة منهما متساويان. بتقسيم طرفي التطابق السابق على هذا الجداء نصل إلى:

$$a^{\phi(m)} \equiv 1 (\mathrm{mod}\, m)$$

و هو المطلوب." (Oystein Ore, 1948)

((ملاحظة: المجموعة S في المبرهنة السابقة تدعى نظام مختصر من البواقي بالقياس m (*reduced residue system modulo* m)))

كيف يمكن استعمال مبرهنة أويلر من أجل إيجاد مقلوب a بالقياس m؟ ببساطة في حال كان a و m أوليان فيما بينهما فإن مقلوب a يساوي: $a' = a^{\phi(m)-1}$ و ذلك لأن
$aa^{\phi(m)-1} = a^{\phi(m)} \equiv 1 (\mathrm{mod}\, m)$ فإذا كان لدينا التطابق $ax \equiv b (\mathrm{mod}\, m)$ حيث a و m أوليان فيما بينهما فبضرب الطرفين بـ $a^{\phi(m)-1}$ نجد أن $x \equiv ba^{\phi(m)-1} (\mathrm{mod}\, m)$ وبذلك نكون حصلنا على الحل المطلوب.

لحساب التابع $\phi(n)$ لا داعي للمرور بالأعداد الأصغر من n و التأكد من أنها أولية فيما بينها مع n إذ أنّ التابع ϕ يتمتع بخاصية تقدّم طريقة مختصرة لحسابه. أولاً سنقوم بتعريف هذه الخاصية و طريقة استخدامها ثم سنثبت تمتع التابع ϕ بها.

"<u>تعريف(2-4):</u> تابع قابل للحساب (*arithmetic function*): هو تابع معرف على جميع الأعداد الصحيحة الموجبة تماماً.

<u>تعريف(2-5):</u> تابع ضربي (*multiplicative function*): نقول عن تابع قابل للحساب f أنه ضربي إذا كان لأي عددين أوليان فيما بينهما m و n يكون $f(nm) = f(n) f(m)$. "
(Kenneth H. Rosen, 1984)

مبرهنة (2-5) : إذا كان التابع f تابع ضربي و كان $n = p_1^{a_1} p_2^{a_2} ... p_s^{a_s}$ هو تحليل العدد n لعوامله الأولية يكون $f(n) = f(p_1^{a_1}) f(p_2^{a_2}) ... f(p_s^{a_s})$.

"البرهان: بما أن f تابع ضربي و $(p_1^{a_1}, p_2^{a_2} p_3^{a_3} ... p_s^{a_s}) = 1$ نجد أن

$$f(n) = f\left(p_1^{a_1} p_2^{a_2} p_3^{a_3} ... p_s^{a_s}\right) = f\left(p_1^{a_1} (p_2^{a_2} p_3^{a_3} ... p_s^{a_s})\right) = f\left(p_1^{a_1}\right) f\left(p_2^{a_2} p_3^{a_3} ... p_s^{a_s}\right)$$

. بما أن $(p_2^{a_2}, p_3^{a_3}...p_s^{a_s})=1$ نعلم أن $f\left(p_2^{a_2}p_3^{a_3}...p_s^{a_s}\right)=f\left(p_2^{a_2}\right)f\left(p_3^{a_3}...p_s^{a_s}\right)$ بذلك يكون $f\left(n\right)=f\left(p_1^{a_1}\right)f\left(p_2^{a_2}\right)f\left(p_3^{a_3}...p_s^{a_s}\right)$ بالمتابعة بهذه الطريقة نصل إلى :

$f(n)=f(p_1^{a_1})f(p_2^{a_2})...f(p_s^{a_s})$ و هو المطلوب." (Kenneth H. Rosen, 1984)

سنناقش أولاً قيم التابع ϕ عند الأعداد الأولية و عند قوى الأعداد الأولية ثم سنتوصل إلى صيغة لحسابه عند أي عدد صحيح موجب.

مبرهنة (2-6) : العدد p أولي إذا و فقط إذا كان $\phi(p)=p-1$.

"البرهان: إذا كان p عدد أولي فكل عدد موجب تماماً أصغر من p أولي فيما بينه مع p و بما أنه يوجد $p-1$ عدد موجب تماماً أصغر من p يكون $\phi(p)=p-1$.

بالمقابل إذا كان p عدد مركب (غير أولي) فيوجد ل p قاسم و ليكن d بحيث $1<d<p$ فبالتأكيد p و d غير أوليان فيما بينهما. بما أن أحد الأعداد $1,2,3...p-1$ و الذي هو d ليس أولي فيما بينه مع p فإن $\phi(p)\le p-2$. وبالتالي إذا كان $\phi(p)=p-1$ يكون p عدد أولي."

(Kenneth H. Rosen, 1984)

مبرهنة (2-7) : إذا كان p عدد أولي و كان a عدد موجب تماماً فإن $\phi(p^a)=p^a-p^{a-1}$.

"البرهان: إن عدد الأعداد الأصغر من p^a التي ليست أولية فيما بينها مع p^a هي عدد الأعداد الأصغر من p^a و التي تقبل القسمة على p و هذه الأعداد عددها $\frac{p^a}{p}=p^{a-1}$. و بالتالي يوجد p^a-p^{a-1} عدد أصغر من p^a و أولي فيما بينه مع p^a . أي $\phi(p^a)=p^a-p^{a-1}$."

(Kenneth H. Rosen, 1984)

لإيجاد صيغة من أجل حساب $\phi(n)$ من خلال تحليل n لعوامله الأولية نحتاج أولاً لإثبات أن التابع ϕ تابع ضربي.

مبرهنة (2-8) : إذا كان m و n عددان صحيحان موجبان تماماً أوليان فيما بينهما, فإن

$$\phi(nm)=\phi(n)\phi(m)$$

"البرهان: لنقم بعرض الأعداد من 1 إلى nm كما يلي:

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \ldots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \ldots & (n-1)m+2 \\ 3 & m+3 & 2m+3 & \ldots & (n-1)m+3 \\ . & . & . & & . \\ . & . & . & & . \\ . & . & . & & . \\ m & 2m & 3m & .... & nm \end{array}$$

والآن لنفرض أن لدينا العدد r أصغر أو يساوي m. إذا كان $d=(m,r)>1$ فلا يوجد أي عدد في السطر r أولي فيما بينه مع mn لأن أي عدد من السطر r يكتب بالشكل $km+r$ حيث $0\le k\le n-1$ فيكون $d\mid km+r$ لأن $d\mid m$ و $d\mid r$.

