CISC-102
Winter 2017
Week 7

We will see two different, yet similar, proofs that there are infinitely many prime numbers. One proof would surely suffice. However, seeing two different ways of proving the same result is instructive, as it demonstrates that there are often many ways in which to make a mathematical argument. I prefer the first proof, but that's simply a matter of taste. Which proof do you prefer?.

Theorem: There exists a prime greater than n for all positive integers n. (We could also say that there are infinitely many primes.)

Proof: (Given any value n we construct a larger value that is either prime or has a prime factor greater than n.)

Consider
$y = n!$ and $x = n! + 1$.

Let p be a prime divisor of x, such that $p \leq n$. This implies that p is also a divisor of y, because n! is the product of all natural numbers from 1 to n. So we have

$p \mid x$ and $p \mid y$.

According to one of the divisibility theorems we have

$p \mid x - y$.

But $x - y = 1$ and the only divisor of 1 is -1, or 1, both not prime. So there are no prime divisors of x less than n. And since every integer is either prime or a product of primes, we either have $x > n$ is prime, or there exists a prime p, $p > n$ in the prime factorization of x. □

Theorem: There is no largest prime.

Proof: (Proof by contradiction.)

Suppose there is a largest prime. So we can write down all of the finitely many primes as: $\{p_1, p_2, \ldots, p_\omega\}$, such that p_ω is largest.

Now let n = $p_1 \times p_2 \times \cdots \times p_\omega + 1$.

Observe that n must be larger than p_ω. Therefore n is composite and is a product of primes. Let p_k denote a prime factor of n. Thus we have

$p_k \mid n$

And since $p_k \in \{p_1, p_2, \ldots, p_\omega\}$ we also have

$p_k \mid (n-1)$

We know that $p_k \mid n$ and $p_k \mid (n-1)$ implies that $p_k \mid n - (n-1)$ or $p_k \mid 1$. But no positive integer divides 1 except 1, and 1 is not prime, so $p_k \mid 1$ is impossible, and raises a mathematical contradiction. This implies that our assumption that p_ω is the largest prime is false, and so we conclude that there is no largest prime. □

Least Common Multiple

Let a = 250, and b = 575. We can construct a prime factorization of a and b.

Prime factorization:
$250 = (2)(5^3)$
$575 = (5^2)(23)$

We can inspect the prime factorization of a and b to obtain a greatest common divisor.

Observe that 5^2 is the greatest number that divides both a and b, that is the gcd(a,b). Using the prime factorizations of a and b is much less efficient than Euclid's algorithm. Nevertheless, the prime factorization is useful for obtaining other properties of the greatest common divisor.

Least Common Multiple

Given two non-zero integers a,b we can have many values that are positive common multiples of both a & b. By the well ordering principle we know that amongst all of those multiples there is one that is smallest, and this is known as the least common multiple of a and b. We can define a function lcm(a,b) that returns this value.

Example: Suppose a = 12, and b = 24,
so we have lcm(a,b) = 24.
In general if a | b then lcm(a,b) = |b|.
At this point it is worth mentioning that if a | b then gcd(a,b) = |a|, and that lcm(a,b) × gcd(a,b) = |ab|.

Example: Suppose a = 13, and b = 24, we have lcm(a,b) = (13)(24).
In general if a and b are relatively prime, that is, if gcd(a,b) = 1 then lcm(a,b) = |ab|

So when gcd(a,b) = 1, we can observe that lcm(a,b) × gcd(a,b) = |ab|.

Let a = 250, and b = 575. We can construct a prime factorization of a and b

Prime factorization
$250 = (2)(5^3)$
$575 = (5^2)(23)$

We can inspect the prime factorization of a and b to obtain the least common multiple.

$250 \times 575 = (2)(5^3) \times (5^2)(23) = (5^2) \times (2)(5^3)(23)$

And since gcd(a,b) = 5^2 we can conclude that
lcm(a,b) = (2) (5^3) (23).

So in this case we also have:

$\text{lcm}(a,b) \times \gcd(a,b) = |ab|$

Let $p_1, p_2, \ldots, p_k$ denote all of the prime factors of both a and b ordered from smallest to largest. In our example the list of prime factors would be 2,5,23.

Let a_i denote the exponent of prime factor p_i, for i, $1 \leq i \leq k$, in a prime factorization of a.

In our example $a_1 = 1$, $a_2 = 3$, $a_3 = 0$.
Similarly we define b_i for i, $1 \leq i \leq k$.
In our example $b_1 = 0$, $b_2 = 2$, $b_3 = 1$.
Again referring to our example we have:

$\gcd(a,b) = 2^{\min(1,0)} \times 5^{\min(3,2)} \times 23^{\min(0,1)}$

and,

$\text{lcm}(a,b) = 2^{\max(1,0)} \times 5^{\max(3,2)} \times 23^{\max(0,1)}$.

