Number Theory: Part 2

1 Primes

Mathematicians have been interested in primes for thousands of years. Many fundamental results regarding primes have been discovered, and yet to this date, many famous conjectures involving primes remain unsolved. In this section we study some of the most important properties of primes. We shall see in later sections how these apply to other areas of number theory, and also to algorithms and cryptography.

A prime number is a number **greater than 1** that is only divisible by 1 and itself. A number that is *not* prime is called a composite number (4,6,8,9,10, etc)

Many facts regarding primes are likely instinctive to you at this point in your education. It is important nevertheless to establish the preliminaries regarding primes, and to ensure that these facts are applied correctly.

Theorem 1. *If p is prime and $p|ab$, then $p|a$ or $p|b$.*

For example, $5|20$ and since 5 is prime, then 5 divides *either* 4 or 5 since $20 = 4 \cdot 5$. Note that the above theorem is *not* necessarily true for a number that is *not* prime. For example, 6 divides $3 \cdot 8$, but 6 does not divide 3 or 8.

In elementary school we were taught that primes are essentially the *building blocks* of positive integers: that every positive integer can be factored into primes. This is something that is often practiced as a child, and perhaps taken for granted. Nevertheless, the fact is due to the following very famous theorem from number theory.

Theorem 2. *The **Fundamental Theorem of Arithmetic** states that every positive integer greater than 1 can be written uniquely as a prime or the product of primes.*

The important consequence of this theorem is that a number is factored in *exactly one way*. We usually factor a number in order of increasing primes, such as in:

$$2244 = 2^2 \cdot 3 \cdot 11 \cdot 17$$

The theorem confirms that *there is no other way* to factor this number into primes. Every factorization will have exactly two 2's, one 3, one 11, and one 17.

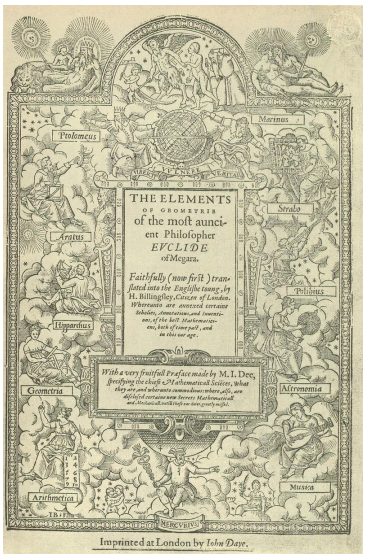
If a number is n *not* prime, then it can be factored into primes. The following theorem states that there is at least one prime divisor that is less than $\sqrt{n}$.

Theorem 3. *If n is composite, then n has a prime divisor less than or equal to $\sqrt{n}$.*

Proof: This seems like a very natural fact and the proof is quite simple. If n is composite, then it can be written as the product of two numbers, $n = ab$. Suppose for contradiction that $a > \sqrt{n}$ and $b > \sqrt{n}$. Then $n = ab > \sqrt{n} \cdot \sqrt{n} = n$, which is a contradiction. Thus one of the divisors is less than $\sqrt{n}$. It may be prime, and if it is not, one of it's prime divisors is then less than $\sqrt{n}$.

This theorem is useful when determining if a number is prime. For example, the number 113 is prime. In order to verify this fact, we do not need to check *all* possible primes that are less than 113. Instead, we

only need to verify if any of the primes $2, 3, 5, 7$ are factors of 113, since they are the only possible primes less than $\sqrt{113} = 10.6$. Since 113 is not divisible by $2, 3, 5$ or 7, then we can conclude that it is prime.

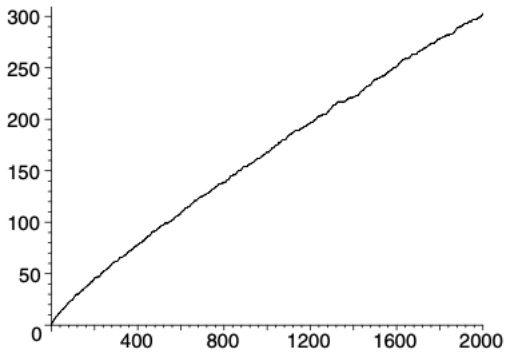


In the third century B.C. the famous Greek mathematician Euclid published his work "*Elements*", which is often referred to as the most successful and influential textbook ever written. In this work, he proved one of the most famous results regarding primes: that there are **infinitely many primes**. We restate the theorem here.