إذا لنبحث عن الأعداد في الشكل السابق الأولية فيما بينها مع mn يجب أن ننظر للسطر r فقط إذا كان $(m,r)=1$. بما أن $(m,r)=1$ فجميع عناصر هذا السطر أولية فيما بينها مع m.بحسب المبرهنة (1-2) العناصر ال n في السطر ال r تشكل نظام كامل من البواقي بالقياس n. بالتالي: $\phi(n)$ من هذه الأعداد أولية فيما بينها مع n. بما أن هذه المجموعة من $\phi(n)$ عدد أيضاً أولية فيما بينها مع m فهذه الأعداد أولية فيما بينها مع mn.

بما أنه لدينا $\phi(m)$ سطر في كل منها $\phi(n)$ عدد أولي فيما بينه مع mn. يمكن أن نستنتج أن:

$$\phi(nm)=\phi(n)\phi(m)$$

و هو المطلوب." (Kenneth H. Rosen, 1984)

بجمع المبرهنات السابقة يمكننا الوصول للصيغة المطلوبة للتابع ϕ و هي كالتالي:

مبرهنة (2-9): ليكن $n=p_1^{a_1}p_2^{a_2}\ldots p_s^{a_s}$ هو تحليل العدد n لعوامله الأولية فإن:

$$\phi(n)=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_s})$$

"البرهان: بما أن ϕ تابع ضربي فبحسب المبرهنة (2-5):

$$\phi(n)=\phi(p_1^{a_1})\phi(p_2^{a_2})\ldots\phi(p_s^{a_s})$$

و من المبرهنة (2-7):

$$\phi(p_j^{a_j}) = p_j^{a_j} - p_j^{a_j-1} = p_j^{a_j}(1-\frac{1}{p_j})$$

فيكون:

$$\phi(n) = p_1^{a_1}(1-\frac{1}{p_1})p_2^{a_2}(1-\frac{1}{p_2})...p_s^{a_s}(1-\frac{1}{p_s}) =$$

$$p_1^{a_1}p_2^{a_2}...p_s^{a_s}(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_s}) =$$

$$n(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_s})$$

و هو المطلوب". (Kenneth H. Rosen, 1984)

و بهذا نكون وصلنا للصيغة المطلوبة لإيجاد قيمة التابع ϕ من أجل استخدامه في حل التطابقات الخطية.

إن مبرهنة أويلر هي في الأصل تعميم لمبرهنة قدمها العالم فيرما و الذي لم يقم بنشر إثباته لها. و نشر إثباتها لأول مرة العالم أويلر ثم قدم العالم أويلر تعميماً لهذه المبرهنة و هذا التعميم هو المبرهنة (2-4) التي ناقشناها سابقاً. و لإثبات مبرهنة فيرما يمكن ببساطة اعتبارها حالة خاصة من مبرهنة أويلر بدل إثباتها بطرق أخرى منفصلة عن مبرهنة أويلر.

مبرهنة (2-10) : (مبرهنة فيرما الصغرى) : إذا كان p عدد أولي و كان a عدد صحيح لا يقبل القسمة على p فإن :

$$a^{p-1} \equiv 1(\text{mod } p)$$

ثالثاً: **البواقي الصينية**

سنهتم في هذا القسم بدراسة أنظمة التطابقات التي تكون بمتغير واحد و لكن بقياسات مختلفة. مثال عن ذلك:

$$x \equiv 1(\text{mod } 3)$$
$$x \equiv 2(\text{mod } 5)$$
$$x \equiv 3(\text{mod } 7)$$

و يهدف حل النظام إلى إيجاد جميع الحلول x التي تحقق جميع هذه التطابقات, و سيتم مناقشة طريقة لحل مثل هذا النظام من خلال مبرهنة البواقي الصينية.

مبرهنة (2-11) : ((مبرهنة البواقي الصينية)): ليكن $m_1, m_2 ... m_r$ أعداد موجبة أولية فيما بينها مثنى مثنى فللنظام من التطابقات :

$$x \equiv a_1 (\mathrm{mod}\, m_1)$$
$$x \equiv a_2 (\mathrm{mod}\, m_2)$$
$$.$$
$$.$$
$$.$$
$$x \equiv a_r (\mathrm{mod}\, m_r)$$

حل وحيد بالقياس : $M = m_1 m_2 ... m_r$

"البرهان: للإثبات نوجد أولاً حل لنظام البواقي ثم نثبت أنه وحيد بالقياس M . لنوجد الحل فلنسند $M_k = M / m_k = m_1 m_2 ... m_{k-1} m_{k+1} ... m_r$. بما أن $(m_k, m_j) = 1$ لكل $k \neq j$ يمكننا أن نرى أن $(M_k, m_k) = 1$ و بالتالي بحسب المبرهنة (2-3) التطابق $M_k y_k \equiv 1 (\mathrm{mod}\, m_k)$ له حل وحيد (أي أن y_k هو مقلوب العدد M_k بالقياس m_k). و الآن لنضع المجموع الآتي:

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_r M_r y_r$$

لنثبت أن x حل للنظام يجب أن نثبت أن $x \equiv a_k (\mathrm{mod}\, m_k)$ من أجل $k = 1, 2, 3 ... r$. بما أن $m_k \mid M_j$ لكل $k \neq j$ أي $M_j \equiv 0 (\mathrm{mod}\, m_k)$ فإنه في المجموع المكون لـ x جميع الأقسام عدا القسم الـ k تطابق 0 بالقياس m_k فبالتالي $x \equiv a_k M_k y_k (\mathrm{mod}\, m_k)$ و بما أن $M_k y_k \equiv 1 (\mathrm{mod}\, m_k)$ نجد أن $x \equiv a_k (\mathrm{mod}\, m_k)$.

و الآن بقي في البرهان أن نثبت أن أي حلين للنظام متطابقان في القياس M . ليكن x_1 و x_2 حلان للنظام المذكور سابقاً. نعلم أن $x_1 \equiv x_2 \equiv a_k (\mathrm{mod}\, m_k)$ أي أن $m_k \mid (x_1 - x_2)$ لكل $k = 1, 2, 3 ... r$ و بما أن $(m_k, m_j) = 1$ لكل $k \neq j$ يمكننا أن نستنتج أن $M \mid (x_1 - x_2)$ و منه $x_1 \equiv x_2 (\mathrm{mod}\, M)$ و هو المطلوب." (Kenneth H. Rosen, 1984)

إن إثبات مبرهنة البواقي الصينية يعطينا خوارزمية لحلها و لتوضيحها أكثر فلنعطي مثال لها:

لنقم بحل نظام البواقي الذي ذكر في بداية هذا القسم أي النظام:

$$x \equiv 1(\mathrm{mod}\,3)$$
$$x \equiv 2(\mathrm{mod}\,5)$$
$$x \equiv 3(\mathrm{mod}\,7)$$

الحل: $M = 3\times 5\times 7 = 105$, $M_1 = M / m_1 = 105/3 = 35$

$M_2 = M / m_2 = 105/5 = 21$, $M_3 = M / m_3 = 105/7 = 15$

$35y_1 \equiv 1(\mathrm{mod}\,3)$ أي $2y_1 \equiv 1(\mathrm{mod}\,3)$ أي $y_1 \equiv 2(\mathrm{mod}\,3)$.

