الفصل السابع

التحليل والنظرية الأساسية في الحساب

Factorization and the Fundamental Theorem of Arithmetic

العدد الأولي هو عدد $p \geq 2$ قواسمه (الموجبة) 1 و p فقط. الأعداد غير الأولية $m \geq 2$ تسمى أعداداً مؤلَفة(composite numbers). مثلاً :

أعداد أولية : $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots\ldots$

أعداد مؤلَفة : $2, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, \ldots\ldots$

إن الأعداد الأولية تتميز بخاصية قابلية قسمتها على 1 وعلى نفسها فقط. وعليه فإنه ليس من البديهي أن الأعداد الأولية يجب أن تمتلك خصائص خاصة تشمل الأعداد التي تقسمها. الحقيقة التالية والمتعلقة بالأعداد الأولية مهمة جدا كما أنها ليست بديهية.

نظرية (٧,١)

ليكن p عدداً أولياً ، ولنفرض أن p يقسم حاصل الضرب ab. عندئذ فإن p إما أن يقسم a وإما أن يقسم b (وإما أن يقسم كليهما).[1]

---

(١) قد تقول إن هذه النتيجة واضحة بمجرد تحليل a و b إلى عواملها الأولية. على كل حال حقيقة أن العدد يمكن تحليله إلى حاصل ضرب عوامله الأولية بطريقة واحدة فقط هي نفسها حقيقة غير واضحة. سوف نناقش ذلك فيما بعد خلال هذا الفصل.

البرهان: من المعطيات فإن $p \mid ab$. إذا كانت $p \mid a$ فقد انتهى البرهان. أما إذا كان $p \nmid a$ وبما أن $p \mid \gcd(a,b)$ فإن $\gcd(p,a)$ يساوي 1 أو p. كما أن $\gcd(p,a) \mid a$ ؛ وعليه ؛ فإن $\gcd(p,a) \neq p$ ؛ وذلك لأننا فرضنا أن $p \nmid a$ ، وهذا يعني أن $\gcd(p,a) = 1$. دعنا الآن نستخدم نظرية المعادلة الخطية (الفصل السادس) مع العددين p و a . نظرية المعادلة الخطية تنص على أننا نستطيع إيجاد عددين صحيحين x و y كحل للمعادلة

$$px + ay = 1.$$

(لاحظ أننا استخدمنا حقيقة أن $\gcd(p,a) = 1$. الآن اضرب طرفي المعادلة في b لتحصل على:

$$pbx + aby = b.$$

طبعا كل من pbx و aby يقبل القسمة على p لأننا نعلم أن $p \mid ab$. إذاً نستنتج أن $p \mid (pbx + aby)$. وهذا يعني أن $p \mid b$ ، وبذلك نكون قد أنهينا البرهان.

النتيجة السابقة تنص على أنه إذا قسم عدد أولي حاصل الضرب ab فإن هذا العدد الأولي يجب أن يقسم احد العاملين a أو b. لاحظ أن هذه الخاصية خاصة فقط بالأعداد الأولية وليست صحيحة للأعداد المؤلَفة، مثلا 6 تقسم حاصل الضرب $14 \cdot 15$ ولكن 6 لا تقسم كلا من 15 و 14.

ليس من الصعب تعميم النتيجة السابقة على حواصل ضرب تتكون من أكثر من عاملين.

نظرية (٢, ٧) (خاصية قابلية القسمة الأولية)

إذا كان p عدداً أولياً ، ويقسم حاصل الضرب:

$$a_1 a_2 \ldots\ldots a_r .$$

فإن p *يقسم على الأقل أحد العوامل* $a_1, a_2, \ldots\ldots, a_r$.

