Math 117 Fall 2014 Lecture 2 (Sept. 4, 2014)

- Number systems:
  - $\mathbb{N} = \{1, 2, 3, ...\}$: Natural numbers;
  - $\mathbb{Z} = \{... - 2, -1, 0, 1, 2, ...\}$: Integers;
  - $\mathbb{Q}$: Rational numbers;
  - $\mathbb{R}$: Real numbers;
  - $\mathbb{C}$: Complex numbers;
  - And many more.
- Relations between number systems: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

  "$A \subset B$" for two sets A, B (a set is a collection of objects) means every member of A (that is every object in the collection A) is also a member of B. For example

$$\{1, 2, 3\} \subset \{1, 2, 3, 4\} \subset \{1, 2, 3, 4, \text{Obama}\}. \tag{1}$$

- Natural numbers are in some sense different – more "natural" than other number systems.

  > Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.
  >
  > — Leopold Kronecker 1839 - 1914.

  - By the end of the 19th century, the whole analysis has been successfully "built" upon arithmetics.[1]
  - It is also possible to further "built" arithmetics on set theory. For example, John von Neumann defined the natural numbers successively as

$$0 := \varnothing, \quad 1 := \{\varnothing\}, \quad 2 := \{\varnothing, \{\varnothing\}\}, \quad 3 := \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, ... \tag{2}$$

    Another interesting development in this direction is J. H. Conway (inventor of "Game of Life")'s theory of surreal numbers, for which a lively introduction is the book *Surreal Numbers: How to ex-students turned on to pure mathematics and found total happiness*, by Donald E. Knuth.[2]
  - However the effort of using set theory as foundation of the whole analysis (or whole mathematics) finally failed, one reason being the "Incompleteness Theorem" proved by Kurt Gödel in the 1930s.
- From now on we accept $\mathbb{N}$ as it is and will not make any effort to define it.
- Prime and composite numbers:
  - A prime number is a natural number greater than 1 that has no positive divisors other than 1 and itself.

    Example 1. Prove that 7 is prime.

1. The book *Differential and Integral Calculus* by Edmund Landau, written in 1928(?), summarized this success. You may want to take a look to see what things look like.

2. Author of the multi-volume classic *The Art of Computer Programming*.

Proof. First observe that any number bigger than 7 cannot be its divisor. Therefore the claim is proved as soon as we have shown that the only divisors of 7 in $1, 2, ..., 7$ are 1 and 7. We check

$$1|\,7, 2\not|\,7, 3\not|\,7, 4\not|\,7, 5\not|\,7, 6\not|\,7, 7|\,7. \tag{3}$$

Thus the proof ends. □

NOTATION. *Here $a|\,b$ means a is a divisor of b while $a\not|\,b$ means a is not a divisor of b.*

- A composite number is a natural number greater than 1 that is not prime.

  Note. Equivalently, a composite number is a natural number great than 1 and has at least one divisor other than 1 and itself.

  Example 2. Prove that 6 is composite.

  Proof. We have $2|\,6$. Since $2 \neq 1, 2 \neq 6$, by definition 6 is composite. □

- We state but not prove the following fact:

  Any composite number has at least one prime divisor.

  In other words, if n is composite, then there is a prime p such that $p|\,n$.

THEOREM 3. *There are infinitely many primes.*

Note. There are two possible strategies to prove this:

1. Assuming that the primes are finite leads to contradiction; If our arguments are all solid, then the cause of the contradiction must be the assumption, which then must be false. This is proof by contradiction.
2. No matter how many primes we have, we can always find one more. This is proof by construction (we "construct" one more prime).

Proof. (BY CONTRADICTION) Assume the contrary. There we can list the finitely many primes as $p_1, p_2, ..., p_n$. Now consider the number $q := p_1 \cdots p_n + 1$ ($p_1 \cdots p_n$ is shorthand for $p_1 \times p_2 \times \cdots \times p_n$, the product of all these n primes). Since $q > p_1, p_2, ..., p_n$, it cannot be in the list and therefore by our assumption cannot be prime. Therefore it is composite. But then there is a prime number dividing q. We show that this is not possible and thus reaching contradiction.

This prime number cannot be p_1. Since $q \div p_1 = p_2 \cdots p_n ....1$ (with remainder 1, just like $7 \div 3 = 2....1$). Similarly it cannot be p_2 or p_3 or p_4 or .... or p_n. But we have assumed there are no other primes than $p_1, p_2, ..., p_n$. Contradiction. □

Proof. (BY CONSTRUCTION) This is essentially the same proof. Except that we take any prime divisor of q as the "one more" prime. □

Exercise 1. Fill in the details for the proof by construction.

- People have been looking for formulas that generate primes without success.

  Example 4. Pierre de Fermat (1601 - 1665), the "greatest amateur mathematician ever" proposed the formula $f(n) := 2^{2^n} + 1$ and checked that $f(1)$, ..., $f(4)$ are all primes. However Leonhard Euler showed in 1732 that $f(5) = 641 \times 6700417$.

Exercise 2. Prove that $f(n) := n^2 - n + 41$ is also not a "prime generating formula". (Hint:[3])

- One of the most important result is the following "Prime Number Theorem", proved by Hadamard and de la Vallee-Poussin (independently) in 1896:

  THEOREM 5. *Let $P(N)$ denote the number of primes in $1, 2, ..., N$, then*

  $$\lim_{N\to\infty} \frac{P(N)}{N} = \ln N. \tag{4}$$

  Here ln *is the natural logarithm (base e).*

  The proof is a result of applying calculus to number theory.