$21y_2 \equiv 1(\mathrm{mod}\,5)$ و هذا يؤدي مباشرة إلى $y_2 \equiv 1(\mathrm{mod}\,5)$.

$15y_3 \equiv 1(\mathrm{mod}\,7)$ و هذا يؤدي مباشرة إلى $y_3 \equiv 1(\mathrm{mod}\,7)$.

$$x \equiv 1\times 35\times 2 + 2\times 21\times 1 + 3\times 15\times 1 \equiv 157 \equiv 52(\mathrm{mod}\,105)$$

بالجمع بين مبرهنة (2-11) البواقي الصينية و المبرهنة (2-4) مبرهنة أويلر يمكننا مباشرة وضع المبرهنة التالية:

مبرهنة (2-12) : حل نظام التطابقات :

$$x \equiv a_1(\mathrm{mod}\,m_1)$$
$$x \equiv a_2(\mathrm{mod}\,m_2)$$
$$.$$
$$.$$
$$.$$
$$x \equiv a_r(\mathrm{mod}\,m_r)$$

حيث $m_1, m_2 \ldots m_r$ أولية فيما بينها مثنى مثنى هو :

$$x \equiv a_1 M_1^{\phi(m_1)} + a_2 M_2^{\phi(m_2)} \ldots a_r M_r^{\phi(m_r)} (\mathrm{mod}\,M)$$

إن المبرهنة (2-11) فعالة و هامة لحل أنظمة البواقي الصينية عندما تكون الأعداد $m_1, m_2 \ldots m_r$ أولية فيما بينها, و لكن ماذا يحدث إذا لم تكن هذه الأعداد أولية فيما بينها **!؟** سنناقش هذه الحالة و لكن لنقوم بذلك أولاً نحتاج إلى التعريف التالي:

<u>تعريف(2-6):</u> المضاعف المشترك الأصغر لعددين a و b هو أصغر عدد موجب تماماً يقبل القسمة على كل منهما و يرمز له ب $lcm[a,b]$ أي *((least common multiplier))* أو بالرمز $[a,b]$.

يحقق المضاعف المشترك الأصغر لعددين a و b الخاصية التالية:

$$\frac{ab}{(a,b)}=[a,b]$$

مبرهنة (2-13) : تطابقان من الشكل :

$$x\equiv a(\mathrm{mod}\, m)$$
$$x\equiv b(\mathrm{mod}\, n)$$

لهما حل فقط عندما :

$$a\equiv b(\mathrm{mod}(n,m))$$

و إذا تحقق ذلك يكون الحل وحيد بالقياس $[n,m]$:

$$x\equiv x_0(\mathrm{mod}[n,m])$$

"البرهان: من التطابق الأول و بحسب تعريف التطابق نجد:

$$x=tm+a$$

حيث t عدد صحيح. بتعويض هذه المساواة في التطابق الثاني نجد:

$$tm+a\equiv b(\mathrm{mod}\, n)$$
$$tm\equiv b-a(\mathrm{mod}\, n)$$

بوضع $d=(n,m)$ بحسب المبرهنة (2-2) التطابق الخطي السابق له حل فقط عندما $d\mid b-a$ بحسب تعريف التطابق نصل إلى:

$$a\equiv b(\mathrm{mod}\, d)$$

و بهذا نكون أثبتنا القسم الأول من المبرهنة و الآن في حال تحقق $d\mid b-a$ يمكننا تقسيم طرفي التطابق $tm\equiv b-a(\mathrm{mod}\, n)$ على d بحسب خواص التطابق نجد:

$$t\frac{m}{d}\equiv\frac{b-a}{d}(\mathrm{mod}\frac{n}{d})$$

ليكن t_0 حل للتطابق السابق و ليكن $x_0=t_0m+a$. إن x_0 هو أحد الحلول للتطابقين الأصليين و t_0 يحقق:

$$t \equiv t_0 (\mathrm{mod}\, \frac{n}{d})$$

أي بحسب تعريف التطابق:

$$t = \frac{n}{d} u + t_0$$

حيث u عدد صحيح. بتعويض قيمة t في قيمة x نجد :

$$x = m(\frac{n}{d} u + t_0) + a$$
$$= \frac{mn}{d} u + mt_0 + a$$
$$= x_0 + [n, m]u$$

أي أنه بحسب تعريف التطابق:

$$x \equiv x_0 (\mathrm{mod}[n, m])$$

عند دراسة مجموعة من التطابقات لعدة قياسات *((moduls))* و في حال كان x_0 حل لها, فمن الواضح أنه إذا أضفنا إلى x_0 أي مضاعف للمضاعف المشترك الأصغر لهذه القياسات فإن العدد الناتج سيكون أيضاً حل لهذه التطابقات لذلك ففي هذه التطابقات يكون الحل وحيداً بقياس المضاعف المشترك الأصغر لهذه القياسات. و هو المطلوب.

يمكن تعميم طريقة الحل السابقة على أكثر من تطابقين بتكرار تطبيق طريقة الحل, فإذا كان لدينا التطابقات:

$$x \equiv a_1 (\mathrm{mod}\, m_1)$$
$$x \equiv a_2 (\mathrm{mod}\, m_2)$$
$$x \equiv a_3 (\mathrm{mod}\, m_3)$$

يمكننا إيجاد حل لأول تطابقين بحسب الطريقة التي تحدثنا عنها في إثبات المبرهنة (2-13) فيكون الحل:

$$x \equiv x_0 (\mathrm{mod}[m_1, m_2])$$

و هذا الحل يتم تعويضه في التطابق التالي و إيجاد الحل و هكذا .. , يمكننا أن نرى أنه إذا وجد حل لهذا النظام من التطابقات فإنه يكون وحيداً بالقياس $[m_1, m_2 ... m_r]$.

ما هو شرط وجود هذا الحل؟ من الواضح أنه ليوجد حل لهذا النظام من التطابقات يجب أن يكون لأي تطابقين من هذه التطابقات حل مشترك بقياس المضاعف المشترك الأصغر لقياسيهما أي أنه يجب أن يتحقق لأي ثنائي a_i و a_j:

(Oystein Ore, 241-244) " $a_i \equiv a_j (\mathrm{mod}(m_i, m_j))$

و بهذا نكون قد توصلنا لطريقة لحل نظام من التطابقات تكون فيه القياسات غير أولية فيما بينها.

