# Chapter 4

# The Chinese Remainder Theorem

**The Monkey-Sailor-Coconut Problem** Three sailors pick up a number of coconuts, place them in a pile and retire for the night. During the night, the first sailor—wanting to make sure that he gets his fair share—gets up and takes 1/3 of the pile. The number of coconuts in the pile is not divisible by 3, there is 1 left over and he gives that coconut to the monkey. A little later, the second sailor gets up to do the same thing. He too finds that in order to take 1/3 of the pile, he needs to give one coconut to the monkey. Even later still, the third sailor gets up and does the same thing, giving 1 coconut to the monkey. In the morning the sailors gather to divide the remaining pile of coconuts evenly among the three of them. None would dare say anything about the size of the pile for fear of incriminating himself, and the monkey isn't talking, since he got 3 coconuts last night. When they divide the pile into 3 equal piles they find that they need to give the monkey 1 more coconut. What is the smallest number of coconuts with which they could have started and how many did each sailor get? We know the monkey got 4. [NOTE: $n = -2$ is, in some respects, the optimal solution but it has it physical drawbacks — especially if there is any interaction between the -2 anti-coconuts and coconuts. The implications for the future of the Universe are colossal.

This is actually a problem that has been passed down through many different cultures. It appears in Chinese manuscripts and Indian manuscripts in forms that are very much like the above problem. It appears in Chinese literature as early as the first century A.D. Sun-Tsu asked: Find a number which leaves the remainders 2,3,2 when divided by 3,5,7 respectively.

In order to solve this problem we need to recall quite a bit of mathematics.

A binary relation $\sim$ on a set $R$ is an equivalence relation if it satisfies the following conditions.

a) *Reflexive*: $a \sim a$ for all $a \in R$.

b) *Symmetric*: If $a, b \in R$ and $a \sim b$, then $b \sim a$.

c) *Transitive*: If $a, b, c \in R$ and if $a \sim b$ and $b \sim c$, then $a \sim c$.

When we have an equivalence relation, we can divide the set $R$ into equivalence classes $[a] = \{b \in R \mid b \sim a\}$. We are interested in the integers, $\mathbb{Z}$ and the equivalence relation $a \sim_n b$ if $n \mid (a - b)$, or if $a$ and $b$ have the same remainder when divided by $n$. The set of *congruence classes* modulo $n$ is denoted by $\mathbb{Z}_n$. Let's recall a few definitions from algebra.

## 4.1 Groups, rings and fields

Recall the following definitions.

**Definition 1** *A non-empty set $G$ together with an operation $\circ$, $(G, \circ)$, is a group if the following holds:*

1. $\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$
2. $\exists e \in G$ *such that* $\forall a \in G$, $a \circ e = e \circ a = a$
3. $\forall a \in G \, \exists A \in G$ *such that* $a \circ A = A \circ a = e$.

*A group $(G, \circ)$ is called commutative or Abelian if $a \circ b = b \circ a$ for all $a$, $b \in G$.*

**Example 4.1.1** $(\mathbb{Z}, +)$ is an Abelian group.

**Definition 2** *A set $R$ together with operations $+$ and $\cdot$ is a* ring *$(R, +, \cdot)$ if the following holds:*

1. $(R, +)$ *is a commutative group.*
2. $\forall a, b, c \in R \, a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3. $\exists \, I \in R$ *such that* $\forall a \in R$, $a \cdot I = I \cdot a = a$.
4. $\forall a, b, c \in R : \; a \cdot (a + b) = a \cdot b + a \cdot c$ *and* $(a + b) \cdot c = a \cdot c + b \cdot c$.

*A ring $(R, +, \cdot)$ is a* commutative *if $\forall a, b \in G$, $a \cdot b = b \cdot a$.*

**Example 4.1.2** $(\mathbb{Z}, +, \cdot)$ is a ring.

**Definition 3** *The characteristic of a ring $R$ is 0 if $nI \neq e$ for any positive integer $n$. Otherwise the characteristic is the smallest integer $m$ such that $mI = e$. Here $e$ and $I$ are the neutral elements of the operations $+$ and $\cdot$, respectively.*

**Example 4.1.3** Rational numbers form the ring $(\mathbb{Q}, +, \cdot)$. Let $M_{2,2}(\mathbb{Q})$ be the set of $2 \times 2$ matrices with rational coefficients. Let $+$ denote the addition of matrices and $\cdot$ the multiplication. Then $(M_{2,2}(\mathbb{Q}), +, \cdot)$ is a ring that is not commutative. This ring has characteristic 0.

**Definition 4** *Let $R$ and $S$ be rings. A map $\varphi : R \to S$ is a* ring homomorphism *if $\varphi(e_R) = e_S$, $\varphi(I_R) = I_S$, $\varphi(a + b) = \varphi(a) + \varphi(b)$ and $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ for all $a$, $b \in R$.*

**Example 4.1.4** Consider integers modulo 4, $\mathbb{Z}_4$ with the usual addition and multiplication. It is clear that $(\mathbb{Z}_4, +, \cdot)$ is a commutative ring. Since $1 + 1 + 1 + 1 = 0$ in $\mathbb{Z}_4$, $\mathbb{Z}_4$ has characteristic at most 4. The characteristic is actually exactly 4, as can be easily seen. The projection $\mathbb{Z} \to \mathbb{Z}_4$, which takes a number $n$ to its reminder under the division by 4, is a ring homomorphism.