Theorem 4. *There are an infinite number of primes. Whenever $p_1, p_2, \ldots, p_n$ are the n smallest primes, there is a larger prime not listed.*

One of the most important questions about primes is, how *many* primes are there, up to a given number n? For example, how many primes are there less than 100? Or less than 1000000?

The notation used for the number of primes up to n is $\pi(n)$. The figure below shows the number of primes less than n for $n = 1$ to 2000.



As one can see above, the number of primes less than n increases and is reasonably smooth Around 1900 the following theorem established a fundamental fact about the number $\pi(n)$, called the **Prime Number Theorem**:

Theorem 5. *The number of primes among $1, 2, \ldots, n$ is approximated as:*

$$\pi(n) \sim \frac{n}{\ln n}$$

For example, the number of primes less than 10000 is approximately $\ln(10000)/10000 \sim 1086$.

Many facts and properties about primes are extremely difficult to prove. In fact, many famous conjectures are still open and have no proof and have haunted mathematicians for centuries. For example, in 1742 **Christian Goldbach** conjectured:

"*Every even integer larger than 2 can be written as the sum of two primes.* "

We can check this conjecture for small numbers:

$$4 = 2 + 2$$

$$6 = 3 + 3$$

$$8 = 5 + 3$$

$$10 = 7 + 3$$

etc. With today's computers, this conjecture has been checked for extremely large numbers, beyond $2 \cdot 10^{17}$, and thus most mathematicians believe it to be true. However, no proof has been found.

The French mathematician Pierre de Fermat (1601-1655) discovered the now famous theorem referred to simply as **Fermat's Little Theorem**. This theorem has profound implications in number theory and computer science.

Fermat's Little Theorem:

Theorem 6. *If p is prime and a is an integer that is **not divisible by** p, then*

$$p|(a^{p-1} - 1)$$

This is equivalent to

$$a^{p-1} \equiv 1 \mod p$$

or

$$a^p \equiv a \mod p$$

Let's test this theorem with an example. Let $p = 7$ and $a = 8$. Then

$$a^{p-1} = 8^6 = 262144 = 1 \mod 7$$

By Fermat's last theorem, *any* prime number p and integer a which have no factors in common with p will satisfy the above equation. In some ancient Chinese sources, some mathematicians believed that this concept could be used to *test* if a number is prime. For example, it was believed that if:

$$2^{n-1} \equiv 1 \mod n$$

then this guaranteed that n was prime. They observed this to be true for all the numbers that they knew of that were prime. Without computers or more advanced techniques, they assumed it was true. However, there are integers that are *not prime* that still satisfy this equation. For example, for $n = 341$ and $a = 2$ the equation is true, even though $n = 341$ is not prime. $(341 = 11 \cdot 31)$.

$$2^{340} \equiv 1 \mod 341$$

2 Greatest common divisors

Until now we have discussed notions and results involving the integers, and how to carry out computations involving the remainder. We now turn the one of the keys to many algorithms in number theory - the greatest common divisor.

Definition. *For non-zero integers a and b, the **largest** integer d such that $d|a$ and $d|b$ is called the **greatest common divisor**, and is denoted $gcd(a, b)$.*

For example, $\gcd(28, 49) = 7$. If either a or b is prime, then the greatest common divisor will be either that prime, or 1. For example, if $a = 7$ and b is not a multiple of 7, then $gcd(7, b) = 1$. On the other hand, if b *is* a multiple of 7, then $gcd(7, b) = 7$.

Definition. *Integers a and b are called relatively prime if their greatest common divisor is 1.*

Certainly if either a or b is prime, then the pair is relatively prime. However, we can also have non-primes that are *relatively prime* to each other, as in 4 and 45: neither of these are prime, yet their only common divisor is 1, thus they are *relatively prime*.