مثال: لنقم بحل نظام التطابقات التالي:

$$x \equiv 2(\mathrm{mod}\,9)$$
$$x \equiv 8(\mathrm{mod}\,15)$$
$$x \equiv 3(\mathrm{mod}\,25)$$

أولاً نتحقق من وجود حل: بالنسبة للتطابق الأول و الثاني: $8 \equiv 2(\mathrm{mod}\,3)$ محققة
بالنسبة للتطابق الثاني و الثالث $8 \equiv 3(\mathrm{mod}\,5)$ محققة.
أما قياسي التطابق الأول و الثالث أوليان فيما بينهما فوجود حل مشترك لهما مؤكد. و بالتالي للنظام حل.

من التطابق الأول نجد $x = 9t + 2$ بتعويض ذلك في التطابق الثاني نجد أن t تحقق:

$$9t \equiv 6(\mathrm{mod}\,15)$$
$$3t \equiv 2(\mathrm{mod}\,5)$$
$$\mathrm{t} \equiv 4(\mathrm{mod}\,5)$$
$$t = 5u + 4$$
$$x = 9t + 2 = 9(5u + 4) + 2$$
$$x = 45u + 38$$

بتعويض ذلك في التطابق الثالث نجد:

$$45u \equiv -35(\mathrm{mod}\,25)$$
$$-5u \equiv 15(\mathrm{mod}\,25)$$
$$-u \equiv 3(\mathrm{mod}\,5)$$
$$u \equiv 2(\mathrm{mod}\,5)$$
$$u = 5k + 2$$

$$x = 45u + 38 = 45(5k + 2) + 38$$
$$x = 225k + 128$$
$$x \equiv 128 (\mathrm{mod}\, 225)$$

و بهذا نكون أنهينا الحل.

و بذلك نكون أنهينا دراستنا لأنظمة التطابقات التي تكون بمتغير واحد و بقياسات مختلفة.

الفصل الثالث:

العمليات الحسابية على الأعداد الكبيرة

إن لكل حاسوب أو آلة حد عددي معين للقيام بالعمليات الحسابية. و لا يمكن القيام بالعمليات الحسابية على أعداد أكبر من هذا الحد بالطرق العادية بل نحتاج إلى خوارزميات تستفيد من الطرق العادية للقيام بالعمليات الحسابية على أعداد أضخم من الحد المتوافر, و في هذا الفصل سنناقش طريقة للقيام بذلك بوساطة التطابقات.

أولاً: فكرة الخوارزمية و اختيار القياسات

إن الخوارزمية تنص على اختيار عدة قياسات $m_1, m_2 ... m_r$ أولية فيما بينها مثنى مثنى و العمل بشكل غير مباشر على البواقي $u \bmod m_1, u \bmod m_2 ... u \bmod m_r$ بدلاً من العمل بشكل مباشر مع العدد u.

من أجل التسهيل فلنعتمد الترميز التالي:

$$u_1 = u \bmod m_1, u_2 = u \bmod m_2 ... u_r = u \bmod m_r$$

يمكن الحصول على الأعداد $u_1, u_2 ... u_r$ من العدد الصحيح u بسهولة بوساطة القسمة. و يجدر بالذكر أنه في حال لم يكن العدد u ضخماً جداً فلن يحدث أي خسارة للمعلومات بهذه الطريقة. فمثلاً بوضع $m_1 = 7$ و $m_2 = 11$ و $m_3 = 13$ فإذا كان $0 \le u, v \le 1000$ و $u \ne v$ فيستحيل أن يكون $(u_1, u_2 ... u_r)$ مساوياً لـ$(v_1, v_2 ... v_r)$ و ذلك من المبرهنة (2-11) مبرهنة البواقي الصينية.

و بذلك يمكننا اعتبار $(u_1, u_2 ... u_r)$ تمثيل جديد للعدد u و لنسمه تمثيل بالتطابقات للعدد u. الأفضلية التي يقدمها التمثيل بالتطابقات هي أن عمليات الضرب و الجمع و الطرح تتم بسهولة و هي كالتالي:

$$(u_1, u_2 ... u_r) + (v_1, v_2 ... v_r) = ((u_1 + v_1) \bmod m_1, ..., (u_r + v_r) \bmod m_r)$$
$$(u_1, u_2 ... u_r) - (v_1, v_2 ... v_r) = ((u_1 - v_1) \bmod m_1, ..., (u_r - v_r) \bmod m_r)$$
$$(u_1, u_2 ... u_r) \times (v_1, v_2 ... v_r) = ((u_1 \times v_1) \bmod m_1, ..., (u_r \times v_r) \bmod m_r)$$

و ذلك بفضل مبادئ أساسية في التطابقات (كما في القسم الأول من الفصل الثاني).

"إن سلبيات تمثيل عدد بالتطابقات هي أنه من الصعب أن نعلم إذا كان العدد سالباً أو موجباً و من الصعب المقارنة بين عددين. كما أنه من الصعب أن نعلم فيما إذا كان قد حدث تجاوز للحد المسموح *(overflow)* نتيجة عمليات جمع أو طرح أو ضرب. كذلك من الصعب أكثر القيام بعمليات قسمة. لذلك فإنه في حال الحاجة بشكل كبير لهذه العمليات مع عمليات الجمع و الطرح و الضرب فيمكن استخدام التمثيل بالتطابقات

فقط في حال وجود طريقة سريعة للتحويل من التمثيل العادي إلى التمثيل بالتطابقات و بالعكس."
(Donald Ervin Knuth, 1981)

"إن الاعتماد على تمثيل العدد بالتطابقات يساعد في تقليل الوقت اللازم للعمليات الحسابية. فهو يساعد على تقليل التعقيد الزمني لعملية الضرب مقارنة مع الطرق الأخرى التي تستخدم في التعامل مع الأعداد الكبيرة (من دون حساب الزمن اللازم للتحويل بين التمثيل العادي و التمثيل بالتطابقات), كما أنه على العديد من الحواسيب عالية السرعة يمكن أداء عدة مهام بشكل متوازٍ (بنفس الوقت), لذلك فإن تحويل عملية حسابية واحدة على عددين كبيرين إلى عدة عمليات حسابية على أعداد صغيرة يؤدي إلى تنفيذ هذه العمليات المتعددة بشكل أسرع." (Kenneth H.Rosen, 1984)

"من المبرهنة (2-11) مبرهنة البواقي الصينية نجد أنه يمكننا القيام بالعمليات الحسابية على أعداد مداها $M = m_1 m_2 ... m_r$ فمثلاً يمكننا العمل على جميع الأعداد الموجبة u الأصغر من M. و لكن عند القيام بعمليات الجمع و الطرح مع الضرب فإنه يفضل عادةً جعل جميع القياسات $m_1 m_2 ... m_r$ أعداد فردية بحيث يكون $M = m_1 m_2 ... m_r$ عدد فردي و القيام بالعمليات الحسابية على المدى:

$$-\frac{M}{2} < u < \frac{M}{2}$$

و التي تكافئ العمليات الحسابية على الأعداد الموجبة الأصغر من M.

