# Number Theory

Number theory is the study of the integers. We also practice and the proof techniques that we developed earlier. In number theory (and in this section) variables range over the set of integers, $\mathbb{Z}$.

## A Divisibility

Let us begin with definition of the *divides* relation:

$$a \text{ divides } b \text{ iff } ak = b \text{ for some } k.$$

The notation, $a|b$ means "$a$ divides $b$". If $a|b$, then $b$ is a *multiple* of $a$. If $a$ divides $b$, then the remainder of $b/a$ is zero. Note that by this definition, every number divides zero.

**Lemma 1.** *The following statements about divisibility hold.*

(a) *If $a|b$, then $a|bc$ for all $c$.*

(b) *If $a|b$ and $b|c$, then $a|c$.*

(c) *If $a|b$ and $a|c$, then $a|(sb+tc)$ for all $s$ and $t$ .*

(d) *For all $c \neq 0$, $a|b$ if and only if $ca|cb$.*

*Proof.* (a) If $a|b$, then there is $k$ such that $b = ka$. Then $bc = (ck)a$ and $a|bc$.

(b) Assume $a|b$ and $b|c$. There exists an integer $k_1$ such that $ak_1 = b$. Similarly, there exists an integer $k_2$ such that $bk_2 = c$. We get

$$c = bk_2 = ak_1k_2 = a(k_1k_2).$$

This implies that $a|c$.

(c) If $a|b$, then there is $k_1$ such that $b = k_1a$. For any $s$, $sb = sk_1a$. Similarly, if $a|c$, then there is $k_2$ such that $c = k_2a$. We obtain the for any $t$, $tsc = tk_1a$. By combining these, we get $sb + tc = (sk_1 + tk_2)a$ and $a|(sb + tc)$.

(d) If $a|b$, then $b = ka$. We have that $cb = k(ca)$ and $ca|cb$. Conversely, if $ca|cb$, then $cb = k(ca)$ for some $k$. Now $cb = c(ka)$ and because $c \neq 0$, we can divide by it. We get $b = ka$, that is, $a|b$. □

We learned in elementary school that if one number does not evenly divide another, you get a "quotient" and a "remainder" left over. We can state this as a theorem:

**Theorem 2** (Division Theorem)**.** *Let $n$ and $d > 0$ be integers. Then there exists a* ***unique*** *pair of integers $q$ and $r$, such that*

$$n = q \cdot d + r \quad \textit{and} \quad 0 \leq r < d.$$

*Proof.* First note that the proof require *existence* and *uniqueness* of the pari $q$ and $r$. We first consider existence.

**Existence** We have three disjoint cases:

**Case 1** $d \mid n$: This means that there is $q$ such that $n = qd$. Now $r = 0$.

**Case 2** $d \nmid n$ and $n > 0$: Let us consider the set

$$S = \{n - qd \mid q \geq 0 \text{ and } n - qd \geq 0\}.$$

Because $S \subseteq \mathbb{N}$ and $\mathbb{N} \neq \emptyset$ (why?), the well-ordering principle says that $S$ has a smallest element $r = n - qd$. Now $n = qd + r$. We need to show that $r \geq 0$ and $r < d$. Now $r \geq 0$ follows directly from the definition of the set $S$. Suppose for contradiction that $r \geq d$. There are two possible cases:

(i) $r = d$: Then $n = qd + d = (q + 1)d$. This contradicts $d \nmid n$. Therefore, $r \neq d$.

(ii) $r > d$: Then we set $r_1 = r - d$. Now $r_1 > 0$ and

$$n - r_1 = qd + r - r_1 = qd + r - (r - d) = qd + d = (q + 1)d.$$

We have $n = (q + 1)d + r_1$. This means that $r_1$ belongs to $S$. Because $r_1 = r - d$ and $d > 0$, we have that $r_1 < d$. This contradicts the assumtion that $r$ is the smallest element of $S$. Therefore, $r \not> d$ either. We conclude that $r \leq d$.

