

## ความพิศวงของตัวเลข จำนวนเฉพาะตอนที่ 1

นำเสนอเมื่อ : 4 ก.ค. 2551

เคยคิดไหมครับว่า เวลาเราเรียนเลขเรื่องตัวประกอบนั้น เราจะเรียนเรื่องจำนวนเฉพาะไปทำไม  
เคยคิดไหมครับว่า

ทำไมเราสามารถส่งเบอร์บัตรเครดิตไปทางอินเทอร์เน็ตได้ ในขณะที่ยังมีชาวบ้านใช้อินเทอร์เน็ตอยู่ด้วย  
หรือว่าโทรศัพท์ที่สัญญาณมันรู้ได้ไงว่าเราต้องการคุยกับคนนี้

**คำตอบอยู่ที่จำนวนเฉพาะนี่แหละครับ**

จำนวนเฉพาะหรือภาษาอังกฤษที่เรียกกันว่า prime number นั้น

เป็นที่ศึกษากันอย่างแพร่หลายของนักคณิตศาสตร์มากมายมาเป็นร้อยปีแล้ว

**แล้วจำนวนเฉพาะคืออะไร**

จำนวนเฉพาะก็คือจำนวนนับที่มีแค่สองตัวเท่านั้นที่หารมันลงตัว คือ 1 และตัวมันเอง

แล้วอย่างนี้หนึ่งถือเป็นจำนวนเฉพาะหรือไม่

คำตอบคือไม่ครับ เพราะ (ตอบแบบกำปั้นทุบดิน) ก็มันมีจำนวนนับแค่ตัวเดียวไง แต่จริงๆแล้วที่เขาไม่นับว่า 1

เป็นจำนวนเฉพาะนั้นมีหลายสาเหตุด้วยกัน แต่สาเหตุหลักๆก็คือ 1 นั้นเป็นเลขพิเศษ (เป็นเอกลักษณ์การคูณ)

รวมไปถึงในการแยกตัวประกอบนั้น

เราต้องการแยกตัวประกอบของจำนวนใดๆ ให้เป็นรูปของการคูณของตัวเลขที่น้อยกว่าจำนวนนั้น เช่น  $2=1 \times 2$  แต่ 1 นั้นมันไม่มีนี่ครับ (แต่ตอนนี้นักคณิตศาสตร์บางคนก็บอกว่า 1 นั้นเป็นจำนวนเฉพาะเหมือนกัน)

**แล้วจำนวนเฉพาะนั้นมีมาตั้งแต่เมื่อไร**

ว่ากันว่ามีมาตั้งแต่สมัยอียิปต์โบราณแล้วครับ ดังนั้นมีมาเป็นพันปีแล้วครับ แต่คนแรกที่พูดถึงจำนวนเฉพาะ ก็คือ

ยูคลิด (Euclid) นักปรัชญาชาวกรีกโบราณ (ซึ่งก็เป็นพันปีอีกเหมือนกัน) ยูคลิดนั้นเขียนหนังสือที่ชื่อว่า The Elements หนังสือเรื่อง The Elements นั้นมีถึง 13 เล่มด้วยกัน

และเป็นหนังสือพิมพ์มากที่สุดอันดับสองทั่วโลกเลยนะครับ

จะเป็นรองก็เป็นเพียงแต่ไบเบิลเท่านั้น

**จำนวนเฉพาะที่ใหญ่ที่สุดและเล็กที่สุด**

จำนวนเฉพาะที่เล็กที่สุดนั้นง่ายใช่ไหมครับ เพราะว่ามันคือ 2 แต่ถ้านับ 1

ว่าเป็นจำนวนเฉพาะตามที่นักคณิตศาสตร์บางคนบอกว่าใช่ ก็หนึ่งแหละครับ

แต่ใหญ่ที่สุดหละ คำตอบคือมันยังหาไม่ได้ครับ

ก็เพราะในหนังสือเรื่อง The Elements ของยูคลิดนะสิครับ ทำพิช

เพราะยูคลิดพิสูจน์ให้เห็นว่า ถ้าเราเจอจำนวนเฉพาะใหญ่มากตัวหนึ่ง แต่หาไปอีกห้อยเราก็จะเจอที่ใหญ่กว่านั้นอีก

เท่าที่คนหาได้ในตอนนี้ จำนวนเฉพาะที่ใหญ่ที่สุดนั้นคือ  $2^{32,582,657} - 1$  หาเจอเมื่อ 11 เดือนกันยายน ปี 2006

นี่เองครับโดย Great Internet Mersenne Prime Search

ในนี้มีคำอยู่คำหนึ่งที่ชื่อว่า Mersenne Prime, Mersenne Prime นั้นเป็นวิธีการหาจำนวนเฉพาะวิธีหนึ่งครับ