بما أننا نريد M أن يكون أكبر ما يمكن فإن الأسهل هو أن نجعل m_1 أكبر عدد فردي أصغر من الحد المسموح به في الحاسوب. و m_2 أكبر عدد فردي أصغر من m_1 و أولي فيما بينه مع m_1. و m_3 أكبر عدد فردي أصغر من m_2 و أولي فيما بينه مع كل من m_1 و m_2. و الاستمرار بهذه الطريقة حتى الوصول إلى عدد كافٍ من القياسات m_j لتعطي المدى المطلوب M.

على الحواسيب التي تعتمد على النظام الثنائي يفضل اختيار القياسات m_j بطريقة مختلفة و هي باختيار:

$$m_j = 2^{e_j} - 1$$

إن هذا الاختيار للقياسات مفضل لأنه يبسّط العمليات الحسابية و ذلك لسهولة العمل بالقياس $2^{e_j} - 1$ كما سنرى لاحقاً. و عند هذا الاختيار للقياس يمكننا السماح بـ $0 \le u_j < 2^{e_j}$ أي أن u_j يمكن أن يكون أي عدد مؤلف من e_j بيت, أي أن الخيار $u_j = 2^{e_j} - 1$ متاح إلى جانب $u_j = 0$ و من الواضح أن ذلك لا يؤثر على الناتج بحسب المبرهنة (2-11) مبرهنة البواقي الصينية." (Donald Ervin Knuth, 1981)

بما أننا سنقوم باختيار قياسات بحيث تكون بالصيغة $m_j = 2^{e_j} - 1$ فإننا سنحتاج لمعرفة متى يكون عددان من هذه الصيغة أوليان فيما بينهما و هو ما سنناقشه الآن. في البداية سنثبت بعض المبرهنات ثم سنستفيد منها في إيجاد طريقة لمعرفة متى يكون عددان $2^a - 1$ و $2^b - 1$ أوليان فيما بينها.

مبرهنة (3-1): إذا كان a و b عددان صحيحان موجبان فإن باقي قسمة $2^a - 1$ على $2^b - 1$ هو $2^r - 1$ حيث r هو باقي قسمة a على b.

"البرهان: يمكننا كتابة a بالشكل $a = bq + r$ حيث r باقي قسمة a على b لدينا :

$$2^a - 1 = 2^{bq+r} - 1 = (2^b - 1)(2^{b(q-1)+r} + \ldots + 2^{b+r} + 2^r) + (2^r - 1)$$

ومنه نجد أن باقي قسمة $2^a - 1$ على $2^b - 1$ هو $2^r - 1$ وهو المطلوب."
(Kenneth H.Rosen, 1984)

سنستفيد من المبرهنة السابقة في إثبات التالي:

مبرهنة (3-2) : في حال كان a و b عددان صحيحان موجبان فإن $(2^a - 1, 2^b - 1) = 2^{(a,b)} - 1$.

"البرهان: بتطبيق خوارزمية إقليدس على العددين $r_0 = a$ و $r_1 = b$ نحصل على التالي:

$$r_0 = r_1 q_1 + r_2 ; 0 \le r_2 < r_1$$
$$r_1 = r_2 q_2 + r_3 ; 0 \le r_3 < r_2$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n ; 0 \le r_n < r_{n-1}$$
$$r_{n-1} = r_n q_n$$

بالاعتماد على المبرهنة (3-1) و خطوات خوارزمية إقليدس عند $r_0 = a$ و $r_1 = b$ فإنه عند تطبيق خوارزمية إقليدس على العددين $R_0 = 2^a - 1$ و $R_1 = 2^b - 1$ نحصل على:

$$R_0 = R_1 Q_1 + R_2 ; R_2 = 2^{r_2} - 1$$
$$R_1 = R_2 Q_2 + R_3 ; R_3 = 2^{r_3} - 1$$
$$\vdots$$
$$R_{n-2} = R_{n-1} Q_{n-1} + R_n ; R_n = 2^{r_n} - 1$$
$$R_{n-1} = R_n Q_n$$

و بذلك نحصل على آخر باقي غير معدوم $R_n = 2^{r_n} - 1 = 2^{(a,b)} - 1$ و الذي هو القاسم المشترك الأكبر ل R_0 و R_1 و هو المطلوب." (Kenneth H.Rosen, 1984)

مباشرة من المبرهنة السابقة يمكننا الوصول إلى:

مبرهنة (3-3): العددان $2^a - 1$ و $2^b - 1$ أوليان فيما بينهما إذا و فقط إذا كان a و b أوليان فيما بينهما.

فمثلاً مما سبق إذا كان الحد المسموح به في حاسوب يساوي 2^{32} فيمكننا اختيار $m_1 = 2^{32} - 1$ و $m_2 = 2^{31} - 1$ و $m_3 = 2^{29} - 1$ و $m_4 = 2^{27} - 1$ و $m_5 = 2^{25} - 1$ و $m_6 = 2^{23} - 1$ فبذلك يصبح بإمكاننا العمل مع أعداد تصل حتى $m_1 m_2 m_3 m_4 m_5 m_6 > 2^{165}$.

ثانياً: **خطوات الخوارزمية**

سنتحدث الآن عن طريقة تطبيق الخوارزمية, في البداية سنتحدث عن طريقة تحويل الأعداد المدخلة إلى تمثيلها بالتطابقات, ثم سنتحدث عن طرق القيام بالعمليات الحسابية الأساسية على الأعداد بالتطابقات ثم سنتحدث عن طريقة تحويل العدد من تمثيله بالتطابقات إلى تمثيله العادي (العشري أو الثنائي).

