# Elementary Number Theory

Jim Belk

May 4, 2013

Number theory is the branch of mathematics concerned with the properties of the positive integers, such as divisibility, prime numbers, and so forth. It is an ancient subject: four volumes of Euclid's *Elements* were devoted entirely to number theory, and Greek mathematicians were arguably as interested in the theory of numbers as they were in geometry.

**Note.** Number theory is primarily concerned with the properties of integers, with real numbers playing at best an ancillary role. For that reason, all variables in these notes should be assumed to represent integers unless otherwise noted.

## 1 Divisors

**Definition 1.1.** We say that $a$ ***divides*** $b$, denoted $a|b$, if

$$b = na$$

for some integer $n$.

If $a$ divides $b$, then $b$ is said to be ***divisible*** by $a$. The number $a$ is called a ***divisor*** (or ***factor***) of $b$, and $b$ is called a ***multiple*** of $a$.

**Example 1.2.** Since $5 \times 7 = 35$, we know that $5|35$ and $7|35$. The divisors of 35 are $\{\pm 1, \pm 5, \pm 7, \pm 35\}$, and the multiples of 5 are $\{\ldots, -10, -5, 0, 5, 10, \ldots\}$.

Note that the definition of divisibility does not exclude 0. In fact, **every integer divides** 0, since $0 = 0a$ for any integer $a$. This is an exception to the general rule that $a|b$ implies $|a| \leq |b|$.

The relation $|$ satisfies a large number of identities. Here are a few of the more important ones:

**Proposition 1.3.**

1. *If $a|b$ and $b|c$, then $a|c$.*
2. *If $a|b$ and $c|d$, then $ac|bd$.*
3. *If $a|b$ and $a|c$, then $a|(b+c)$.*

*Proof.*

1. If $b = ma$ and $c = nb$, then $c = (mn)a$.
2. If $b = ma$ and $d = nc$, then $bd = (mn)(ac)$.
3. If $b = ma$ and $c = na$, then $b + c = (m+n)a$. □

A natural way to compare two numbers is to compare their divisors:

**Definition 1.4.** The ***greatest common divisor*** of $a$ and $b$ is the greatest integer that divides both $a$ and $b$.

We shall write $\gcd(a, b)$ for the greatest common divisor of $a$ and $b$. For example:

$$\gcd(12, 20) = 4, \qquad \gcd(7, 12) = 1, \qquad \text{and} \qquad \gcd(0, 6) = 6.$$

Note that $\gcd(0, a) = a$ for any nonzero integer $a$. (The greatest common divisor of 0 and 0 is undefined.)

Since 1 divides every integer, the greatest common divisor of $a$ and $b$ is always at least 1. If it is equal to 1, it means that $a$ and $b$ have no other positive factors in common. In this case, we say that $a$ and $b$ are ***relatively prime*** (or ***coprime***).

# 2 Primes

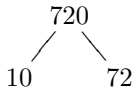
**Definition 2.1.** A number $p > 1$ is ***prime*** if its only positive factors are 1 and $p$.

Any number $a > 1$ that is not prime is ***composite***. This means that $a$ can be written as a product

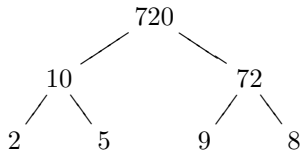
$$a = bc$$

where both $b$ and $c$ are greater than one. This is called ***factoring***.

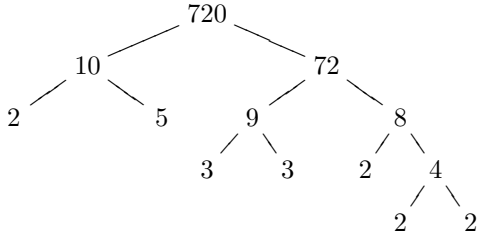
Using repeated factoring, any composite number can be expressed as a product of primes. For example, suppose that we factor the number 720 as follows:




Since 10 and 72 are both composite, we can factor these as well:




At this point, we have broken our number into four pieces, whose product ($2 \times 5 \times 9 \times 8$) is 720. Two of these pieces (the 2 and the 5) are prime, but the other two can be factored further:



This is called a ***factor tree***. The "leaves" of the tree are prime numbers that multiply to 720:

$$2 \times 5 \times 3 \times 3 \times 2 \times 2 \times 2 = 720.$$

This is a ***prime factorization*** of 720. The same procedure will produce a prime factorization of any composite number.

Of course, none of this discussion has been rigorous. If we want to *prove* that every composite number can be factored into primes, we must use induction:

**Prime Factorization Theorem.** *Every composite number can be expressed as a product of primes.*

*Proof.* Let $a$ be a positive integer. We must prove that if $a$ is composite, then $a$ can be expressed as a product of primes. We proceed by induction on $a$.

*Base Case:* If $a = 1$, then $a$ is not composite, so the statement is vacuously true.