- The two major open problems regarding primes are
  - Twin Prime Conjecture: There are infinitely many pairs of "twin primes". Here a pair of "twin prime" is a pair of natural numbers (p, q) such that $q - p = 2$.
    - Major progress has been made last year on this problem. Yitang Zhang proved last year that there are infinitely many pairs of primes with difference less than seventy million ($< 7 \times 10^7$). See the video *Twin prime conjecture* from Numberphile: http://youtu.be/vkMXdShDdtY.

    Exercise 3. Given that there are infinitely many pairs of prime numbers with difference $< 7 \times 10^7$. Prove that there is a natural number $d < 7 \times 10^7$ such that there are infinitely many pairs of prime numbers with difference exactly d.

  - Goldbach's Conjecture: Every even number greater or equal to 4 is the sum of two prime numbers.
    - The best result up to now is the one obtained by Jingrun Chen in 1960s: Every even number greater or equal to 4 is the sum of two numbers, one of which is prime, the other the product of two primes.
    - Goldbach's Weak Conjecture – Every odd number greater or equal to 7 is the sum of three prime numbers – was proved last year by Harold Helfgott.

    Exercise 4. Explain why Goldbach's weak conjecture is indeed weaker than Goldbach's conjecture. (Claim A is "weaker" than claim B if the following hold: if B is true than A is true; But if A is true B is not necessarily true.)

  The proofs are all applications of calculus to number theory.

- Fundamental Theorem of Arithmetic. Also called "unique factorization theorem".

  THEOREM 6. *Every natural number greater than 1 either is prime or is a product of primes. Furthermore, this factorization is unique: the order of the primes is arbitrary, but the primes themselves are not.*

  Example 7. The only factorization of 12 is $2 \times 2 \times 3$. The only change one can make is changing the order of $2, 2, 3$.

  COROLLARY 8. *Every natural number n greater than 1 has a unique representation as*

  $$n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k} \tag{5}$$

3. There is no need to calculate $f(1), f(2), ...$ one by one. Notice $f(n) = (n-1)\, n + 41$.

where $p_1, ..., p_k$ are primes and $a_1, ..., a_k$ are natural numbers.

Example 9. $12 = 2^2 \cdot 3$.

NOTATION. *Since $\times$ and x are hard to tell apart, often $\cdot$ or simple a small space is used to denote multiplication. Thus $2^2 \cdot 3$ means $2^2 \times 3$.*

Proof. (OF THE FUNDAMENTAL THEOREM) We will prove only the second half, the uniqueness part, as the first half requires some set up which totally belongs to a number theory course.

Assume the contrary. Thus there are natural numbers enjoying two different factorizations into primes. Let m be the smallest such number.

Exercise 5. Why is this possible? Why can we pick such a "smallest" number?

Then

$$m = p_1 \cdots p_r = q_1 \cdots q_s \tag{6}$$

where $p_1, ..., p_r; q_1, ...q_s$ are primes. Since the order is arbitrary, we can assume $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_r$; $q_1 \leqslant q_2 \leqslant \cdots \leqslant q_s$.

Exercise 6. Why is this possible?

We claim that $p_1 \neq q_1$. Assume otherwise. Then we define $m' = p_2 \cdots p_r$ and there holds

$$m' = p_2 \cdots p_r = q_2 \cdots q_s \tag{7}$$

contradicting the fact that m is the smallest such number.

Therefore either $p_1 > q_1$ or $p_1 < q_1$. We prove the $p_1 < q_1$ case and leave the other one as exercise.

Define

$$m'' := m - p_1\, q_2 \cdots q_s. \tag{8}$$

Then we have

$$m'' = p_1 \left(p_2 \cdots p_r - q_2 \cdots q_s\right) \tag{9}$$

and also

$$m'' = (q_1 - p_1)\, q_2 \cdots q_s. \tag{10}$$

Since $m'' < m$, it has only one prime factorization. Thus one of the following must be true:

$$p_1 | \,(q_1 - p_1), \quad p_1 = q_2, \quad p_1 = q_3, \quad \ldots \quad p_1 = q_s. \tag{11}$$

If $p_1 | \,(q_1 - p_1)$ then $p_1 | \, q_1$ which contradicts the fact that q_1 is prime. None of the other $s-1$ equalities could hold because $p_1 < q_1 \leqslant q_2 \leqslant \cdots \leqslant q_s$.

Thus we have reached contradiction and the proof ends. □

Exercise 7. Prove the case $q_1 < p_1$.

One important consequence of the Fundamental Theorem of Arithmetic is the following:

> Let a, b be natural numbers and let p be prime. If $p | \,(a\, b)$ then either $p | \, a$ or $p | \, b$.

Exercise 8. Let a, b, c be natural numbers. Prove or disprove: If $c | \,(a\, b)$ then either $c | \, a$ or $c | \, b$.

- If you have some number theory background, you may want to read this: Scott Aaronson *The Prime Facts: From Euclid to AKS*. http://www.scottaaronson.com/writings/prime.pdf.

- Another interesting article from Scott Aaronson is *Who Can Name the Bigger Number?* about whether it is possible to name the biggest natural number. The answer may surprise you. http://www.scottaaronson.com/writings/bignumbers.html.