We now present some rather natural facts regarding the greatest common divisor:

Theorem 7. *Suppose that a and b are positive integers.*

- *If $a|b$, then $gcd(a, b) = a$*
- *If $gcd(a, b) = 1$ and $a|bc$ then $a|c$.*

The first item above requires little thought to prove. As an example, consider $6|18$, in which case $\gcd(6, 18) = 6$ since no larger divisor could divide 6. The second item we will prove formally in the next section, although the result should be familiar to you and you may have already become accustomed to using it. For example, notice that $10|360$, and since $360 = 40 \cdot 9$, and $gcd(10, 9) = 1$ then we can conclude that $10|40$. On the other hand, since $10|25 \cdot 4$, then we *cannot* conclude that $10|25$ or $10|4$ since $gcd(10, 4) \neq 1$ and $gcd(10, 25) \neq 1$.

2.1 Least Common Multiples

The smallest positive integer that is divisible by both a and b is called the least common multiple of a and b and is denoted $lcm(a, b)$. For integers $a = 20$ and $b = 14$, the least common multiple is 140 since both $20|140$ and $14|140$ and no smaller number is divisible by both 20 and 14.

Finding the gcd and lcm with prime factorization:

The prime factorization of each of a and b can be used to find *both* the least common multiple and the greatest common divisor. For the greatest common divisor, we take the **minimum** number of each prime that appear in **both** a and b. For example, if

$$a = 1660120 = 2^3 \cdot 5 \cdot 7^3 \cdot 11^2$$

$$b = 100100 = 2^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$$

then the greatest common divisor is:

$$\gcd(a, b) = 2^2 \cdot 5 \cdot 7 \cdot 11 = 1540$$

For the least common multiple, we take the **maximum** number of each prime that appear in **either** a or b:

$$lcm(a, b) = 2^3 \cdot 5^2 \cdot 7^3 \cdot 11^2 \cdot 13$$

2.2 Chinese Remainder Theorem

Systems of equations with congruences are extremely useful in many areas of mathematics. Arithmetic with large numbers is often simplified using systems of congruences. In ancient Chinese and Hindu puzzles there are writings that ask how to solve such systems. For example, how would we solve for the variable x in:

$$x \equiv 2 \mod 5$$

$$x \equiv 3 \mod 7$$

The theorem that solves such equations is called the *Chinese Remainder Theorem*. It is stated below (the simpler version):

Theorem 8. *Chinese Remainder Theorem: If m and n are **relatively prime** then the system of equations*

$$x \equiv a \mod m$$
$$x \equiv b \mod n$$

has a unique solution for x modulo mn.

The solution x is found using the following steps:

- Find the inverse of m in modulo n: m_n^{-1} Find the inverse of n in modulo m: n_m^{-1}.
- The solution x is then:

$$x = a \cdot n \cdot n_m^{-1} + b \cdot m \cdot m_n^{-1}$$

Example. *Solve the system of equations for x using the Chinese Remainder Theorem:*

$$x \equiv 2 \mod 5$$
$$x \equiv 3 \mod 7$$

Solution: In the system above, $m = 5$ and $n = 7$. Then $mn = 35$ and we are looking for a unique solution in modulo 35. The solution x will be between 0 and 34 and *any* other x that also solves this system of equations will be congruent to our x in modulo 35.

- The inverse of 5 in modulo 7 is 3 since $5 \cdot 3 = 15 = 1 \mod 7$. The inverse of 7 in modulo 5 is 3 since $7 \cdot 3 = 21 = 1 \mod 5$.
- The solution x is:
$$x = 2 \cdot 7 \cdot 3 + 3 \cdot 5 \cdot 3 = 87 = 17$$

We can check that indeed 17 is a solution. Certainly $17 = 2 \mod 5$ and $17 = 3 \mod 7$. Therefore $x = 17$ is a solution, and no other solution exists unless it is equivalent to $17 \mod 35$.