البرهان: إذا كان p يقسم a_1 فقد انتهى البرهان، بمعنى آخر نكون قد طبقنا النتيجة السابقة على العاملين $a = a_1$ و $b = a_2 a_3 \ldots\ldots a_r$. نعلم أن $p \mid ab$ ، لذلك إذا كان $p \nmid a$ ؛ فالنتيجة السابقة تنص على أن p يجب أن يقسم b . نعرف الآن أن p يقسم $a_2 \ldots\ldots a_r$. إذا كان p يقسم a_2 فقد انتهى البرهان، أما إذا كانت $p \nmid a_2$ فنطبق النتيجة السابقة على حاصل الضرب $a_2(a_3 \ldots\ldots a_r)$ لنستنتج أن p يقسم $a_3 \ldots\ldots a_r$. وهكذا إذا تابعنا بهذه الطريقة لا بد من إيجاد a_i يقبل القسمة على p .

فيما تبقى من هذا الفصل سوف نستخدم خاصية قابلية القسمة الأولية لإثبات أن كل عدد صحيح موجب يمكن أن يكتب كحاصل ضرب أعداد أولية بطريقة واحدة فقط. إن هذه الحقيقة الهامة مألوفة جدا لمعظم القُراء والذين سوف يتساءلون لماذا تتطلب هذه الحقيقة برهاناً؟ لذلك وقبل أن نعطي البرهان، أريد أن أقنعك أن التحليل الوحيد للعوامل الأولية بعيد كل البعد عن كونه واضحا. لهذا الغرض. فإنني أدعوك إلى أن تترك هذه الحقيقة المألوفة وراء ظهرك وأن تدخل في:

عالم العدد الزوجي

المعروف بالمنطقة E "$\mathrm{E}-Zone$"

تخيل نفسك في عالم غير معروف فيه إلا الأعداد الزوجية، بمعنى أن الأعداد الوحيدة الموجودة في هذا العالم هي

$$E = \{\ldots, -8, -6, -4. -2, 0, 2, 4, 6, 8, \ldots\}$$

لاحظ أنه في المجموعة E تستطيع جمع، طرح، وضرب الأعداد الزوجية كما هو معتاد. لأن جمع، طرح، وضرب الأعداد الزوجية هو عدد زوجي أيضا. كذلك نستطيع التحدث عن القسمة في هذا العالم. نقول إن m (يقسم- E) n إذا وجد عدد k بحيث $n = mk$. ولكن تذكر أننا موجودون في المجموعة E، وعليه فإن كلمة عدد تعني عدداً زوجيًّا. على سبيل المثال، 6 (يقسم- E) 12، لأن $12 = 6 \cdot 2$، لكن 6 (لا يقسم- E) 18 لأنه لا يوجد عدد (زوجي) k يحقق $18 = 6 \cdot k$. كذلك نستطيع التحدث عن الأعداد الأولية في هذا العالم، فنقول إن العدد (الزوجي) p هو (أولي- E) إذا كان لا يقبل القسمة على أي عدد (زوجي).

(لاحظ أنه في المنطقة E العدد لا يقبل القسمة على نفسه!). على سبيل المثال الأعداد التالية تعتبر أعدادا أولية في المنطقة E

$$2, 6, 10, 14, 18, 22, 26, 30$$

لنراجع الآن النتيجة 7.1 والتي أثبتناها للأعداد العادية. لقد بينا أنه إذا كان عدد أولي p يقسم حاصل الضرب ab ؛ فإن p يقسم a أو يقسم b. لننتقل الآن إلى المنطقة E ولنأخذ العدد الأولي- E 6 و العددين $a = 10\ ,\ b = 18$. العدد 6 يقسم- E $ab = 180$، لأن $180 = 6 \cdot 30$، لكن 6 لا يقسم- E 10 ولا يقسم- E 18. وعليه ؛ فإن نتيجتنا "الواضحة" ليست صحيحة في المجموعة E !. كما أن هناك "حقائق واضحة بحد ذاتها" ليست صحيحة في المنطقة E. منها الحقيقة التي تقول إن أي عدد يمكن كتابته على شكل حاصل ضرب أعداد أولية بطريقة وحيدة (طبعا، إعادة ترتيب العوامل لا يعتبر طريقة جديدة). ليس من الصعب إثبات أنه حتى في المنطقة E يمكن كتابة أي عدد (زوجي) على شكل حاصل ضرب أعداد أولية- E. لكن انظر إلى التحليل التالي:

