

Terence Tao: Structure and Randomness in the Prime Numbers, UCLA 3:00 – 8:20

<http://www.youtube.com/watch?v=PtsrAw1LR3E>

- a) What is a prime number?
- b) What does the Fundamental Theorem of Arithmetic state?
- c) What do you know about Euclid?

Decide whether the following statements are true or false.

- 1) Dr. Tao's subject of research is a prime number.
- 2) This topic is 200 years old.
- 3) There is still much work to be done concerning prime numbers.
- 4) Natural numbers are similar to elements in physics.
- 5) One of the first theorems about primes goes back to the ancient Greece.
- 6) There is only one way of expressing 50 as a multiplication of primes.
- 7) The product of primes cannot be rearranged.
- 8) 1 cannot be split into smaller numbers, therefore the Fundamental Theorem of Arithmetic is not true.
- 9) Euclid believed that the number of primes is infinite.
- 10) There are not so many prime numbers as atomic elements.
- 11) Reduction ad absurdum means a proof by confirmation.
- 12) You prove something, then pretend it is false, and then show that it can happen, which indirectly shows it is false.

Fill in the missing words in the proof:

Euclid's proof is the classic example of reduction ad absurdum.

- Suppose, for sake of contradiction, that there were only finitely many prime numbers p_1, p_2, \dots, p_n (e.g. suppose 2,3,5 were ????????? primes).
- Multiply all the primes together and add (or ??????) 1: $P = p_1 p_2 \dots p_n + 1$. (e.g. $P = 2 \times 3 \times 5 + 1 = 31$.)
- Then P is a ????????? number larger than 1 but P is not ????????? by any of the prime numbers.
- This contradicts the fundamental theorem of arithmetic. Hence there are infinitely many primes.

Primal Surge

Ivars Peterson

1) *What is a prime number? Give examples.*

I. Read the first part and fill in the missing words.

What do the following numbers have in common?

3, 7, 31, 127, 8191, 131071, 524287, 2147483647, 2305843009213693951,
618970019642690137449562111, 162259276829213363391578010288127,
170141183460469231731687303715884105727.

Each one is a 1) _____, evenly divisible only by 2) _____ and 1.
Each one can also be written in the form a 3) _____ of 2, less 1: $2^p - 1$,
where p is itself a 4) _____ number.

II. Read the second part of the text, then answer Qs.

In 1644, French monk and mathematician Marin Mersenne (1588–1648) stated that numbers of the form $2^p - 1$ are primes only when p has the following and no other values:

$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, \text{ and } 257.$

Mersenne himself didn't actually test his assertion for any values greater than $p = 19$. In fact, it wasn't until 1750 that Leonhard Euler (1707–1783) verified that $2^{31} - 1$ (or 2147483647) is a prime.

In 1811, in his book *An Elementary Investigation of the Theory of Numbers*, Peter Barlow (1776–1862) stated that this prime number "is the greatest that will ever be discovered, for, as they are merely curious without being useful, it is not likely that any person will attempt to find one beyond it."

It turns out that Mersenne and Barlow were both wrong. In 1903, mathematician Frank Nelson Cole (1861–1926) demonstrated that $2^{67} - 1$ is not a prime but the product of 193707721 and 761838257287. At the same time, the discovery of ever-larger Mersenne primes, as these numbers came to be called, steadily progressed to larger and larger values.

Last month saw the discovery of the 42nd known Mersenne prime, the largest prime yet identified. The new Mersenne prime is $2^{25,964,951} - 1$. When written out in full, it runs to a whopping 7,816,230 decimal digits. The previous record holder, discovered less than a year ago, consisted of 7,235,733 decimal digits.

The new champion was found by Martin Nowak, a German eye surgeon and participant in the Great Internet Mersenne Prime Search (GIMPS). He used one of his business computers and software provided by George Woltman and Scott Kurowski to find the enormous prime.

Nowak's computer is one of more than 250,000 computers worldwide engaged in testing Mersenne numbers for primality. GIMPS volunteers are responsible for checking Mersenne numbers within specified ranges of exponents, whenever their computers would otherwise be idle.

In the 10 years since George Woltman started the GIMPS effort, participants have discovered eight Mersenne primes. Nowak, who's from Michelfeld, Germany, got involved about 6 years ago after he read about GIMPS in his local newspaper. He now has 24 computers taking part in the search.

GIMPS volunteers haven't yet tested every Mersenne number smaller than the current champion, so another Mersenne prime may yet lurk among the untested numbers. Only exponents less than 15,130,000 have all been tested at least once.

There's still time to join the search. Maybe your computer will ring up the next champion!

1) What was it that Mersenne did not test? _____

2) What was verified by Euler in 1750? _____

3) Why did Barlow think that greater primes would not be discovered? _____

4) What did Frank Nelson Cole demonstrate? _____

5) What progressed at the same time? _____

6) What was discovered less than a year ago? _____

7) Why did Martin Nowak use one of his business computers and a special software? _____

8) When do GIMPS volunteers check Mersenne numbers? _____

9) When did Nowak get involved? _____

10) Which exponents have been tested at least once? _____

11) Would you be interested in participating in such a project? Why Y/N.

Puzzle



Eight cards are marked with numbers, and the cards are placed in two columns (as shown above). The numbers in the left and right columns add up to different totals.

Rearrange the cards, using as few moves as possible, so that each of the two columns gives the same total.

Adapted from Science News Online, March 5, 2005, Vol. 167, No.10