**Case 3** $d \nmid n$ and $n < 0$: Now $-n$ is positive, so the are $q_0$ and $r_0$ such that

$$-n = q_0 d + r_0,$$

for some $0 \leq r_0 < d$. Because $n$ (and $-n$) is not divisible by $d$, we actually have $0 < r_0 < d$. We set

$$q = -q_0 - 1 \quad \text{and} \quad r = -r_0 + d.$$

We need to prove that $n = qd + r$ and $0 \leq r < d$. We have

$$\begin{aligned} n &= -q_0 d - r_0 \\ &= (q + 1)d + r - d \\ &= qd + d + r - d \\ &= qd + r. \end{aligned}$$

Now $0 < r_0 < d$ and $0 > -r_0 > -d$. So, $r = -r_0 + d > -d + d = 0$. Because $r_0 > 0$, $r = d - r_0$ gives $r < d$. Thus, $0 < r < d$, as required.

**Uniqueness** Suppose that there are $q_1, q_2, r_1, r_2$ such that

$$\begin{aligned} n &= q_1 d + r_1, \quad 0 \leq r_1 \leq d \\ n &= q_2 d + r_2, \quad 0 \leq r_2 \leq d. \end{aligned}$$

We see that

$$0 \leq r_1, \quad r_1 < d, \quad -d < -r_2, \quad -r_2 \leq 0.$$

From this we get

$$-d < r_1 - r_2 \quad \text{and} \quad r_1 - r_2 < d.$$

On the other hand,

$$q_1 d + r_1 = q_2 d + r_2.$$

and so

$$r_1 - r_2 = d(q_2 - q_1).$$

Therefore,

$$-d < d(q_2 - q_1) < d.$$

Dividing by $d$ gives $-1 < q_2 - q_1 < 1$. This is possible only if $q_2 - q_1 = 0$ and $q_1 = q_2$. From this we obtain $r_1 = r_2$. □

The number $q$ is called the **quotient** and $r$ is the **remainder** of $n$ divided by $d$.

In programming languages there are in-built functions for these. For instance in Python:

```
>>> q = 10 // 3
>>> r = 10 % 3
>>> print(q,r)
3 1
```

There is a function `divmod`() which does both:

```
>>> divmod(10, 3)
(3, 1)
```

## B The Greatest Common Divisor

The greatest common divisor of $a$ and $b$ is the largest number that is a divisor of both $a$ and $b$. It is denoted by $\gcd(a, b)$. For example, $\gcd(18, 24) = 6$.

```
>>> import math
>>> math.gcd(18,24)
6
```

Note that by definition, $\gcd(a, b)$ is always positive!

A linear combination is an expression constructed from a set of terms by multiplying each term by a constant and adding the results.

**Proposition 3.** *The greatest common divisor of $a$ and $b$ is a linear combination of $a$ and $b$.*

For example, the greatest common divisor of 52 and 44 is 4. The number 4 is a linear combination of 52 and 44:

$$6 \cdot 52 - 7 \cdot 44 = 4.$$

We will present the proof a little later.

**Lemma 4.** *Let $a$ and $b$ be two integers. Then $\gcd(a, b)$ is the smallest positive linear combination of $a$ and $b$*

*Proof.* We know by Proposition 3 that $\gcd(a, b)$ is a linear combination of $a$ and $b$. It is always $\geq 1$, so $\gcd(a, b)$ is always positive. We need to show only the minimality.

Let us denote

$$S = \{sa + tb \mid sa + tb \geq 1\}.$$

The set $S$ is by definition a subset of $\mathbb{N}$. Now we know that $\gcd(a, b)$ is a member of $S$, therefore $S \neq \emptyset$. By the well-ordering principle, $S$ has a smallest element $m$. We have immediately that $m \leq \gcd(a, b)$.

Let $c$ be a common factor of $a$ and $b$, that is, $c|a$ and $c|b$. Then by Lemma 1, $c|(sa+tb)$ for any $s$ and $b$. In particular, we have that $\gcd(a, b)|(sa + tb)$. Because $m \in S$, $m$ is a linear combination of $a$ and $b$, we have $\gcd(a, b)|m$. This implies $\gcd(a, b) \leq m$.