$$180 = 6 \cdot 30 = 10 \cdot 18$$

لاحظ أن الأعداد $6,10,18,30$ جميعها أعداد أولية- E ، وهذا يعني أن 180 يمكن كتابته بطريقتين مختلفتين، وفي الواقع، توجد حتى طريقة ثالثة لكتابة 180 كحاصل ضرب أعداد أولية- E وهي:

$$180 = 2 \cdot 90$$

لنترك الآن المجموعة E ونعود إلى عالمنا المعتاد، حيث تعيش الأعداد الزوجية والفردية في سلام ووئام، ولكننا نأمل أن يكون اقتحامنا للمنطقة E قد أقنع القارئ بأن بعض الحقائق التي تبدو بديهية قد تتطلب برهانا مكتوبا بدقة وحذر.

نهاية حدود المنطقة E – مرحبا بعودتك إلى أرض الوطن

الجميع يعرف أن أي عدد صحيح موجب يمكن تحليله إلى حاصل ضرب أعداد أولية بطريقة واحدة فقط. لكن زيارتنا للمنطقة E أعطتنا عدداً من الدلائل المقنعة على أن هذه العبارة تحتاج إلى برهان دقيق وحذر.[1]

نظرية (٣, ٧) (النظرية الأساسية في الحساب)

أي عدد صحيح $n \geq 2$ يمكن تحليله إلى حاصل ضرب أعداد أولية:

$$n = p_1 p_2 \ldots\ldots p_r$$

بطريقة واحدة فقط.

قبل أن نقدم برهان النظرية الأساسية في الحساب، سوف نعرض بعض الملاحظات. أولاً: إذا كان n نفسه عدداً أوليًّا، فما علينا إلا أن نكتب $n = n$ ونعتبر هذا حاصل ضرب مكون من عدد واحد. ثانياً: عندما نكتب $n = p_1 p_2 \ldots\ldots p_r$ ،

(١) المبادئ الرياضية المعروفة جدا والتي توصف دائما "بالحقائق" تفحص بشكل دقيق من قبل الرياضيين.

فهذا لا يعني بالضرورة أن $p_1, p_2, \ldots\ldots, p_r$ هي أعداد أولية مختلفة. على سبيل المثال، $300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5$. ثالثاً: عندما نقول إن n يمكن كتابته على شكل حاصل ضرب أعداد أولية بطريقة وحيدة فإننا نعتبر أن إعادة ترتيب عوامل n ليس تحليلاً جديداً. فعلى سبيل المثال، التحليلات $12 = 2 \cdot 2 \cdot 3$, $12 = 2 \cdot 3 \cdot 2$, $12 = 3 \cdot 2 \cdot 2$ تعتبر جميعها تحليلاً واحداً.

البرهان: إن النظرية الأساسية في الحساب تتألف من ادعاءين.

الادعاء 1. العدد n يمكن تحليله إلى حاصل ضرب أعداد أولية بطريقة ما.

الادعاء 2. هذا التحليل وحيد (بغض النظر عن ترتيب العوامل).

نبدأ بالادعاء الأول.سنقوم بإعطاء البرهان بالاستقراء. وهذا يعني أننا سنتحقق من صحة الادعاء عندما $n = 2$ ، ومن ثم عندما $n = 3$ ، وبعد ذلك عندما $n = 4$ وهكذا. بما أن $2 = 2$ و $3 = 3$ و $4 = 2^2$ ، فهذا يعني أن جميع هذه الأرقام يمكن كتابتها على شكل حاصل ضرب أعداد أولية. بذلك نكون قد تحققنا من صحة الادعاء الأول عندما $n = 2, 3, 4$. الآن افرض أننا تحققنا من صحة الإدعاء الأول عندما $n = N$. وهذا يعني أن أي عدد $n \leq N$ يمكن كتابته على شكل حاصل ضرب أعداد أولية. الآن سنتحقق من أن الإدعاء الأول صحيح عندما $n = N + 1$.