In general using p_i, a_i, and b_i as defined above we can express this formula as

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} \times p_2^{\min(a_2,b_2)} \times \cdots \times p_k^{\min(a_k,b_k)}$$

and

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} \times p_2^{\max(a_2,b_2)} \times \cdots \times p_k^{\max(a_k,b_k)}$$

One more example

$630 = (2) (3^2) (5) (7)$
$84 = (2^2) (3) (7)$

By inspection we can see that
$\gcd(630,84) = (2) (3) (7) = 42$
And $\text{lcm}(630,84) = (2^2) (3^2) (5) (7) = 1260$
Again we have

$$\begin{aligned} 630 \times 84 &= (2) (3^2) (5) (7) \times (2^2) (3) (7) \\ &= (2) (3) (7) \times (2^2) (3^2) (5) (7) \\ &= \gcd(630,84) \times \text{lcm}(630,84) \end{aligned}$$

These ideas lead to the following theorem that is given without proof.

Theorem: Let a,b be non-zero integers, then

$$\gcd(a,b) \times \text{lcm}(a,b) = |ab|.$$

Factoring vs. GCD

Factoring an integer N into its prime factors will use roughly $\sqrt{N}$ operations.

Computing gcd(N,m) with Euclid's algorithm for $N > m \geq 0$ will use roughly $\log_2 N$ operations.

N	$\log_2 N$	$\sqrt{N}$
1024	10	32
1099511627776	40	1,048,576
1×10^{301}	1000	3.27×10^{150}

The efficiency of Euclid's gcd algorithm is essential for implementing current public key crypto systems that are commonly used for e-commerce applications.

With a "key" decoding an encrypted message using Euclid's algorithm takes about 1000 operations. Without a "key" breaking an encrypted messaged uses approximately 3.27×10^{150} operations. This amounts to a small fraction of a second for decoding and many millions of years for breaking the encrypted message.

Congruence Relations

Let a and b be integers. We say that a is congruent to b modulo m written as:

$a \equiv b \pmod{m}$

and defined as follows:

$a \equiv b \pmod{m}$ if and only if $m \mid (a-b)$.

Arithmetic with congruences

Suppose we have $a \equiv b \pmod m$ and $c \equiv d \pmod m$.

Then

$a + c \equiv (b + d) \pmod m$,

$a - c \equiv (b - d) \pmod m$, and

$ac \equiv (bd) \pmod m$.

Examples

$5 \equiv 2 \pmod 3$ and $10 \equiv 1 \pmod 3$

$5 + 10 \equiv (2 + 1) \pmod 3$, that is, $15 \equiv 3 \pmod 3$

$5 - 10 \equiv (2 - 1) \pmod 3$, that is, $-5 \equiv 1 \pmod 3$

(Note: By the Division Algorithm Theorem we have $-5 = (-2)(3) + 1$)

$(5)(10) \equiv (2)(1) \pmod 3$, that is, $50 \equiv 2 \pmod 3$

These properties require a proof.

Suppose we have $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.
Then $a + c \equiv (b + d) \pmod{m}$.

Proof: (We need to show that $a + c \equiv (b + d) \pmod{m}$.)

If $a \equiv b \pmod{m}$ then $m \mid (a-b)$.
And if $c \equiv d \pmod{m}$ we have $m \mid (c-d)$.

This in turn implies that

$$m \mid ((a - b) + (c - d))$$

which can be written as

$$m \mid ((a + c) - (b + d)).$$

So we can conclude that $a + c \equiv (b + d) \pmod{m}$. □

Suppose we have $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.
Then $ac \equiv (bd) \pmod{m}$. □

Proof: (We need to show that $m \mid (ac - bd)$.)

If $a \equiv b \pmod{m}$ then $m \mid (a-b)$.
And if $c \equiv d \pmod{m}$ we have $m \mid (c-d)$.

This in turn implies that
$m \mid (a - b)c$ (because $m \mid (a - b)p$ for all integers p)
and that
$m \mid (c - d)b$ (because $m \mid (a - b)p$ for all integers p).

Therefore we have

$$m \mid ((a - b)c + (c - d)b)$$

Which can be written as:

$$m \mid (ac - bd)$$

So we can conclude that $ac \equiv (bd) \pmod{m}$. □

Congruence modulo m is an equivalence relation. Observe that we can partition the integers by their congruences.

Examples:

Congruence (mod 2) partitions integers into those that are even and odd.

Congruence (mod 3) partitions integers into three classes those that are divisible by 3 (remainder 0) and those with remainder 1, and remainder 2 when divided by 3.

In general we say that congruence modulo m partitions the integers into m classes called *residue classes modulo m*. Furthermore, each of these residue classes can be denoted by an integer x within the class using the notation $[x]_m$. Using set notation we can express this as follows:

$$[x]_m = \{a \in \mathbb{Z} : a \equiv x \bmod m\}$$

And each of the residue classes can be denoted by its smallest member as follows:

$$[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m$$