We have now proved $m \leq \gcd(a, b)$ and $m \geq \gcd(a, b)$. Therefore, $m = \gcd(a, b)$. □

**Lemma 5.** *The following statements about the greatest common divisor hold:*

(a) *Every common divisor of $a$ and $b$ divides $\gcd(a, b)$.*

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

(c) *$\gcd(ac, bc) = c \cdot \gcd(a, b)$ for all $c > 0$.*

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

*Proof.* (a) By Proposition 3,

$$\gcd(a, b) = d_1a + d_2b$$

for some $d_1$ and $d_2$. Let $x$ be some common divisor of $a$ and $b$. Then $a = xs_1$ and $b = xs_2$ for some $s_1$ and $s_2$. We have

$$\gcd(a, b) = d_1xs_1 + d_2xs_2 = x(d_1s_1 + d_2s_2).$$

Thus, $x|\gcd(a, b)$.

(b) By Proposition 3, there exist integers $s$, $t$ , $u$, and $v$ such that:

$$sa + tb = 1$$
$$ua + vc = 1$$

Multiplying these two equations gives:

$$(sa + tb)(ua + vc) = a(sua + svc + tbu) + bc \cdot tv = 1$$

This is a linear combination of a and bc that is equal to 1. This is the smallest *positive* linear combination of $a$ and $bc$. Lemma 4 implies that $\gcd(a, bc) = 1$.

(c) We know that $\gcd(a, b)$ is the smallest positive linear combination of $a$ and $b$. We have that $\gcd(ac, bc)$ is a linear combination of $ac$ and $bc$. Because $c > 0$,

$$\gcd(ac, bc) = s_1ac + t_1bc = c(s_1a + t_1b) \geq c \cdot \gcd(a, b).$$

On the other hand,

$$c \cdot \gcd(a, b) = c(sa + tb) = s \cdot ca + t \cdot cb \geq \gcd(ac, bc).$$

(d) By Proposition 3, $\gcd(ac, bc)$ is equal to some linear combination of $ac$ and $bc$. Now $a|ac$ is trivial and $a|bc$ holds by assumption. Therefore, $a$ divides also every linear combination of $ac$ and $bc$. In particular, $a$ divides $\gcd(ac, bc) = c \cdot \gcd(a, b) = c \cdot 1 = c$. □

Euclid's Algorithm (see below) for finding the greatest common divisor of two numbers relies on repeated application of the equation:

**Proposition 6.** *Let $a$ and $b$ be positive.*

$$\gcd(a, b) = \gcd(b, \text{rem}(a, b)),$$

*where* $\text{rem}(a, b)$ *is the remainder of $a$ divided by $b$.*

*Proof.* Note that we cannot use facts given in Lemma 5, because we proved them by using Proposition 3. Proposition 6 is essential in verifying Proposition 3.

Denote $g = \gcd(a, b)$ and because $a = nb + r$ for some $n$ and $0 \leq r < b$, we have $r = \text{rem}(a, b)$. We have to prove that $g = \gcd(b, r)$. Now $g|a$ and $g|b$. The latter gives $g|na$. We have that $g|(a - nb)$, that is, $g|r$. Because $g$ is a common divisor of $b$ and $r$, then $g \leq \gcd(b, r)$.

On the other hand, let $f$ be any common divisor of $b$ and $r$. Then, $f|b$ and $f|r$. We have that $f|nb$. Because $a = nb - r$, then $f|a$. This means that $f$ is a divisor of $a$ and $b$ and $f \leq \gcd(a, b) = g$. In particular, $\gcd(b, r) \leq g$. We have proved the claim. □

The **Euclidean Algorithm** for finding $\gcd(a, b)$ is the following:

1. If $a = 0$ then $\gcd(a, b) = b$, since the $\gcd(0, b) = b$, and we can stop.
2. If $b = 0$ then $\gcd(a, b) = a$, since the $\gcd(a, 0) = a$, and we can stop.
3. Write $a$ in quotient-remainder form $a = b \cdot q + r$.
4. Find $\gcd(b, r)$ using the Euclidean Algorithm since $\gcd(a, b) = \gcd(b, r)$.