إن هناك احتمالين. الاحتمال الأول أن يكون $N + 1$ عدداً أوليًّا، وهذا يحقق صحة الادعاء الأول. الاحتمال الثاني أن يكون $N + 1$ عدداً مؤلَفاً، وهذا يعني أن $N + 1 = n_1 n_2$ ، حيث $2 \leq n_1, n_2 \leq N$. و بما أن الادعاء الأول صحيح بالنسبة للعددين n_1, n_2 كون كل منهما أقل من أو يساوي N ، فهذا يعني أن كلا من n_1 و n_2 يمكن كتابته على شكل حاصل ضرب أعداد أولية، أي أن:

$$n_1 = p_1 p_2 \ldots\ldots p_r \quad , \quad n_2 = q_1 q_2 \ldots\ldots q_s$$

وعليه ؛ فإن :

$$N+1 = n_1 n_2 = p_1 p_2 \ldots\ldots p_r q_1 q_2 \ldots\ldots q_s$$

إذا $N+1$ يمكن كتابته على شكل حاصل ضرب أعداد أولية ، وبذلك نكون قد تحققنا من صحة الادعاء 1 عندما $n = N+1$. وبذلك نكون قد أنهينا الخطوات الثلاث المعمول بها في البرهان الاستقرائي ، وبهذا نكون قد برهنا أن الادعاء 1 صحيح لأي عدد صحيح.

لننتقل الآن للتحقق من صحة الادعاء الثاني. يمكن هنا أيضا استخدام البرهان الاستقرائي للتحقق من صحة هذا الادعاء ولكننا سنسلك طريقا مباشرا. افرض أننا نستطيع تحليل n إلى حاصل ضرب عوامل أولية بطريقتين مختلفتين ، ولنقل :

$$n = p_1 p_2 p_3 p_4 \ldots\ldots p_r = q_1 q_2 q_3 q_4 \ldots\ldots q_s$$

المطلوب الآن التحقق من أن كلا التحليلين هما نفس التحليل. بما أن $p_1 \mid n$ ، إذاً $p_1 \mid q_1 q_2 \ldots\ldots q_s$. من نظرية خاصية قابلية القسمة الأولية فإن p_1 يجب أن يقسم (على الأقل) أحد العوامل $q_1, q_2, \ldots\ldots, q_s$. وبدون نقص في التعميم يمكننا فرض أن $p_1 \mid q_1$. ولكن q_1 هو عدد أولي ، وبالتالي فإن قواسمه الوحيدة هي 1 و q_1 ، وعليه ؛ فإن $p_1 = q_1$.

بإمكاننا الآن حذف p_1 (والذي هو نفسه q_1) من طرفي المعادلة لنحصل على :

$$p_2 p_3 p_4 \ldots\ldots p_r = q_2 q_3 q_4 \ldots\ldots q_s$$

باستخدام نفس هذا الإجراء يمكننا التوصل إلى أن $p_2 \mid q_2$. بحذف p_2 (والذي هو نفسه q_2) من طرفي المعادلة لنحصل على :

$$p_3p_4.....p_r = q_3q_4.....q_s$$

نستمر بنفس الأسلوب حتى تنتهي عوامل الطرف الأيمن أو الطرف الأيسر. إذا انتهت عوامل الطرف الأيمن فهذا يعني أن الطرف الأيمن من المعادلة يساوي 1 ؛ وعليه لا يمكن أن يكون هناك أي عوامل في الطرف الأيسر. نفس الوضع إذا انتهت عوامل الطرف الأيسر. بعبارة أخرى، فإن عدد العوامل في كلا الطرفين يجب أن يكون نفسه. بذلك نكون قد بينا أنه إذا كان :

$$n = p_1p_2p_3p_4.....p_r = q_1q_2q_3q_4.....q_s$$

حيث جميع $p_i's$ و $q_i's$ أعداد أولية، فإن $r = s$ ، وبالإمكان إعادة ترتيب $q_i's$ بحيث :

$$p_1 = q_1 \ , \ p_2 = q_2 \ , \ p_3 = q_3 \ , ... , \ p_r = q_s$$

وهذا ينهي برهان أن أي عدد يمكن كتابته على شكل حاصل ضرب أعداد أولية بطريقة وحيدة.

