# CSC265: Modular Arithmetic

## 1 Notation

For two integers $a$ and $q$, we use $q \mid a$ to denote that $q$ divides $b$. We use $a \bmod q$ to denote the remainder when dividing $a$ by $q$. I.e. $a \bmod q$ is the unique integer $r$ in $\mathbb{Z}_q = \{0, \ldots, q-1\}$ such that $a = kq + r$ for an integer $k = \lfloor a/q \rfloor$. We use $a \equiv b \pmod q$ to denote that $q \mid (a - b)$, or, equivalently that $a \bmod q = b \bmod q$. The "equation" $a \equiv b \pmod q$ is called a congruence. Notice that when $a, b \in \mathbb{Z}_q$, then $a \equiv b \pmod q$ implies $a = b$.

A prime number is a positive integer which is divisible by exactly two positive integers: 1 and itself. By convention 1 is not prime.

For some intuition, you can imagine $(a + b) \bmod q$ for $a, b \in \mathbb{Z}_q$ as going around a circle. Imagine a circle with $q$ equally spaced marks on it, labeled from 0 to $q-1$ clockwsise. Then $(a+b) \bmod q$ is the mark you get by starting from the mark $a$ and counting $b$ marks forward, i.e. clockwise. You can interprete $(a - b) \bmod q$ and $ab \bmod q$ similarly. Figure 1 illustrate $(4 + 5) \bmod 8 = 1$ this way.

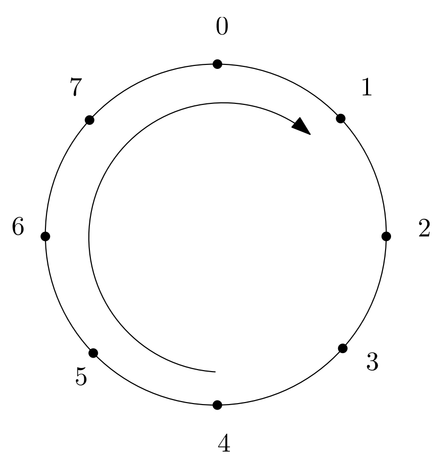


Figure 1: $(4 + 5) \bmod 8 = 1$

## 2 Greatest Common Divisor

The greatest common divisor of two non-negative integers $a$ and $b$, denoted $\gcd(a, b)$, is equal to the largest non-negative integer $g$ such that $g \mid a$ and $g \mid b$. The greatest common divisor can be computed very efficiently using Euclid's algorithm: in time linear in the number of bits needed to write $a$ and $b$.

The most important fact about the greatest common divisor is Bézout's identity: for any non-negative integers $a, b$, there exist (possibly zero or negative) integers $s, t$ such that

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

The integers $s$ and $t$ can also be computed efficiently using Euclid's algorithm.

Notice that if $p$ is a prime number then $\gcd(a, p) \in \{1, p\}$. Specifically, for any $a \in \mathbb{Z}_p$, $\gcd(a, p) = 1$.

## 3 Basic Properties of Modular Arithmetic

Assume we have the following congruences:

$$a \equiv b \pmod{q}$$
$$c \equiv d \pmod{q}$$

Then the following congruences also hold:

$$a + c \equiv b + d \pmod{q}$$
$$-a \equiv -b \pmod{q}$$
$$ac \equiv bd \pmod{q}$$

From these you can also derive many other equivalent congruences, e.g. $a - c \equiv b - d \pmod{q}$, etc.

Assume that $\gcd(a, q) = 1$. Then $q \mid (ab)$ implies $q \mid b$.

For any $a$ such that $\gcd(a, q) = 1$ there exists a unique $b \in \mathbb{Z}_q$ such that $ab \equiv 1 \pmod{q}$. We denote this $b$ by $a^{-1} \bmod q$. To see this, take $s$ and $t$ be such that $sa + tq = 1$, and let $b = s \bmod q$. Then, using $tq \equiv 0 \pmod{q}$,

$$ba \equiv sa \equiv sa + tq \equiv 1 \pmod{q}.$$

To show that this is the unique solution, assume towards contradiction that there is $y \in \mathbb{Z}_q, y \neq x$ such that $ay \equiv 1 \pmod{q}$. Then $a(x - y) \equiv 0 \pmod{q}$, i.e. $q \mid a(x - y)$. But $\gcd(a, q) = 1$, so $q \mid (x - y)$, i.e. $x \equiv y \pmod{q}$. But, since we assumed that $x, y \in \mathbb{Z}_q$, it must be that $x = y$, and we have reached a contradiction.

This implies also that, for any $a$ such that $\gcd(a, q) = 1$, and any integer $b$, there is a unique $x \in \mathbb{Z}_q$ such that $ax \equiv b \pmod{q}$. Namely, we can take $x = ((a^{-1} \bmod q)b) \bmod q$. The proof of uniqueness is analogous to the case $b = 1$ we addressed above.