**Example 7.**

$$\begin{aligned}
\gcd(1147, 899) &= \gcd(899, \underbrace{\text{rem}(1147, 899)}_{=248}) \\
&= \gcd(248, \underbrace{\text{rem}(899, 248)}_{=155}) \\
&= \gcd(155, \underbrace{\text{rem}(248, 155)}_{=93}) \\
&= \gcd(93, \underbrace{\text{rem}(155, 93)}_{=62}) \\
&= \gcd(62, \underbrace{\text{rem}(93, 62)}_{=31}) \\
&= \gcd(31, \underbrace{\text{rem}(62, 31)}_{=0}) \\
&= \gcd(31, 0) \\
&= 31
\end{aligned}$$

Proposition 3 (which is not proved) states that for any two integers $a$ and $b$ we are given, there are integers $s$ and $t$ such that

$$\gcd(a, b) = sa + tb$$

We can get these $s$ and $t$ always from the Euclid's Algorithm. Therefore, Euclid's algorithm **provides a proof** for Proposition 3.

For example, we can compute the GCD of 259 and 70 as follows:

$$\begin{aligned}
\gcd(259, 70) &= \gcd(70, 49) && \text{since } \text{rem}(259, 70) = 49 \\
&= \gcd(49, 21) && \text{since } \text{rem}(70, 49) = 21 \\
&= \gcd(21, 7) && \text{since } \text{rem}(49, 21) = 7 \\
&= \gcd(7, 0) && \text{since } \text{rem}(21, 7) = 0 \\
&= 7
\end{aligned}$$

After minor additions of Euclid's Algorithm, we can find the integers $s$ and $t$. The idea is that we can always present the current remainder in terms of $a$ and $b$. We start with $x = a$ and $y = b$. Then we iterate $x = y$ and $y = \text{rem}(x, y)$. The last nonzero remainder is the greatest common divisor. Such a linear combination can be found by reversing the steps of the Euclidean Algorithm:

| $x$ | $y$ | $\text{rem}(x,y)$ | $= x - q \cdot y$ |
|---|---|---|---|
| 259 | 70 | 49 | $= 259 - 3 \cdot 70$ |
| 70 | 49 | 21 | $= 70 - 1 \cdot 49$ |
| | | | $= 70 - 1 \cdot (259 - 3 \cdot 70)$ |
| | | | $= -1 \cdot 259 + 4 \cdot 70$ |
| 49 | 21 | 7 | $= 49 - 2 \cdot 21$ |
| | | | $= (259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$ |
| | | | $= \boxed{3 \cdot 259 - 11 \cdot 70}$ |
| 21 | 7 | 0 | $= 21 - 3 \cdot 7$ |

## C The Fundamental Theorem of Arithmetic

A *prime number* (or a *prime*) is a natural number greater than 1 that is not a product of two smaller natural numbers. A natural number greater than 1 that is not prime is called a *composite number*. For example, 5 is prime because the only ways of writing it as a product, $1 \cdot 5$ or $5 \cdot 1$, involve 5 itself. However, 4 is composite because it is a product $(2 \cdot 2)$ in which both numbers are smaller than 4.

**Theorem 8** (Fundamental Theorem of Arithmetic)**.** *Every positive integer $n$ can be written in a unique way as a product of primes:*

$$n = p_1 \cdot p_2 \cdots p_j, \quad \textit{where } p_1 \leq p_2 \leq \cdots \leq p_j$$

Note that we leave out exponents since we will explicitly write out repeated primes, for example, it is possible to have $p_1 = p_2 = 2$). This means that the same prime can appear in the product several times, like:

**Example 9.**

$$4312 = 2 \cdot 2156 = 2 \cdot 2 \cdot 1078 = 2 \cdot 2 \cdot 2 \cdot 539 = 2 \cdot 2 \cdot 2 \cdot 7 \cdot 77 = 2 \cdot 2 \cdot 2 \cdot 7 \cdot 7 \cdot 11.$$

This means that $4312 = 2^3 \cdot 7^2 \cdot 11$.