إن النظرية الأساسية في الحساب نصت على أن أي عدد صحيح $n \geq 2$ يمكن كتابته بصورة وحيدة على شكل حاصل ضرب أعداد أولية. لنفرض أن لدينا عدداً صحيحاً ما n. كمسألة تطبيقية، كيف يمكن كتابة هذا العدد على شكل حاصل ضرب أعداد أولية؟ إذا كان n عدداً صغيراً (على سبيل المثال، $n = 180$) فيمكننا تحليله بالمعاينة :

$$180 = 2 \cdot 90 = 2 \cdot 2 \cdot 45 = 2 \cdot 2 \cdot 3 \cdot 15 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$$

أما إذا كان n عدداً كبيراً (على سبيل المثال، $n = 9105293$) فسنجد صعوبة في تحليله إلى عوامله الأولية. إحدى الطرق هي محاولة قسمة n على أحد

الأعداد الأولية $2,3,5,7,11,\ldots\ldots$ حتى نجد قاسماً. بالنسبة للعدد $n = 9105293$ ، سوف نجد بعد شيء من العمل أن أصغر عدد أولي يقسم n هو 37. نحلل:

$$9105293 = 37 \cdot 246089$$

نستمر بفحص الأعداد الأولية $37,41,43,\ldots\ldots$ حتى نجد عدداً أوليًّا يقسم 246089. سنجد أن $43 \mid 246089$ ؛ لأن $246089 = 43 \cdot 5723$. وهكذا حتى نحلل $5723 = 59 \cdot 97$ ، لنجد أن 59 و 97 كليهما أولي. هذا يعطينا التحليل الأولي الكامل:

$$9105293 = 37 \cdot 43 \cdot 59 \cdot 97$$

إذا كان n نفسه ليس عددا أوليا، فإنه يوجد عدد أولي $p \leq \sqrt{n}$ يقسم n. للتحقق من صحة ذلك، نلاحظ أنه إذا كان p أصغر عدد أولي يقسم n فإن $n = pm$ ، حيث $m \geq p$ ؛ لذلك $n = pm \geq p^2$ ، وبأخذ الجذر التربيعي للطرفين ينتج أن $\sqrt{n} \geq p$. إن هذا يقودنا إلى الطريقة السهلة التالية والتي تساعدنا على كتابة أي عدد على شكل حاصل ضرب أعداد أولية:

> لكتابة n على شكل حاصل ضرب أعداد أولية، حاول أن تقسمه على كل عدد (أو فقط على كل عدد أولي) $2,3,\ldots\ldots$ أقل من أو يساوي $\sqrt{n}$. إذا لم تجد أي عدد يقسم n فإن n نفسه عدد أولي. عدا ذلك، فإن أول قاسم وجدته هو عدد أولي p. اكتب $n = pm$ وكرر العملية السابقة مع m.