"لتحويل العدد u من تمثيله العادي إلى تمثيله بالتطابقات يمكننا ببساطة تقسيمه على $(m_1, m_2 ... m_r)$ و أخذ بواقي القسمة $(u_1, u_2 ... u_r)$. هناك أيضا طريقة أكثر سهولة, إذا كان لدينا $u = (v_m v_{m-1} ... v_1)_b$ و الذي هو تمثيل العدد u بنظام العد b, فيمكننا حساب كثير الحدود:

$$(...(v_m b + v_{m-1})b + ...)b + v_1$$

بوساطة التطابقات. عندما يكون نظام العد ثنائي أي $b=2$ و القياسات m_j لها الصيغة الخاصة $2^{e_j}-1$ فإن طريقة حساب باقي قسمة العدد u على m_j تصبح أبسط بكثير:
لنأخذ التمثيل الثنائي للعدد u و لنجمّع كل e_j بيت معاً, نجد:

$$u = a_t A^t + a_{t-1}A^{t-1}...a_1 A^1 + a_0$$

حيث $A=2^{e_j}$ و $0 \le a_k < 2^{e_j}; k = 0,1,2...t$. عندها:

$$u \equiv a_t + a_{t-1} + ... + a_1 + a_0 (\mathrm{mod}\, 2^{e_j}-1)$$

و ذلك ببساطة لأن $A=2^{e_j} \equiv 1 (\mathrm{mod}\, 2^{e_j}-1)$. و بذلك فإننا نحصل على u_j بجمع الأعداد ذات ال e_j بيت $a_0, a_1...a_t$". (Donald Ervin Knuth, 1981)

((ملاحظة: سنشرح طريقة جمع هذه الأعداد لاحقاً في هذا الفصل.))

"بعد التحويل إلى التمثيل بالتطابقات علينا القيام بالعمليات الحسابية. أي أنه لعددين $0 \le u_j, v_j < m_j$ نريد أن نقوم بحساب $u_j + v_j (\mathrm{mod}\, m_j)$ و $u_j - v_j (\mathrm{mod}\, m_j)$ و $u_j \times v_j (\mathrm{mod}\, m_j)$.
بالنسبة لعملية الضرب فعلينا القيام بعملية ضرب ثم قسمة. و لكن بالنسبة لعمليتي الجمع و الطرح فالموضوع أبسط و هو كالتالي:

$$u_j + v_j (\mathrm{mod}\, m_j) \begin{cases} u_j + v_j, & u_j + v_j < m_j \\ u_j + v_j - m_j, & u_j + v_j \ge m_j \end{cases}$$

$$u_j - v_j (\mathrm{mod}\, m_j) \begin{cases} u_j - v_j, & u_j - v_j \ge 0 \\ u_j - v_j + m_j, & u_j - v_j < 0 \end{cases}$$

و لكن بما أن $m_j = 2^{e_j} - 1$ و $0 \le u_j < 2^{e_j}$ فإن عمليتي الضرب و الجمع يمكن أن تتم بالشكل:

$$u_j \oplus v_j \begin{cases} u_j + v_j, & u_j + v_j < 2^{e_j} \\ (u_j + v_j (\mathrm{mod}\, 2^{e_j})) + 1, & u_j + v_j \ge 2^{e_j} \end{cases}$$

$$u_j \otimes v_j = (u_j v_j (\mathrm{mod}\, 2^{e_j})) \oplus \left\lfloor u_j v_j / 2^{e_j} \right\rfloor$$

حيث $\oplus$ و $\otimes$ تمثلان عمليتي الجمع و الضرب (بالترتيب) على العناصر $(u_1, u_2 \ldots u_r)$ و $(v_1, v_2 \ldots v_r)$". (Donald Ervin Knuth, 1981)

((ملاحظة: إن فكرة القيام بعملية الضرب بهذه الطريقة تماثل الفكرة المستخدمة لحساب باقي قسمة u على القياسات $m_1, m_2 \ldots m_r$ التي شُرحت سابقاً في هذا الفصل))

سنشرح لاحقاً في هذا الفصل عملية أخرى يمكن القيام بها على التمثيل بالتطابقات و لكن قبل ذلك سنناقش طريقة التحويل من التمثيل بالتطابقات إلى التمثيل العادي للعدد.

من أجل تحويل العدد من تمثيله بالتطابقات إلى تمثيله العادي نحتاج إلى المبرهنة (2-11) مبرهنة البواقي الصينية التي ناقشناها في الفصل الثاني. من هذه المبرهنة يكون العدد u مساوياً:

$$u = u_1 M_1 y_1 + u_2 M_2 y_2 \ldots u_r M_r y_r \pmod{M}$$

حيث $M_i = \frac{M}{m_i}$ و $y_i M_i \equiv 1 \pmod{m_i}$.

إن طريقة التحويل بين التمثيل بالتطابقات للعدد إلى التمثيل العادي للعدد و التي تمت مناقشتها سابقاً تنفع لهذا التحويل و هي مجدية لأن الأعداد M_i و y_i هي ثوابت لا نحتاج إلّا إلى حسابها مرة واحدة. و لكننا سنحتاج الأن في خوارزميتنا إلى طريقة أخرى أفضل و أسهل و ستفيدنا بعمليات أخرى غير التحويل إلى التمثيل العادي.

"إن هذه الطريقة تحتاج إلى $C(r,2)$ ثابت $c_{i,j}$ (أي $\frac{r(r-1)}{2}$ ثابت) بحيث :

$$c_{i,j} m_i \equiv 1 \pmod{m_j}; 1 \le i < j \le r$$

بعد حساب الثوابت نسند كما يلي:

$$v_1 \leftarrow u_1 \pmod{m_1}$$
$$v_2 \leftarrow (u_2 - v_1) c_{1,2} \pmod{m_2}$$
$$v_3 \leftarrow ((u_3 - v_1) c_{1,3} - v_2) c_{2,3} \pmod{m_3}$$

.

.

.

$$v_r \leftarrow ((\ldots((u_r - v_1) c_{1,r} - v_2) c_{2,r} \ldots - v_{r-2}) c_{r-2,r} - v_{r-1}) c_{r-1,r} \pmod{m_r}$$

كما يمكن إجراء الإسناد بطريقة أخرى (أسهل التطبيق برمجياً) و هي بوضع في البداية $(v_1...v_r) \leftarrow (u_1 (\mathrm{mod}\, m_1)...u_r (\mathrm{mod}\, m_r))$ و من ثم نكرر بعدّاد j و عند كل مرحلة j بحيث $1 \le j < r$ نسند $v_k \leftarrow (v_k - v_j) c_{j,k} (\mathrm{mod}\, m_k)$ لكل $j < k \le r$. عند ذلك:

مبرهنة (3-4): وفق الإسناد السابق لـ v_i يكون العدد:

$$u = v_r m_{r-1} m_{r-2} ... m_1 + v_{r-1} m_{r-2} m_{r-3} ... m_1 + ... + v_3 m_2 m_1 + v_2 m_1 + v_1$$

محققاً الشروط:

$$"0 \le u < M, u \equiv u_j (\mathrm{mod}\, m_j); 1 \le j \le r$$

(Donald Ervin Knuth, 1981)

البرهان: لنبرهن أولاً أن الشرط $u \equiv u_j (\mathrm{mod}\, m_j); 1 \le j \le r$ محقق.

