Mathematics, English for Sek I and Sek II

Mathematica - The Principles of Math

16. The Uniqueness of Prime Numbers

08:59 minutes

00:22 (caption)
prime numbers
numbers larger than 1 which have no divisors other than 1 and itself

00:36 Try to imagine what numbers can go into these numbers with no remainder.

00:41 Besides 1 and the number itself, can they be divided by any other number evenly? No. We can't come up with any other divisors. These numbers are prime numbers.

00:54 In addition to 2, 3, and 5, there's 7, 11, 13, 17 …

00:59 These are all prime numbers. But there are prime numbers even larger than these.

01:09 Natural numbers that have other divisors besides 1 and themselves are not prime numbers. Instead, these are called composite numbers.

01:20 (caption)
composite numbers
numbers that are not prime numbers because they have divisors besides 1 and themselves

01:23 Natural numbers larger than 1 are either prime numbers or composite numbers. Composite numbers can be expressed by multiplying prime numbers together.

01:34 Let's show how this is done by multiplying prime numbers to get the composite numbers 16 and 45.

01:42 We can get to 16 by multiplying the prime number 2.

01:46 We can get to 45 by multiplying the prime numbers 5 and 3.

01:50 What this means is that composite numbers are made by multiplying prime numbers together.

01:56 You can think of prime numbers as building blocks or atoms, which are impossible to break down further.

02:08 This process of expressing composite numbers as the product of prime numbers is called integer factorization.

02:20 (caption) What is the largest prime number?

02:22 Actually, trying to find out the largest prime number is the wrong way to go. Just as natural numbers can reach infinite, prime numbers

also have no upper limit. The fact that prime numbers are limitless was proven in the ninth chapter of Euclid's famous mathematical text, Elements of Geometry.

02:47 While supposing that prime numbers had an upper limit, Euclid defined the largest as P.

02:50 (caption)
Prime numbers are limited.
The largest prime number = P.

02:58 (caption) Set S consists of the limited set of all prime numbers.

02:56 Let's call the set of all prime numbers S. Now multiply all the numbers in Set S and add 1. If that result is N, then N is naturally larger than P.

03:18 But if N is a composite number, it must be divided with those prime numbers in Set S. Any prime numbers will leave a remainder of 1.

03:19 (caption) composite number

03:27 In that case, N is not a composite number.

03:31 If it's not a composite number, then N must be a prime number. That contradicts the first supposition that states that prime numbers have an upper limit and P is the largest prime number.

03:34 (caption)
prime number
the largest prime number

03:46 (caption)Set S consists of the limited set of all prime numbers.

03:53 The entire set of prime numbers is infinite, without limit.

03:52 This all means that prime numbers keep growing infinitely.

03:59 The fact that prime numbers are limitless and infinite was proven.
But this leads to a question: How can we find prime numbers?

04:02 (caption) another prime number

04:08 Since prime numbers don't have a regular pattern, it's not an easy task to find the next larger one.

04:16 (caption) no rules

04:22 (caption) Marin Mersenne (1588 – 1648)
French theologian, philosopher, and mathematician

04:21 In the seventeenth century, French theologian Marin Mersenne discovered that taking one from a power of 2, or 2n – 1 (READ: "two to

the nth power minus 1), could be a prime number. Let's take a look at some examples.

04:37 But not every number calculated from 2n – 1 (READ: "two to the nth power minus 1) is a prime number.

04:34 (caption)
prime numbers
composite numbers

04:45 But people called these numbers "Mersenne number" or "Mersenne Prime" if it's a prime number that can be expressed as 2n – 1 (READ: "two to the nth power, minus 1). And they have been trying to find larger and larger Mersenne numbers.

04:53 (caption) Mersenne number or Mersenne prime

05:05 (caption) As of 2010, who has found the largest Mersenne prime number?

05:09 The 47th Mersenne prime number

05:13 Do you see that huge exponent?

05:18 This Mersenne prime number has a value with over 12.8 million places. It's a number so huge we can't read it or even imagine it.

05:20 (caption) a number with 12,837,064 places

05:30 Now do you get a sense for how limitless and infinite prime numbers are?

05:49 Let's look for prime numbers around us.

05:41 This is a cicada, a common insect found in summer.

05:45 It's only for a month that they come to the surface and use a loud sound to find a mate. They actually spend many years as larvae living underground.

05:57 Depending on the species of cicada, they may spend five, seven, thirteen, or even seventeen years underground. These are all prime numbers. Do you know why? This is to reduce the possibility of meeting their natural enemies.

06:11 Prime numbers have only 1 and themselves as divisors, which means a greater gap between potential enemy encounters.

06:30 This is a mystery found in nature where they are preserving their species by elongating their short existence to its maximum.

06:44 (caption) electronic certificate (or identification) key

In 1977, three scientists from MIT, a prestigious American university, created this code by using integer factorization. The method was

named after the first letters of their last names.

06:47 (caption)
R. Rivest, A. Shamir, L. Adleman
RSA encryption system

06:49 This password system has a public key which can be known by anyone, and a private key which only the individual knows. If you know the public key but not the private key, you cannot crack the code.

06:55 (caption)
public key
private key

07:03 The public key works by using a number made by multiplying two prime numbers p and q together.
And the private key works by using the two prime numbers which were multiplied to make that number.

07:03 (caption)
product of two prime numbers = prime number 1 * prime number 2
$N = p \times q$
public, private

07:15 That means when the public key is factorized, you can find the private key. So wouldn't it be easy to crack the code?

07:25 But what if those two private prime numbers were unexpectedly large numbers?

07:29 The number you're looking at right now is a prime number from the RSA laboratory.
How long would it take to factorize this huge number?

07:48 (caption)
a prime number with 617 places
How long would it take to factorize this?
It's so long that it's impossible to estimate!

07:56 (caption)
Time required to factorize a prime number with more than 200 places
▸ a computer making one million calculations per second: 100 years
▸ a human being doing the calculation: more than the history of the Universe

08:05 No, I think we should just give up and forget about it.
Ultimately, the key to cracking the RSA code is integer factorization.

08:15 (caption)
prime numbers
numbers larger than 1 which have no divisors other than 1 and itself