

8 Number Theory Concluded

Let's review the progression of the results so far:

- We defined the notion of *prime* and *composite* numbers, and set out to understand how numbers are constructed in terms of primes (ultimate goal: the Fundamental Theorem of Arithmetic)
- Introduced the basic notion of divisibility, introduced the notation $|$, and enumerated a list of properties for the operation $|$.
- Started proving increasingly “deep” results about primes and divisibility. The proof of a given result often relied on ones that came before. Often of the results were useful for concrete operations.

Some of the results:

1. Every positive integer has at least one prime divisor.
2. Every positive number N has at least one prime divisor $\leq \sqrt{N}$. (This one is useful in practice, for testing primality.)
3. There are infinitely many primes. (Intro-

duced the notion of *proof by contradiction*.)

4. Division algorithm: *Suppose a and d are positive integers; then there are unique $k, r \in \mathbb{N}$ such that $a = kd + r$ and $0 \leq r < d$.*
5. Defined LCM and GCD. Showed how the division algorithm could be turned into a procedure for finding the GCD of two numbers (*Euclidean Algorithm*)
6. For any $M, N \in \mathbb{Z}^+$, there is $r, s \in \mathbb{Z}$ such that $rM + sN = \text{GCD}(M, N)$. (This followed by tracing the Euclidean algorithm backwards.)
7. Used this fact to prove: If p prime and $p|(mn)$ then $p|m$ or $p|n$
8. Did some applications (clock arithmetic, irrationality of $\sqrt{2}$).

General observations:

Only the proof of the Fundamental Theorem of Arithmetic is left.

The progression from *definition* (which is meant to make an intuition rigorous) to the final result had no holes or guesses; everything was proved rigorously. This process of *Deductive Proof* is what sets mathematical reasoning apart from most other forms of reasoning.

While the final goal (FTA) has no obvious applications, along the way it spun off a useful algorithm (Euclidean Algorithm), and results like the one in line (6) which are at the heart of RSA cryptography.

This kind of mathematical proof would be a lot easier if it could be reduced to a mechanical procedure; this is part of what we'll be talking about during the next topic of the course.

9 Logical connectives (negation, disjunction, conjunction, implication)

The following are examples of statements that have (or might have) a definite *truth value*, that is, be either true or false:

1. $5 + 7 = 12$
2. $5 + 7 = 14$
3. My dog is black.
4. The King of France is bald.
5. $x = 5$
6. $A > B$

Note that the truth value of the last two can change, depending on the values of x , or of A and B . Nevertheless, they are assertions that *might* have a truth value, and *will* do if x , A , B take on values.

Similarly, the truth value of (4) is a matter of some debate; it depends on whether you interpret the sentence as asserting the existence of a King of France.

For comparison, here are some sentences with no notion of a truth value:

1. Ouch.
2. Let x be an integer.
3. Smell the ocean!

A statement that has (or could have) a truth value is called a *proposition*; the terms ‘proposition’, ‘assertion’, and ‘statement’ are generally used interchangeably.

A *logical connective* is an operation we apply to one or more proposition to get a new proposition.

We will look at the following logical connectives: implication (\implies), negation (\sim), disjunction (\vee), conjunction (\wedge or $\&$).

9.1 Implication

Suppose A and B are propositions. The following are all different ways of saying the same thing:

If A then B
 A implies B
 A , therefore B
 A is sufficient for B
For B it is sufficient that A
 B is necessary for A
 B follows from A
 $A \implies B$

Intuitively, if $A \implies B$ and A is true then this ‘forces’ B to be true as well. However, if A is false then it doesn’t force anything about B . We therefore say that $A \implies B$ is true unless A is true and B is false.

Examples (determine the truth value if possible)

1. If $1 + 1 = 2$ then $1 + 1 = 3$.
2. If $1 + 1 = 3$ then $1 + 1 = 2$.
3. Sunlight is necessary for photosynthesis. (Equivalently, “if there is photosynthesis, then there is sunlight.”)
4. For N to be composite it is sufficient that $\exists p > 1 (p|N)$. (Equivalently, “ $\exists p > 1 (p|N)$ is sufficient for N to be composite;” or, “if $\exists p > 1 (p|N)$ then N is composite.”)