"لكل $j; 1 \le j \le r$ من الواضح أن الأقسام $j+1, j+2...r$ من المجموع المكون لـ u تطابق 0 بالقياس m_j (لأنها من مضاعفات m_j), أم القسم j :

$$v_j \times m_{j-1} m_{j-2} ... m_2 m_1 \equiv$$
$$((...((u_j - v_1) c_{1,j} - v_2) c_{2,j} ... - v_{j-2}) c_{j-2,j} - v_{j-1}) c_{j-1,j} \times m_{j-1} m_{j-2} ... m_2 m_1$$
$$\equiv ((...((u_j - v_1) c_{1,j} - v_2) c_{2,j} ... - v_{j-2}) c_{j-2,j} m_{j-2} ... m_2 m_1 - v_{j-1} m_{j-2} ... m_2 m_1$$
$$\equiv ... \equiv u_j - v_1 - v_2 m_1 - ... - v_{j-1} m_{j-2} m_{j-3} ... m_2 m_1 (\mathrm{mod}\, m_j)$$

فبجمع القسم j مع باقي الأقسام نصل إلى $u \equiv u_j (\mathrm{mod}\, m_j)$ فيكون هذا الشرط محقق."

(Donald Ervin Knuth, 1981)

من الواضح أن الشرط $0 \le u$ محقق لأن u عبارة عن ضرب و جمع أعداد موجبة.
أما الشرط $u < M$ فيمكن برهانه كما يلي:

$$v_r \le m_r - 1 \Rightarrow v_r m_{r-1} m_{r-2} ... m_2 m_1 \le M - m_{r-1} m_{r-2} ... m_2 m_1$$
$$v_{r-1} \le m_{r-1} - 1 \Rightarrow v_{r-1} m_{r-2} m_{r-1} ... m_2 m_1 \le m_{r-1} m_{r-2} ... m_2 m_1 - m_{r-2} m_{r-3} ... m_2 m_1$$
$$.$$
$$.$$
$$.$$
$$v_3 \le m_3 - 1 \Rightarrow v_3 m_2 m_1 \le m_3 m_2 m_1 - m_2 m_1$$

$$v_2 \le m_2 - 1 \Rightarrow v_2 m_1 \le m_2 m_1 - m_1$$
$$v_1 \le m_1 - 1$$
$$u \le M - 1$$

و بذلك نصل إلى $u < M$, و هو المطلوب.

"في حال لم يكن المدى $0 \le u < M$ هو المدى المطلوب فيمكن بعد حساب u إضافة مضاعفات M المناسبة للوصول إلى المدى المطلوب. الشكل السابق لـ u يمكن حسابه بطريقة مشابهة لطريقة التحويل بين النظم العددية, و ذلك لأن حساب u من الشكل السابق يكافئ حساب:

$$u = ((...(v_r m_{r-1} + v_{r-1}) m_{r-2} + ...) m_2 + v_2) m_1 + v_1$$

و هو مشابه للتحويل بين النظم العددية لأن تحويل العدد $(v_r v_{r-1} ... v_2 v_1)_b$ من النظام العددي b إلى النظام العشري يكون بحساب:

$$((...(v_r b + v_{r-1}) b + ...) b + v_2) b + v_1$$

و بذلك نكون قد أوجدنا طريقة سهلة للتحويل من التمثيل بالتطابقات إلى التمثيل العادي للعدد."
(Donald Ervin Knuth, 1981)

ثالثاً: **المقارنة و تجاوز الحد و القسمة باستخدام التطابقات**

سنتحدث الآن عن إمكانية القيام بعمليات المقارنة بين أعداد كبيرة و قسمة أعداد كبيرة باستخدام التطابقات و التحقق من عدم حدوث تجاوز للحد المسموح و الصعوبات في تنفيذ هذه العمليات.

"بالإضافة إلى سهولة إيجاد الناتج u باستخدام المبرهنة (4-3) فإن للتمثيل $(v_r, v_{r-1} ... v_2, v_1)$ أفضلية أخرى, إذ أنّه يمكن استعمال هذا التمثيل للمقارنة بين عددين. فإذا كنا نعلم أن $0 \le u < M$ و $0 \le u' < M$ فيكون $u < u'$ إذا كان $v_r < v'_r$ أو $v_r = v'_r$ و $v_{r-1} < v'_{r-1}$ ...الخ. و بالتالي لا نحتاج إلى التحويل بشكل كامل من تمثيل بالتطابقات إلى تمثيل عادي لإجراء عملية مقارنة.

التمثيل ل u بالشكل $(v_r, v_{r-1} ... v_2, v_1)$ له استخدام آخر, و هو التأكد من عدم حدوث تجاوز للحد المسموح M في عملية الجمع (أي حدوث *overflow*) و ذلك بشرط أن M فردي. نقوم بذلك بوضع متحول إضافي لكل عدد u و هو $u_0 \equiv u \pmod 2$. عندها نعلم أنه حدث تجاوز للحد المسموح في العملية $a + b$ في حال كان $a_0 + b_0 \neq v_1 + v_2 ... v_r \pmod 2$ حيث $(v_r, v_{r-1} ... v_2, v_1)$ هو الإسناد المعرف في المبرهنة (4-3) للعدد $a + b$." (Donald Ervin Knuth, 1981)

((ملاحظة: الفكرة السابقة صحيحة بسبب ما يلي: إن a_0+b_0 سيعطينا باقي قسمة الناتج الصحيح $a+b$ على 2. أما $v_1+v_2...v_r$ سيعطينا إما باقي قسمة $a+b$ على 2 (في حال عدم حدوث تجاوز), أو سيعطينا باقي قسمة $a+b-M$ على 2 و الذي لا يساوي باقي قسمة $a+b$ على 2 لأن M فردي (في حال حدوث تجاوز) و هو المطلوب.))