هذا الإجراء، ورغم كونه غير فعّال، فإنه يعمل بشكل جيد على الحاسوب للأعداد الكبيرة بدرجة معقولة، ولنقل أعداداً تضم 10 خانات. ولكن كيف سيكون الوضع لو أخذنا عددا مثل $n = 10^{128} + 1$. إذا أردنا التحقق فيما إذا كان n عدداً أوليًّا أم لا ؛ فسنقوم بتجربة $\sqrt{n} \approx 10^{64}$ قاسم محتمل، وهذا غير معقول أبدا. فلو كان باستطاعتنا تجربة $1000,000,000$ قاسم محتمل في الثانية الواحدة، فستستغرق هذه العملية $3 \cdot 10^{43}$ سنة! هذا يقودنا إلى طرح السؤالين التاليين (لا توجد لهما إجابة حتى الآن):

السؤال رقم (١). كيف يمكننا التحقق فيما إذا كان عدد معطى أوليًّا أم مؤلَفاً؟

السؤال رقم (٢). إذا كان n عدداً مؤلَفاً، فكيف يمكن كتابته على شكل حاصل ضرب أعداد أولية؟

على الرغم من أنه يبدو أن هذين السؤالين هما نفس السؤال، إلا أن السؤال 1 أسهل على الإجابة بكثير من السؤال 2. سوف نرى لاحقا كيف نكتب أعدادا كبيرة نعرف مسبقا أنها مؤلَفة، حتى على الرغم من أننا لن نكون قادرين على كتابة أي من عواملها. بنفس الأسلوب، سنكون قادرين على إيجاد عددين أوليين كبيرين p, q، بحيث إذا أردنا أن نرسل لشخص ما قيمة حاصل الضرب $n = pq$، فإنه لن يكون قادرا على تحليل n ليحصل على العددين p, q. هذه الحقيقة المثيرة للفضول، وهي أنه يمكن بغاية السهولة ضرب عددين ولكن في غاية الصعوبة تحليل حاصل الضرب، تقع في قلب تطبيقات نظرية الأعداد لإنشاء شيفرات سرية. سوف نناقش هذه الشيفرات في الفصل الثامن عشر.

تمارين

(٧,١) ليكن $\gcd\big(a,b\big)=1$ ، وافرض أن a يقسم حاصل الضرب bc. بين أن a يجب أن يقسم c.

(٧,٢) ليكن $\gcd\big(a,b\big)=1$ ، وافرض أن a يقسم c و b يقسم c. بين أن حاصل الضرب ab يجب أن يقسم c.

(٧,٣) أعط برهاناً استقرائيًّا لكل صيغة من الصيغ التالية:

[لاحظ أن (a) هي الصيغة التي برهنّاها في الفصل الأول باستخدام الهندسة وأن (c) هي أول n حد للمتسلسلة الهندسية

$$(a)\quad 1+2+3+\cdots+n=\frac{n\big(n+1\big)}{2}$$

$$(b)\quad 1^2+2^2+3^2+\cdots+n^2=\frac{n\big(n+1\big)\big(2n+1\big)}{6}$$

$$(c)\quad 1+a+a^2+a^3+\cdots+a^n=\frac{1-a^{n+1}}{1-a}\quad,\quad \big(a\neq 1\big)$$

$$(d)\quad \frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{\big(n-1\big)n}=\frac{n-1}{n}$$

(٧,٤) هذا التمرين يطلب منك مواصلة البحث في المنطقة (E-zone). تذكر خلال حلك لهذا التمرين أن الأعداد الفردية غير موجودة!

(a) صف جميع الأعداد الأولية في المنطقة E.

(b) بيّن أن كل عدد زوجي يمكن تحليله كحاصل ضرب عددين أوليين في المنطقة E.

[مساعدة: قلّد البرهان المستخدم على الأعداد العادية].

(c) رأينا أن العدد 180 يحلل إلى حاصل ضرب أعداد أولية في المنطقة E بثلاث طرق مختلفة. أوجد أصغر عدد يحلل إلى حاصل ضرب أعداد أولية في المنطقة E

بطريقتين مختلفتين. هل العدد 180 هو أصغر عدد يمكن تحليله إلى حاصل ضرب أعداد أوليه في المنطقة E بثلاث طرق مختلفة؟ أوجد أصغر عدد يحلل بأربع طرق مختلفة.