**Definition 5** *A* field $F = (F, +, \cdot)$ *is a ring for which* $0 \neq 1$ *and whose every non–zero element has a multiplicative inverse.*

Observe that $(F, +, \cdot)$ is a field if and only if both $(F, +)$ and $(F, \cdot)$ are groups.
Which of the following are fields:

- $\mathbb{Z}_3$
- $\mathbb{Z}_4$
- $\mathbb{Z}$
- $\mathbb{Q}$
- $\mathbb{R}$

**Theorem 1** $(\mathbb{Z}_n, +, \cdot)$ *is a ring.* $(\mathbb{Z}_n, +, \cdot)$ *is a field if and only if* $n$ *is prime.*

Note that this distinction is important. When can we cancel, *i.e.*, when does $ca \cong cb \mod n$ imply that $a \cong b \mod n$?

**Theorem 2** *If* $ca \cong cb \mod n$, *then* $a \cong b \mod (n/d)$, *where* $d = \gcd(c, n)$.

**Corollary 1** *If* $ca \cong cb \mod n$ *and* $\gcd(c, n) = 1$, *then* $a \cong b \mod n$.

**Corollary 2** *If* $ca \cong cb \mod p$, $p$ *a prime, and* $p$ *does not divide* $c$, *then* $a \cong b \mod p$.

## 4.2 Linear Congruences

An equation of the form $ax \cong b( \mod n)$ is called a *linear congruence*. We will want to solve this equation for $x$.

**Theorem 3** *The linear congruence* $ax \cong b( \mod n)$ *has a solution if and only if* $d \mid b$, *where* $d = \gcd(a, n)$. *If* $d$ *does not divide* $b$, *then there are* $d$ *mutually incongruent solutions modulo* $n$.

If $d$ does not divide $b$ and if $x_0$ is a solution, then the $d$ incongruent solutions are given by

$$x_0,\ x_0 + n/d,\ x_0 + 2(n/d), \ldots,\ x_0 + (d-1)(n/d).$$

**Corollary 3** *If* $\gcd(a, n) = 1$, *then the linear congruence* $ax \cong b( \mod n)$ *has a unique solution modulo* $n$.

## 4.3 Chinese remainder theorem

Let $m$ and $n$ be relatively prime positive integers. Consider the system of congruences

$$x \equiv a \pmod{m} \tag{4.1}$$
$$x \equiv b \pmod{n} \tag{4.2}$$

Equivalently one may write

$$\texttt{irem}(x, m) = a \tag{4.3}$$
$$\texttt{irem}(x, n) = b \tag{4.4}$$

To solve these equations, observe first that both $\mathbb{Z}_m$ and $\mathbb{Z}_n$ are rings and also the product $\mathbb{Z}_m \times \mathbb{Z}_n$ is a ring. It is a finite ring having $mn$ elements.

Consider the mapping

$$\pi \colon \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n,\ s \mapsto (\texttt{irem}(s, m), \texttt{irem}(s, n)).$$

This mapping is a homomorphism of rings. Clearly $\pi(s) = (0, 0)$ if and only if $s$ is divisible by $mn$.

It follows that $\pi$ induces a one-to-one ring homomorphism

$$\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n,\ s \mapsto (\texttt{irem}(s, m), \texttt{irem}(s, n)).$$

Since $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ both have $mn$ elements, the above ring homomorphism must be onto. This means the the above equations have a solution for any $a$ and $b$. This is the *Chinese remainder theorem.*

**Theorem 4** *Let $m$ and $n$ be relatively prime positive integers. The system*

$$x \equiv a \pmod{m} \tag{4.5}$$
$$x \equiv b \pmod{n} \tag{4.6}$$

*has integer solutions for any integers $a$ and $b$. Moreover the solution is unique up to a multiple of $mn$ (i.e. as an element of $\mathbb{Z}_{mn}$ the solution is unique).*

In fact, the general Chinese Remainder Theorem holds for more than two equations:

**Theorem 5** *Let $n_1, n_2, \ldots, n_r$ be positive integers so that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences*

$$x \equiv a_1 \pmod{n_1} \tag{4.7}$$
$$x \equiv a_2 \pmod{n_2} \tag{4.8}$$
$$\vdots \tag{4.9}$$
$$x \equiv a_r \pmod{n_r} \tag{4.10}$$

*has a simultaneous solution, which is unique modulo $n_1 n_2 \ldots n_r$.*

The solution is given by taking $N_k = (n_1 n_2 \dots n_r)/n_k$ for $k = 1, 2, \dots r$. Since $\gcd(N_k, n_k) = 1$ there is a solution, $x_k$, to $N_k x \equiv 1 \mod n_k$. Then the solution is given by

$$\overline{x} = \sum_{i=k}^{r} a_k N_k x_k.$$

The problem posed by Sun-Tsu is

$$x \equiv 2 (\mod 3) \tag{4.11}$$
$$x \equiv 3 (\mod 5) \tag{4.12}$$
$$x \equiv 2 (\mod 7) \tag{4.13}$$

Then $N_1 = 35$, $N_2 = 21$, and $N_3 = 15$. We have to solve the congruences $35x \equiv 1 \mod 3$, $21x \equiv 1 \mod 5$, and $15x \equiv 1 \mod 7$. These solutions are $x_1 = 2$, $x_2 = 1$, and $x_3 = 1$. Thus,

$$x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 (\mod 105)$$

or $x \equiv 233 \equiv 23 \mod 105$.