"كما وجدنا فإنه يوجد طرق للقيام بعمليات المقارنة بين الأعداد و التحقق من حدوث تجاوز للحد العددي المسموح به بوساطة التطابقات, إلا أن هذه الطرق معقدة بشكل عام ممّا قد يفقد استخدام التطابقات لأفضليته." (Donald Ervin Knuth, 1981)

بالنسبة لعملية القسمة فهي تعد الأصعب تطبيقاً باستخدام التطابقات. إن عملية القسمة $\frac{u}{v}$ لا يمكن إجرائها إلّا في حال كان $v|u$ و في حال تحقق ذلك فلكل $u_j,v_j;1\le j\le r$ نحتاج لحساب $\frac{u_j}{v_j}(\mathrm{mod}\, m_j)$ أي $u_jv_j'(\mathrm{mod}\, m_j)$ حيث v_j' مقلوب v_j بالقياس m_j و الذي لايمكن إيجاده بحسب المبرهنة (2-2) إلا في حال كان $(v_j,m_j)=1$.بما أن v_j هو باقي قسمة v على M نجد من المبرهنة (1-5)

(مبرهنة إقليدس) أنه يجب أن يتحقق أن $(v,m_j)=1$. أي أنه لإجراء عملية قسمة واحدة $\frac{u}{v}$ يجب أن يتحقق أن $v|u$ و $(v,M)=1$ و يجب حل r تطابق خطي للحصول على الناتج, لذلك فعملية القسمة بوساطة التطابقات معقدة و غير مجدية لحاجتها إلى حل تطابقات خطية و لا يمكن الاعتماد عليها لعدم إمكانية إجرائها دائماً.

إن إيجاد باقي قسمة عدد على عدد باستخدام التطابقات أيضاً يخضع لتعقيدات و شروط تجعل منه غير نافع. فلإيجاد $z\equiv u(\mathrm{mod}\, v)$ باستخدام التطابقات يجب أن يتحقق أن $v|M$. و عندها نحلل v إلى عوامله الأولية: $v=p_1^{a_1}p_2^{a_2}...p_s^{a_s}$, بما أن $(m_i,m_j)=1;i\ne j$ فلابد أن يكون لكل $1\le i\le s$ يوجد عدد $1\le j\le r$ يحقق $p_i^{a_i}\,|\,m_j$. و من $u\equiv u_j(\mathrm{mod}\, m_j)$ نجد $z\equiv u_j(\mathrm{mod}\, p_i^{a_i})$. بحل نظام البواقي الصيني السابق (باستخدام المبرهنة (2-11) (مبرهنة البواقي الصينية)) نحصل على $z\equiv u(\mathrm{mod}\, v)$ أي على $u \bmod v$ و هو المطلوب. نجد أن عملية إيجاد باقي قسمة بوساطة التطابقات غير مجدية لحاجتها لتحليل المقسوم عليه إلى عوامله الأولية و حل نظام بواقي صيني و لا يمكن الاعتماد عليها لعدم إمكانية أجرائها دائماً.

((ملاحظة: إن حاجة عملية باقي القسمة باستخدام التطابقات إلى تحليل v إلى عوامله الأوليّة يمنع بشدّة تنفيذ هذه العملية, لأن التعقيد الزمني لعملية التحليل إلى العوامل الأولية هو $O(\sqrt{n})$ أي أنه في حال كان v عدداً كبيراً فقد يلزم سنوات لإتمام العملية على الحاسوب.))

الخاتمة:

تعرفنا في البحث على طريقة حل المعادلات الديفونتية الخطية بطريقة بسيطة لا تحتاج إلى عمليات طويلة, كما ناقشنا طرق مختلفة لحل التطابقات الخطية و نظم البواقي الصينية و أنظمة التظابقات التي تكون بمتغير واحد و قياسات مختلفة.

كما أننا في البحث تعرفنا على كيفية تطبيق خوارزمية للقيام بالعمليات الحسابية على الأعداد الكبيرة على الحاسوب بالاعتماد على التطابقات, و وجدنا أنه عن طريق الاختيار الصحيح للقياسات في هذه الخوارزمية و اختيار أفضل الطرق لتطبيق كل مرحلة منها يمكننا اختصار العمليات الحسابية التي تتضمن أعداد كبيرة بشكل كبير, كما أنه عند استخدام حواسيب تسمح بالقيام بمهمات متعددة في آن واحد فيمكن لهذه الخوارزمية تسريع عمل الحواسيب بشكل كبير جداً.

أما بالنسبة للعمليات الحسابية التي يمكن القيام بها بوساطة هذه الخوارزمية, فقد وجدنا أن عمليات الجمع و الطرح و الضرب (والرفع إلى قوّة) يمكن تأديتها بسهولة و فاعلية كبيرة باستخدام هذه الخوارزمية و حتى أن هذه الخوارزمية تختصر بعض الوقت اللازم لعملية الضرب. أما بالنسبة لعملية المقارنة و التأكد من عدم حدوث تجاوز للحد المسموح به في الخوارزمية فيمكن القيام بها إلّا أنّها أعقد من العمليات الأساسية فيعتبر البعض أنّها تُفقد الحساب بالتطابقات بعض أفضلياته, و لكن رغم ذلك فإنه يمكن تنفيذ العمليتين باستخدام التطابقات دون الحاجة إلى أي تعامل مع أعداد كبيرة و الذي قد يكون نافعاً في حال كان تقليل التعقيد الزمني للخوارزمية أقل أهمية من تقليل التعامل مع الأعداد الكبيرة فيها. أمّا بالنسبة لعمليتي القسمة و باقي القسمة فلا تعد التطابقات طريقة مجدية لتنفيذها لذلك عند الحاجة للقسمة يمكن تحويل العدد من تمثيله بالتطابقات إلى تمثيله العددي العادي ثم إجراء عملية القسمة أو باقي القسمة باستخدام الطرق التقليدية ثم إعطاء الناتج أو إعادة تحويل الناتج إلى تمثيل بالتطابقات لإجراء عمليات إضافية, و بفضل الطرق السهلة و السريعة التي تم طرحها في البحث للتحويل بين التمثيل العادي العددي للعدد و تمثيله بالتطابقات فلا تشكل القسمة عائق كبير أمام هذه الخوارزمية.

المصادر و المراجع:

1) Cormen, Thomas H. - Leiserson, Charles E. - Rivest, Ronald L. - Stein, Clifford, Introduction To Algorithms, Third edition, The MIT Press, Cambridge, Massachusetts, 2009.
(929 - 930 - 934 - 935)

2) Knuth, Donald Ervin, Art of Computer Programming: semi-Numerical Algorithms volume 2, Second edition, Addison Wesley, Reading Massachusetts, 1981.
(269 - 271 - 272 - 273 - 274 - 275 - 302 - 586 - 587 - 589)

3) Ore, Oystein, Number Theory and its History ,McGRAW-HILL, 1948.
(236 - 237 - 238 - 241 - 242 - 243 - 244 - 274 - 275)

4) Rosen, Kenneth H., Elementary Number Theory and its Applications, Addison Wesley, Reading Massachusetts, 1984.
(60 - 61 - 62 - 63 - 65 - 91 - 92 - 93 - 103 - 104 - 107 - 108 - 111 - 112 - 166 - 167 - 168 -169)

5) Silverman, Joseph H., A Friendly Introduction to Number Theory, Forth edition, Pearson, 2012.
(38 - 39 - 40 - 41 - 42)