

الحمد لله رب العالمين والصلاة والسلام على سيدنا محمد وعلى آله وأصحابه أجمعين
والسلام عليكم ورحمة الله وبركاته ..

أما بعد ..

من المواضيع الرياضية الشائقة والتي شغلت علماء الرياضيات طويلاً ولا تزال تشغلهم .. الأعداد الأولية ..

منذ اقليدس وحتى اليوم .. لا يزال مجهولاً إن كان هناك علاقة تربط الأعداد الأولية ببعضها ..

كان هناك الكثير من المحاولات الجيدة لتطوير خوارزميات اختبار أولية العدد Test Primality ..

كما تم تطوير عدد من الخوارزميات لإيجاد جميع الأعداد الأولية الأصغر من عدد ما ..

في هذه المقالة القصيرة .. سنتحدث ببعض التفصيل إحدى خوارزميات اختبار أولية الأعداد .. والتي لا تزال من أفضل الخوارزميات في وقتنا الحاضر .. والتي تعتمد Fermat little theory

هذا المقال موجه لمحبي الرياضيات البحتة .. دون النظر في تطبيقات الأعداد الأولية ..

العدد الأولي هو عدد أكبر من الواحد .. لا يقبل القسمة إلا على نفسه وعلى الواحد .. مثل ٥ و ٧ و ٢٣ و ٩٧ ..

هل للأعداد الأولية نهاية ؟

الجواب هو لا .. والبرهان :

لو افترضنا أن للأعداد الأولية نهاية .. وأوجدنا جداء جميع الأعداد الأولية في العالم .. سينتج لنا رقم x فلو قمنا بجمع ١ إلى هذا العدد سينتج عدد لا يقبل القسمة على أي من الأعداد الأولية التي شكلت x وبالتالي سيكون أولياً بالنسبة لها ...

الأولية النسبية :

نقول عن عدد x أنه أولي بالنسبة لعدد آخر y إذا كان القاسم المشترك الأكبر لهما هو ١ ..

أي أنه إذا كان $\gcd(x,y)=1$ فإن x أولي بالنسبة ل y

وهنا يمكننا تعريف تابع أولر Euler Totient Function .. والذي يعبر عن عدد الأعداد الأصغر من x والأولية بالنسبة له ...

فنقول مثلاً ... $\varphi(10) = 4$ أي أن عدد الأعداد الأصغر من ١٠ والأولية بالنسبة له هو ٤ ..

وهي ١ و ٣ و ٧ و ٩ ...

وكذلك فإن .. $\varphi(11) = 10$..

إن أي عدد أولي p سيكون قيمة تابع أولر له هو $p-1$ لأن جميع الأعداد الأصغر من p أولية بالنسبة له ..

أوجد أولر قانوناً .. بالاعتماد على هذا التابع :

$$a^{\varphi(m)} \% m = 1$$

حيث % هي عملية باقي القسمة .. a هو اي عدد موجب أصغر من m وأولي بالنسبة له ..

بالاعتماد على هذا القانون .. وكما رأينا أن $\varphi(P) = P - 1$ حيث P هو عدد أولي ...

فإن :

$$a^{p-1} \% p = 1$$

أوجد العالم Fermat نظرية تقول :

إذا كان لدينا عدد ما m وكان $a^{m-1} \% m \neq 1$ فإن m هو عدد مركب ...

أما عكس النظرية فهو غير مطلق الصحة .. أي أنه إذا كان $a^{m-1} \% m = 1$ فإن m ليس أولياً بالمطلق .. ولكن يمكننا أن نقول أنه شبه أولي .. أو أنه أولي باحتمال كبير يصل إلى ٩٩%

هذا التوجه الجديد في اختبار الأعداد الأولية والذي يعتمد مبدأ الاحتمالات في إيجاد هذه الأعداد أثبت جدواه ..

بحيث أن عدد الأرقام المركبة التي يفشل الاختبار عندها والأصغر من 10^{17} يبلغ تقريباً ٥٠٠ ألف .. فقط ..

في الحالة البسيطة فإننا سنختبر الرقم P من أجل قيمة عشوائية a (حيث $\gcd(a,p)=1$)

وكلما اختبرنا p على عدد أكبر من الأرقام .. a .. ونجح الاختبار .. فهذا يزيد احتمالية كون p أولياً ..

ولكن أين تكمن صعوبة الاختبار السابق ؟

علاوة على كونه لا يعطي نتيجة مؤكدة .. فإن الحصول على نتيجة الاختبار (حتى بالنسبة لأرقام صغيرة) لا يعد أمراً سهلاً ...