จากสมการ

$$M_n = 2^n - 1$$

$M_n$  นั้นจะเป็นจำนวนเฉพาะ ถ้า  $n$  เป็นจำนวนเฉพาะครับ แต่จริงๆแล้ววิธีนี้

ก็ไม่ใช่ว่าจะหาจำนวนเฉพาะได้ทุกตัวหรอกนะครับ เพราะว่า ลองแทน  $n=11$ ,

$$M_{11} = 2^{11} - 1 = 2047$$

แต่ 2047 มันหารได้ด้วย 23 กับ 89 ลงตัว

**วิธีการตรวจดูว่าตัวเลขไหนที่เป็นจำนวนเฉพาะ**

แล้วมีวิธีไหนที่เราจะรู้ว่าตัวเลขนั้น เช่น  $N$  เป็นจำนวนเฉพาะ

วิธีแรกก็คือ ก็ลองหารดูสิครับหารตั้งแต่ 1 ถึงตัวมันเลย ก็คือ  $N$  วิธีนี้ดูเหนื่อยใช่ไหมครับ งั้นก็เอาใหม่

ก็ลองหารด้วย 1 ถึง  $\sqrt{n}$  ก็ลดลงได้เยอะ แต่ก็ยังช้าอยู่ดีใช่ไหมครับ

งั้นคราวนี้มาลองวิธีฉลาดๆดูบ้าง

วิธีฉลาดๆเช่น Fermat's little theorem

Fermat นั้นเป็นนักคณิตศาสตร์ชาวฝรั่งเศสครับ แต่จะบอกว่าเป็นนักคณิตศาสตร์ก็ไม่เชิง เพราะว่า Fermat นั้นหาकिनทางกฎหมายครับ แต่คิดเลขเป็นงานอดิเรกเท่านั้น

Fermat's little theorem บอกว่า

ถ้า  $a$  เป็นจำนวนนับใดๆ และ  $p$  เป็นจำนวนเฉพาะ

$a^{p-1}$  หารด้วย  $p$  ชะ แล้วถ้าได้เศษ 1 แล้วละก็  $p$  ก็เป็นจำนวนเฉพาะ

แต่แหม มันก็ดูยากนะครับ เพราะเราต้องหาว่า  $a$  ตัวไหน ที่จะทำให้ขอความข้างบนเป็นจริง ดูแล้วก็เหนื่อยมาตุ้ออีกวิธีที่ฉลาดๆกันดูบ้างครับ (แต่วิธีนี้นั้นไม่ได้แน่นอนเสมอ)

เห็นคำว่า Mersenne prime ที่ตอนต้นไหมครับ  $M_n = 2^n - 1$

ถ้าเราเอา  $a$  ก็เอา  $M_n$  มาหารด้วย  $n$  ชะ ถ้าเหลือเศษหนึ่ง ก็อุปบิก่อน แต่ถ้าไม่ใช่หนึ่ง  $M_n$  ก็ตัวประกอบแน่นอนครับ

แต่ถ้าเป็นหนึ่ง ก็ฮ่าๆๆๆๆๆๆๆๆๆ  $M_n$  อาจจะเป็นจำนวนเฉพาะก็ได้ หรืออาจจะไม่ใช่ก็ได้

(เพียงแต่ว่ามีแนวโน้มที่จะเป็นจำนวนเฉพาะมากกว่าเท่านั้นเอง)

ลักษณะของจำนวนเฉพาะนั้นมีมากมายครับ เช่น

Wilson's theorem ที่บอกว่า จำนวนเต็ม  $p > 1$  เป็นจำนวนเฉพาะ ก็ต่อเมื่อ  $(p-1)! + 1$  หารด้วย  $p$  ลงตัว

Bertrand's postulate ที่บอกว่า ถ้า  $n$  เป็นจำนวนเต็มบวกที่มากกว่า 1 แล้ว จะมีจำนวนเฉพาะหนึ่งตัว  $p$  ที่

$n < p < 2n$

ทั้งหมดเป็นเรื่องเกี่ยวกับจำนวนเฉพาะที่นักคณิตศาสตร์นั้นศึกษากันมาเป็นพันๆปีเลยนะครับเนี่ย

ตอนหน้าเราจะมาดูกันว่า แล้วจำนวนเฉพาะนั้นสามารถนำมาประยุกต์ใช้กับอะไรกันไดบ้าง

ตอนนี้เอาแค่นี้ก่อนนะครับ ตอนหน้า เรามาดูกันว่า

แล้วทำไมเราถึงส่งเบอร์บัตรเครดิตออกไปชื่อของออนไลน์กันได้ครับ

อ้างอิง

du Sautoy, M. *The Music of the Primes: Searching to Solve the Greatest Mystery in Mathematics*.

HarperCollins 2004 (มีเว็บไซต์ที่ <http://www.musicofthepimes.com/>)

Derbyshire, J. *Prime Obsession*, John Henry Press. Washington DC. 2003

Devlin, K. *The language of mathematics*, W. H. Freeman and Company, NY. 1998

[http://en.wikipedia.org/wiki/Prime\\_number#There\\_are\\_infinitely\\_many\\_prime\\_numbers](http://en.wikipedia.org/wiki/Prime_number#There_are_infinitely_many_prime_numbers)

ที่มา <http://gotoknow.org/blog/mathbeauty/93000>