**Lemma 10** (Euclid's lemma)**.** *If $p$ is a prime and $p|ab$, then $p|a$ or $p|b$.*

*Proof.* The greatest common divisor of $a$ and $p$ must be either 1 or $p$, since these are the only positive divisors of $p$. If $\gcd(a,p) = p$, then the claim holds, because then $a$ is a multiple of $p$. Otherwise, $\gcd(a,p) = \gcd(p,a) = 1$ and $p|b$ by Lemma 5(d). □

**Lemma 11.** *Let $p$ be a prime. If $p|a_1 a_2 \cdots a_n$, then $p$ divides some $a_i$.*

*Proof.* By induction with respect to the length $n$ of the term $a_1 a_2 \cdots a_n$. □

Now we are ready to prove the Fundamental Theorem of Arithmetic, that is, every positive integer $n$ can be written in a unique way as a product of primes:

$$n = p_1 \cdot p_2 \cdots p_j, \quad \text{where } p_1 \leq p_2 \leq \cdots \leq p_j$$

*Proof.* There are two parts we need to prove:

- The existence of such a product of primes
- The product of primes is unique up to their order

**Existence** We have already proved this in Theorem 18 of 'Induction' section.

**Uniqueness** To prove uniqueness, suppose, that a number $n$ can be expressed as a product of primes in two ways:

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l.$$

For simplicity, let us denote $p = p_1 p_2 \cdots p_k$ and $q = q_1 q_2 \cdots q_l$. We will show that $p$ and $q$ consists of the same primes.

Let us consider the elements $p_i$ in $p$. It is clear that $p_i | (p_1 p_2 \cdots p_k)$ and because $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$, we have that $p_i | (q_1 q_2 \cdots q_l)$. This implies by Lemma 11 that $p_i | q_j$ for some $1 \leq j \leq l$. Since $p_i$ and $q_j$ are primes, we must have that $p_i = q_j$. Now we may *divide out* this common factor in the two products. This means that $p$ and $q$ have now become shorter.

We repeat with the remaining factors, until all common prime factors have been divided out. If $k = l$, then the products $p$ and $q$ contained exactly the same primes and the product is unique.

Let us prove that $k = l$. Suppose for contradiction that $k > l$. This would mean that the above 'cancellation method' terminates so that all $q_i$'s are cancelled out and only the number 1 remains on the right side. This means that there are some $p_{i_1}, \ldots, p_{i_m}$ left. But now $p_{i_1} p_{i_2} \cdots p_{i_m} = 1$. Since all primes are integers greater than 1, this is impossible! Therefore $k \not> l$. Similarly, we can show that $k < l$ is not possible. We have proved that $k = l$. □

# D Modular Arithmetic

**Arithmetic** is generally understood as the mathematics of numbers under addition, subtraction, multiplication, and division. Next we consider these mathematical operations with respect to congruence relations. Congruences are useful in dealing with divisibility. As we shall see in next section, they are also critical in cryptography.

Given an integer $n > 1$, called a **modulus**, two integers $a$ and $b$ are said to be **congruent modulo** $n$, if $n | (a - b)$. This is written

$$a \equiv b \bmod n.$$

Clearly, $\equiv$ is a *relation* between integers. For example: $29 \equiv 15 \bmod 7$, because $7|\underbrace{(29-15)}_{14}$. We can write also:

$$1 \equiv 8 \equiv 15 \equiv 22 \equiv 29 \equiv 36 \bmod 7.$$

Note that if any of these numbers is divided by 7, their remainder is 1. In fact, there is a close connection between congruences and remainders:

**Lemma 12.** *Let $a$, $b$ and $n > 1$ be integers. Then,*

$$a \equiv b \bmod n \iff \mathrm{rem}(a,n) = \mathrm{rem}(b,n)$$

*Proof.* By the Division Theorem, there are integers $q_1$, $r_1$ and $q_2$, $r_2$ such that:

$$\begin{aligned} a &= q_1 n + r_1, & 0 \le r_1 < n, \\ b &= q_2 n + r_2, & 0 \le r_2 < n, \end{aligned}$$

where $r_1 = \mathrm{rem}(a,n)$ and $r_2 = \mathrm{rem}(b,n)$. Subtracting the second equation from the first gives:

$$a - b = (q_1 - q_2)n + (r_1 - r_2). \qquad (\star)$$

Note that $r_1 < n$ and $r_2 \ge 0$ give $r_1 - r_2 < n$. Similarly, $-n < -r_2$ and $r_1 \ge 0$ give $-n < r_1 - r_2$. Together they mean that $-n < r_1 - r_2 < n$.