فلو أردنا اختبار الرقم ٥١١ هل هو أولي أم لا .. واخترنا الرقم ٢ مثلاً ليمثل العدد a

فإن العملية التي يتوجب علينا القيام بها هي : $2^{510} \% 511$

وبالطريقة التقليدية .. فإن 2^{510} يساوي

٣٣٥١٩٥١٩٨٢٤٨٥٦٤٩٢٧٤٨٩٣٥٠٦٢٤٩٥٥١٤٦١٥٣١٨٦٩٨٤١٤٥٥١٤٨٠٩٨٣٤٤٤٣٠٨٩٠٣٦٠٩٣٠
٤٤١٠٠٧٥١٨٣٨٦٧٤٤٢٠٠٤٦٨٥٧٤٥٤١٧٢٥٨٥٦٩٢٢٥٠٧٩٦٤٥٤٦٦٢١٥١٢٧١٣٤٣٨٤٧٠٧٠٢٩٨٦٦
٤٢٤٨٦٦٠٨٤١٢٢٥١٥٢١٠٢٤

ثم عند أخذ باقي قسمته على ٥١١ سيكون الناتج : ٦٤ وبالتالي فإن ٥١١ مركب ..

هل يستحق الاختبار كل هذا العناء ؟

لو اختبرنا باقي قسمة الرقم ٥١١ على ٢ ثم ٣ ثم ٥ ثم ٧ .. لتبين أنه من مضاعفات الرقم ٧ ..

و بحديث أكثر احترافية .. فإن التعقيد الزمني لخوارزمية الاختبار الثانية ..

فإنها تستغرق عددا من العمليات هو $\sqrt{n}$ بالنسبة لاختبار الرقم n ..

ولكن علاقة Fermat والتي تقتضي التعامل مع BigInt كما أن الوصول إلى a^n بالطرق التقليدية .. يتطلب n عملية

وبالطرق السريعة $\ln(n)$ ولكن لا ننسى الحجم الكبير من الذاكرة الذي ستستهلكه عملية مثل هذه .. مما سيجعلنا
نفضل خوارزميتنا التقليدية على هذه النظرية ... ولكن .

إن أي رقم X لابد أن يكون باقي قسمته على Y أصغر من Y وبالتالي فإننا لا نحتاج إلى إيجاد الرقم كاملاً ثم أخذ باقي قسمته !

وبناء على ذلك قام الرياضيون بتبسيط العمليات التي تحوي mod (باقي قسمة) في نهايتها ..

حتى أصبح modular arithmetic من أحد فروع الرياضيات ..

وهناك علاقة هامة نتجينا من التعامل مع هذه الأعداد الضخمة .. وهي :

$$(a \cdot b) \% m \equiv (a \cdot (b \% m)) \% m$$

فلو كان لدينا مثلاً : $2^8 \% 9$ مثلاً ...

$$2^8 = 4^2 \cdot 4^2$$
 فإن ..

وبما أن $4^2 = 16$ وبالتالي $16 \% 9 = 7$..

$$2^8 \% 9 = (7 \cdot 7) \% 9 = 49 \% 9 = 4$$
 فإن

وبالمثل $9^{12} \% 8$

$$9 \% 8 = 1 \text{ لأن } 1^{12} \% 8$$
 هي نفسها

وعلى هذا المنوال ... يوجد خوارزميات تحسب لنا هذا الـ Modular Exponentiation أي العدد المرفوع لقوة ونريد باقي قسمته على عدد آخر ..

وتعقيد خوارزميته تقريباً $\ln(n)$ دون استخدام BigInt وأي حجرات ذاكرة إضافية ..

(التابع pow في لغة python يمكنه أخذ ٣ وسطاء .. الأول هو الأساس والثاني هو الأس والثالث هو mod أي الرقم الذي نريد أخذ باقي قسمة الجواب عليه ..)

ويبقى السؤال .. كم مرة سنكرر الاختبار للتأكد من أولية العدد ؟

من التجربة العملية يتبين لنا أن ٥ مرات تكرار هو عدد كاف جداً .. للتأكد من أولية العدد ..

أي أننا سنختار ٥ أعداد عشوائية وأولية بالنسبة للرقم الذي نختبره ونطبق القانون .. وننتظر النتيجة ..

وبذلك تصبح خوارزميتنا ببساطة :

١- لدينا رقم m نريد اختبار أوليته

٢- نختار رقماً a موجبا أصغر من m وأولي بالنسبة له (الأفضل هو ان نختار رقماً أولياً معروفاً مثل ٢ و ٣ ..)

٣- نوجد $a^{m-1} \% m$ فإذا كان الناتج لا يساوي الواحد فلا بد أن m مركب .. وينتهي الاختبار

٤- إذا كان الناتج يساوي الواحد .. فإن m هو شبه أولي .. ويمكننا تكرار الاختبار من أجل a مختلف لمزيد من التأكد

كانت هذه نظرية Fermat ببساطة .. وكما رأينا تحتاج إلى استخدام `mod Exp` لتجنب التعامل مع `BigInt`

وبذلك .. نكون قد وصلنا إلى ختام هذه المقالة القصيرة .. أرجو أن يكون فيها الفائدة ...

مصطفى 36a2