*Induction Step:* Now suppose that $a > 1$, and assume that the statement holds for all positive integers less than $a$. If $a$ is composite, then $a$ can be written as a product

$$a = bc$$

where $1 < b < a$ and $1 < c < a$. If these numbers are prime, we are done. If only one of these numbers is prime, say $b$, then the other number $c$ must be composite. By our induction hypothesis, $c$ can be expressed as a product of primes $p_1 \times \cdots \times p_n$, and therefore $a = b \times p_1 \times \cdots \times p_n$.

Finally, if both $b$ and $c$ are composite, then each can be written as a product of primes:

$$b = p_1 \times \cdots \times p_m \qquad \text{and} \qquad c = q_1 \times \cdots \times q_n.$$

In this case, $a$ is the product of all of these:

$$a = p_1 \times \cdots \times p_m \times q_1 \times \cdots \times q_n$$ □

As you are no doubt aware, the prime factorization of a number is actually unique up to reordering of the factors. This statement is known as the ***fundamental theorem of arithmetic***. You should not fool yourself into thinking that the fundamental theorem of arithmetic is trivial—excluding the formula for the area of a circle, it is probably the deepest theorem that you learned in elementary school.

The proof of the fundamental theorem of arithmetic requires the following key fact about prime numbers:

**Euclid's Lemma.** *If $p$ is prime and $p|ab$, then either $p|a$ or $p|b$.*

This lemma does not follow in any direct way from the definition of a prime number, and we are not currently in a good position to prove it. Instead, we must begin by developing some additional machinery. We will return to the proof of the fundamental theorem of arithmetic in section 5.

# 3 Division with Remainders

**Definition 3.1.** Let $a$ and $b$ be integers, with $b > 0$. The ***integer quotient*** of $a$ and $b$ is the greatest integer $q$ for which $qb \leq a$

If $a$ is not divisible by $b$, then the product $qb$ will be less than $a$. The difference $r = a - qb$ is called the ***remainder*** of the division, and we write

$$a \div b \;=\; q \text{ R } r$$

to mean that the division of $a$ by $b$ has quotient $q$ and remainder $r$. For example,

$$20 \div 7 \;=\; 2 \text{ R } 6 \qquad \text{and} \qquad -20 \div 7 \;=\; -3 \text{ R } 1.$$

Note that the remainder is always nonnegative, and is always less than $b$.

There is no standard notation in mathematics for the integer quotient and remainder. The quotient can be written as $\lfloor a/b \rfloor$ (the greatest integer less than or equal to $a/b$), which is clunky but sufficient. There are several common notations for the remainder:

$$a \bmod b \qquad\qquad \operatorname{mod}(a, b) \qquad\qquad a \,\%\, b$$

The third is from the C programming language; it is rare among mathematicians, but popular in computer science.

# 4 Bézout's Identity

**Definition 4.1.** Let $a$ and $b$ be integers. A ***linear combination*** of $a$ and $b$ is any integer of the form

$$ma \;+\; nb$$

where $m$ and $n$ are integers.

For example, 26 is a linear combination of 6 and 10, since $26 = 2 \cdot 10 + 1 \cdot 6$. Though it is less obvious, 2 is also a linear combination of 6 and 10, since

$$2 \;=\; -3 \cdot 6 \;+\; 2 \cdot 10.$$

It follows that any even number can be expressed as a linear combination of 6 and 10.

**Bézout's Identity.** *Let $a$ and $b$ be nonzero integers, and let $d = \gcd(a, b)$. Then there exist integers $m$ and $n$ such that*

$$ma \;+\; nb \;=\; d.$$

That is, the greatest common divisor of $a$ and $b$ can always be expressed as a linear combination of $a$ and $b$. This is particular surprising when $a$ and $b$ are relatively prime, in which case $ma + nb = 1$.

*Proof.* Let $x$ be the smallest positive integer that can be expressed as a linear combination of $a$ and $b$. We know that $x$ is a multiple of $d$, since $a$ and $b$ are both multiples of $d$. We claim that $x = d$.

Suppose to the contrary that $x > d$. Then $x$ cannot be a common divisor of $a$ and $b$, so either $x \nmid a$ or $x \nmid b$. Without loss of generality, suppose that $x \nmid a$. Then

$$a \div x \;=\; q \text{ R } r$$

where the remainder $r$ is positive. But $r = a - qx$, so $r$ can be written as a linear combination of $a$ and $b$. This is a contradiction, since $r$ is necessarily less than $x$. □

The numbers $m$ and $n$ for which $ma + nb = \gcd(a, b)$ are known as ***Bézout coefficients***.

**Corollary 4.2.** *Let $a$, $b$, and $c$ be nonzero integers. Then $c$ can be written as a linear combination of $a$ and $b$ if and only if $c$ is a multiple of* $\gcd(a, b)$.

We can use Bézout's identity to prove Euclid's lemma:

**Euclid's Lemma.** *If $p$ is prime and $p|ab$, then either $p|a$ or $p|b$.*

*Proof.* Suppose that $p|ab$ and $p \nmid a$. We must prove that $p|b$.