(d) العدد 12 له تحليل وحيد كحاصل ضرب عددين أوليين في المنطقة E: $12 = 2 \cdot 6$ (طبعاً نحن نعتبر أن $2 \cdot 6$, $6 \cdot 2$ هما نفس التحليل). صِف جميع الأعداد الزوجية التي لها تحليل وحيد كحاصل ضرب أعداد أولية في المنطقة E.

(٧,٥) أهلاً بك في عالم M (M-World) ، حيث إن الأعداد الموجودة في هذا العالم هي فقط الأعداد الصحيحة الموجبة التي تُعطي الباقي 1 عند قسمتها على 4. بكلمات أخرى، الأعداد M الموجودة هي فقط

$$\{1,5,9,13,17,21,\ldots\}$$

(وصف آخر لهذه الأعداد هو أنها الأعداد التي على الشكل $4t+1$ حيث $t = 0,1,2,\ldots$). في العالم M ، لا نستطيع جمع الأعداد لكن نستطيع ضربها؛ لأنه إذا كان العددان a, b كلاهما يُعطي الباقي 1 عند قسمتها على 4 فإن حاصل ضربهما ab يُعطي الباقي 1 عند قسمته على 4. (لماذا؟).

نقول إن m يقسم-M n إذا كان $n = mk$ ، حيث k عدد-M. ونقول إن n عدد أولي-M إذا كانت قواسمه-M هي فقط $1, n$. (طبعاً، لا نعتبر العدد 1 أولي-M).

(a) أوجد أول ستة أعداد أولية -M.

(b) أوجد عدد -M n يُحلل كحاصل ضرب أعداد أولية -M بطريقتين مختلفتين.

(٧,٦) يطلب منك هذا التمرين كتابة برامج لتحليل عدد صحيح موجب n إلى عوامله الأولية. (إذا كان $n = 0$ ، تأكد من أن البرنامج يُعطي رسالة خطأ بدلاً من أن يستمر في العمل في حلقة لا نهائية!). من الطرق المناسبة لعرض تحليل n هو إظهاره على شكل مصفوفة $2 \times r$. لذلك إذا كان :

$$n = p_1^{k_1}\, p_2^{k_2} \ldots\, p_r^{k_r}$$

عندئذ يظهر التحليل على الشكل :

$$\begin{pmatrix} p_1 & p_2 & \cdots & p_r \\ k_1 & k_2 & \cdots & k_r \end{pmatrix}$$

(a) اكتب برنامجاً لتحليل n يتعامل مع كل عامل محتمل $d = 2,3,4,5,6,\ldots$ (هذه طريقة غير فعَّالة أبداً، ولكنها تقوم بدور الإحماء قبل حل التمرين).

(b) عَدّل برنامجك ليقوم بتخزين أول 100 (أو أكثر) عدد أولي ومن ثم يقوم أولاً بإزالة هذه الأعداد الأولية من n قبل أن يبدأ بالبحث عن عوامل أولية أكبر. يمكن تسريع برنامجك عندما تجعله يحاول مع قيم أكبر d كعوامل محتملة إذا كنت لا تهتم بفحص قيم d الزوجية ، أو التي تقبل القسمة على 3 أو 5. يمكنك أيضاً أن تزيد من فاعلية البرنامج باعتمادك على حقيقة أن العدد m يكون أولياً إذا لم يقبل القسمة على أي عدد بين 2 , $\sqrt{m}$.

استخدم برنامجك لإيجاد التحليل الكامل لجميع الأعداد بين 1,000,000 و 1,000,030.

(c) اكتب برنامجاً صغيراً يطبع تحليل n بشكل جميل. من الأفضل أن تظهر الأسس على شكل أسس لكن إذا لم يكن ذلك بالإمكان ، عندئذ اطبع التحليل (ولنقُل) $n = 75460 = 2^2 \cdot 5 \cdot 7^3 \cdot 11$ على الشكل :

$$2\ \hat{}\ 2 * 5 * 7\ \hat{}\ 3 * 11$$

(لتجعل الناتج أسهل على القراءة ، لا تقوم بطباعة الأسس التي تساوي ١).