We have now that $a \equiv b \bmod n$ if and only if $n$ divides the right side of $(\star)$.

Suppose that $n$ divides the right side of $(\star)$. But because we have that $-n < r_1 - r_2 < n$, this can happen only when $r_1 - r_2 = 0$. This means that $r_1 = r_2$ and $\mathrm{rem}(a,n) = \mathrm{rem}(b,n)$. Thus, $a \equiv b \bmod n$ implies $\mathrm{rem}(a,n) = \mathrm{rem}(b,n)$.

Conversely, if $r_1 = \mathrm{rem}(a,n) = \mathrm{rem}(b,n) = r_2$, then by $(\star)$,

$$a - b = (q_1 - q_2)n.$$

This means that $n|(a-b)$, that is, $a \equiv b \bmod n$. □

**Lemma 13.** *Let $a$ and $n > 1$ be integers. Then,*

$$a \equiv \mathrm{rem}(a,n) \bmod n.$$

*Proof.* We know that

$$a = qn + \mathrm{rem}(a,n),$$

for some $q$. From this we get

$$a - \mathrm{rem}(a,b) = qn.$$

The number $qn$ is clearly divisible by $n$. Therefore, $a \equiv \mathrm{rem}(a,n) \bmod n$. □

Yet another way to think about "congruence modulo $n$" is that it defines a 'classification' of the integers into $n$ sets so that congruent numbers are all in the same set. For example, suppose that we are working modulo 3. Then we can divide the integers into 3 sets as follows:

$$\{\ldots, -6, -3, \boxed{0}, 3, 6, 9, \ldots\}$$
$$\{\ldots, -5, -2, \boxed{1}, 4, 7, 10, \ldots\}$$
$$\{\ldots, -4, -1, \boxed{2}, 5, 8, 11, \ldots\}$$

according to whether their remainders on division by 3 are 0, 1, or 2. The point is that when arithmetic is done modulo $n$ there are really only $n$ different numbers to deal with. This is because there are only $n$ possible remainders $0, 1, \ldots, n-1$ and by Lemma 13, $a \equiv \text{rem}(a, n) \bmod n$. We will see that because of this, modular arithmetic is a "simplification" of ordinary arithmetic.

The properties of congruence "$\equiv$" are very similar to the properties of equality "$=$", as we see in the next lemma.

**Lemma 14.** *The following hold for $n \geq 1$:*

(1) $a \equiv a \bmod n$

(2) $a \equiv b \bmod n$ *implies* $b \equiv a \bmod n$

(3) $a \equiv b \bmod n$ *and* $b \equiv c \bmod n$ *implies* $a \equiv c \bmod n$

(4) $a \equiv b \bmod n$ *implies* $a + c \equiv b + c \bmod n$

(5) $a \equiv b \bmod n$ *implies* $ac \equiv bc \bmod n$

(6) $a \equiv b \bmod n$ *and* $c \equiv d \bmod n$ *imply* $a + c \equiv b + d \bmod n$

(7) $a \equiv b \bmod n$ *and* $c \equiv d \bmod n$ *imply* $ac \equiv bd \bmod n$

*Proof.* (1) It is clear that $n|(a - a) = 0$, that is, $a \equiv a \mod n$.

Cases (2) and (3) follow immediately from Lemma 12.

For (4), assume $a \equiv b \bmod n$, that is, $n|a - b$. Now $(a + c) - (b - c) = a - b$ means that $n$ divides $(a + c) - (b + c)$ Therefore, $(a + c) \equiv (b + c) \bmod n$.

Let us suppose $a \equiv b \bmod n$ for (5). Now $ac - bc = c(a - b)$. Because $n$ divides $a - b$, the number $n$ divides also $ac - bc$. Thus, $ac \equiv bc \bmod n$.

To prove (6), assume

$$a \equiv b \bmod n \qquad \text{and} \qquad c \equiv d \bmod n.$$

Then by (4),

$$a + c \equiv b + c \bmod n \qquad \text{and} \qquad c + b \equiv d + b \bmod n.$$

Using (3), we get

$$a + c \equiv b + d \bmod n.$$

Case (7) can be proved similarly. □