Since $p \nmid a$ and $p$ is prime, the greatest common divisor of $p$ and $a$ must be 1. Therefore, by Bézout's identity, there exist integers $m$ and $n$ such that

$$ma + np = 1.$$

Multiplying through by $b$ gives

$$mab + npb = b.$$

Since $p|ab$, the left side of this equation is divisible by $p$, and therefore $p|b$. □

# 5 The Fundamental Theorem of Arithmetic

We are now in a position to prove the fundamental theorem of arithmetic. We begin by proving a slightly stronger version of Euclid's lemma:

**Generalized Euclid's Lemma.** *If $p$ is prime and $p|a_1 \cdots a_n$, then $p|a_i$ for some $i$.*

*Proof.* This is a straightforward induction. The base case $n = 2$ is Euclid's lemma. For $n > 2$, observe that

$$a_1 \cdots a_n = (a_1 \cdots a_{n-1})a_n.$$

By Euclid's lemma, either $p|a_1 \cdots a_{n-1}$ or $p|a_n$. In the first case, it follows from our inductive hypothesis that $p|a_i$ for some $i \leq n - 1$. □

The next lemma tells us exactly which primes must appear in a prime factorization:

**Lemma 5.1.** *Let $p$ and $q_1, \ldots, q_n$ be primes. Then $p|q_1 \cdots q_n$ if and only if $p \in \{q_1, \ldots, q_n\}$.*

*Proof.* If $p \in \{q_1, \ldots, q_n\}$, then clearly $p|q_1 \cdots q_n$. Conversely, if $p|q_1 \cdots q_n$, then by the previous lemma $p|q_i$ for some $i$. Since $q_i$ is prime and $p \neq 1$, we deduce that $p = q_i$. □

**The Fundamental Theorem of Arithmetic.** *Let $a$ be composite. Then there exists a unique sequence of primes $p_1 \leq \cdots \leq p_n$ such that $a = p_1 \cdots p_n$.*

In the statement of this theorem, we have added the artificial requirement that $p_1 \leq \cdots \leq p_n$ to eliminate any ambiguity regarding the ordering of the primes in the factorization of $a$.

*Proof.* The prime factorization theorem establishes existence. For uniqueness, suppose that

$$p_1 \cdots p_m = q_1 \cdots q_n$$

where $p_1 \leq \cdots \leq p_m$ and $q_1 \leq \cdots \leq q_n$ are primes. We wish to prove that $m = n$ and $p_i = q_i$ for each $i$. Without loss of generality, we may assume that $m \leq n$. We proceed by induction on $m$.

*Base Case:* For $m = 1$, the equation is $p_1 = q_1 \cdots q_n$. Since $p_1$ is prime, the only possibility is that $n = 1$, with $p_1 = q_1$.

*Induction Step:* For $m > 1$, it follows from the previous lemma that $p_m$ is the largest prime divisor of $p_1 \cdots p_m$, and $q_n$ is the largest prime divisor of $q_1 \cdots q_n$. Since $p_1 \cdots p_m = q_1 \cdots q_n$, we conclude that $p_m = q_n$. Dividing these out leaves

$$p_1 \cdots p_{m-1} = q_1 \cdots q_{n-1}.$$

The rest now follows from our induction hypothesis. □

# 6 Exercises

1. Compute the following greatest common divisors.
   (a) $\gcd(120, 75)$
   (b) $\gcd(32, 45)$
   (c) $\gcd(0, 8)$

2. Find the prime factorization of the following numbers.
   (a) 210
   (b) 330
   (c) 365

3. Let $a, b \in \mathbb{Z}$. Prove that $\gcd(a, b) = \gcd(a + b, b)$.

4. Let $a, b \in \mathbb{Z}$, and let $p$ be a prime number. Suppose that $ab \equiv 0 \pmod{p}$. Prove that either $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

5. Let $p$ be a prime number.
   (a) Let $a, b \in \mathbb{Z}$. Suppose that $p|b$, $p \not| a$, and $a|b$. Prove that $p \,|\, \frac{b}{a}$.
   (b) Let $k \in \mathbb{Z}$. Suppose that $0 < k < p$. Use part (a) to prove that the binomial coefficient $\binom{p}{k}$ is a multiple of $p$.

6. Let $p$ be a prime number. Use induction to prove that

   $$n^p \equiv n \pmod{p}$$

   for all $n \in \mathbb{N}$. (*Hint:* Use the Binomial Theorem and part (a)). This result is known as **Fermat's Little Theorem**.

7. The greatest common divisor can be defined for more than two integers at a time:

   **Definition 6.1.** Let $a_1, \ldots, a_n$ be integers. The ***greatest common divisor*** of $a_1, \ldots, a_n$, denoted $\gcd(a_1, \ldots, a_n)$, is the greatest integer that divides every $a_i$.

   Prove that $\gcd(a_1, \ldots, a_n, b) = \gcd(\gcd(a_1, \ldots, a_n), b)$.

8. We can also define linear combinations of more than two integers:

   **Definition 6.2.** A ***linear combination*** of integers $a_1, \ldots, a_n$ is any number of the form

   $$m_1 a_1 + \cdots + m_n a_n$$

   where the coefficients $m_1, \ldots, m_n$ are integers.

   For $n \geq 2$, use induction to prove that $\gcd(a_1, \ldots, a_n)$ can be expressed as a linear combination of $a_1, \ldots, a_n$.