12. The Chinese Remainder Theorem

**Theorem 1.** *(The Chinese Remainder Theorem)* Let $m$ and $n$ be relatively prime positive integers and $u$ and $v$ any integers. Then there exists a unique integer $x$ with $1 \leq x \leq mn$ such that

$$x \equiv u \pmod{m}, \text{ and } x \equiv v \pmod{n}.$$ 

**Example:** Let $m = 10$, $n = 11$, $u = 72$ and $v = 5943$. The Chinese Remainder Theorem says that there exists a unique integer $x$ between 1 and 110 such that $x \equiv 72 \pmod{10}$ and $x \equiv 5943 \pmod{11}$. Reducing $u$ and $v$, we want $x \equiv 2 \pmod{10}$ and $x \equiv 3 \pmod{11}$. By trial and error we can see that $x = 102$ works. (Note: there are methods for solving these equations besides trial and error!)

We’ll need the following Lemma:

**Lemma 2.** Let $m, n$ be positive integers such that $\gcd(m, n) = 1$. Suppose for integers $a, b$ we have $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$. Then $a \equiv b \pmod{mn}$.

**Proof.** We have $m$ and $n$ each divide $a - b$. So $a - b = mq$ for some $q \in \mathbb{Z}$. Then $n$ divides $mq$. Since $\gcd(m, n) = 1$, we have $m$ divides $q$, so $q = nt$ for some $t \in \mathbb{Z}$. Thus, $a - b = mq = mnt$, so $mn$ divides $a - b$. Hence, $a \equiv b \pmod{mn}$.

To prove the Chinese Remainder Theorem, we first introduce some notation. Let $m$ and $n$ be positive integers with $\gcd(m, n) = 1$. We’ll define two sets:

$$S_{mn} := \{0, 1, 2, \ldots, mn - 1\}$$

and

$$T_{m,n} := \{(a, b) \mid 0 \leq a \leq m - 1, \ 0 \leq b \leq n - 1\}.$$ 

**Example:** Suppose $m = 2$ and $n = 3$. Then

$$S_6 = \{0, 1, 2, 3, 4, 5, 6\}$$

and

$$T_{2,3} = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}.$$ 

Notice that $S$ and $T$ both have exactly $mn$ elements. This is easy to see for $S$. For $T$, think of the ordered pairs as lattice points in the plane $\mathbb{R}^2$. (A lattice point is just a point in $\mathbb{R}^2$ whose $x$- and $y$-coordinates are integers.) The points of $T$ form a grid or matrix having $m$ columns and $n$ rows. Thus, there are $mn$ lattice points in this grid.

We now define a function $f_{m,n}$ from $S_{mn}$ to $T_{m,n}$ as follows:

$$f_{m,n} : S \rightarrow T \quad \text{is defined by} \quad f_{m,n}(x) = (\ln(x, m), \ln(x, n)).$$

Let’s look at an example:
**Example:** Suppose $m = 2$ and $n = 3$. Let’s compute the function $f_{2,3}$ for every element of $S_6$:

- $f_{2,3}(0) = (\lnr(0, 2), \lnr(0, 3)) = (0, 0)$
- $f_{2,3}(1) = (\lnr(1, 2), \lnr(1, 3)) = (1, 1)$
- $f_{2,3}(2) = (\lnr(2, 2), \lnr(2, 3)) = (0, 2)$
- $f_{2,3}(3) = (\lnr(3, 2), \lnr(3, 3)) = (1, 0)$
- $f_{2,3}(4) = (\lnr(4, 2), \lnr(4, 3)) = (0, 1)$
- $f_{2,3}(5) = (\lnr(5, 2), \lnr(5, 3)) = (1, 2)$

Note that $f_{2,3}$ is one-to-one and onto. We wish to show this is always true:

**Theorem 3.** Let $m$ and $n$ be positive integers. If $\gcd(m, n) = 1$ then $f_{m,n} : S_{mn} \to T_{m,n}$ is both one-to-one and onto.

**Proof.** We first show that $f_{m,n}$ is one-to-one. Let $x, y$ be integers in the set $S_{mn}$ and suppose $f_{m,n}(x) = f_{m,n}(y)$. We want to show that $x = y$. We have $\lnr(x, m) = \lnr(y, m)$ and $\lnr(x, n) = \lnr(y, n)$. This means that $x \equiv y \pmod{m}$ and $x \equiv y \pmod{n}$. Since $\gcd(m, n) = 1$, we obtain $x \equiv y \pmod{mn}$. But since $0 \leq x, y \leq mn$, this implies that $x = y$. Thus, $f_{m,n}$ is one-to-one. Since $S_{mn}$ and $T_{m,n}$ have the same number of elements (namely, $mn$), $f_{m,n}$ must be onto as well.

We can now give a proof of the Chinese Remainder Theorem:

**Corollary 4.** *(The Chinese Remainder Theorem)* Let $m$ and $n$ be relatively prime positive integers and $u$ and $v$ any integers. Then there exists a unique integer $x$ with $1 \leq x \leq mn$ such that

$$x \equiv u \pmod{m}, \text{ and } x \equiv v \pmod{n}.$$

**Proof.** Let $S = S_{mn}$ and $T = T_{m,n}$. Let $r = \lnr(u, m)$ and $s = \lnr(v, n)$. Then $(r, s)$ is in the set $T$ and $u \equiv r \pmod{m}$ and $v \equiv s \pmod{n}$. Since the map $f_{m,n}$ is onto, we know that there exists an integer $x$ in the set $S$ such that $f_{m,n}(x) = (\lnr(x, m), \lnr(x, n)) = (r, s)$. Thus, $x \equiv r \pmod{m}$ and $x \equiv s \pmod{n}$. Thus, $x \equiv u \pmod{m}$ and $x \equiv v \pmod{n}$. Furthermore, there is only one $x$ in the set $S$ which works since $f_{m,n}$ is one-to-one.

Now we are going to restrict the function $f_{m,n}$ to a smaller domain. Let

$$S_{mn}^* := \{x \in S_{mn} \mid \gcd(x, m) = 1\}$$
$$T_{m,n}^* := \{(a, b) \in T_{m,n} \mid \gcd(a, m) = 1, \gcd(b, n) = 1\}.$$

So $S_{mn}^* \subset S_{mn}$ and $T_{m,n}^* \subset T_{m,n}$. Notice by definition of Euler’s $\phi$-function that $S_{mn}^*$ has $\phi(mn)$ elements and $T_{m,n}^*$ has $\phi(m)\phi(n)$ elements.

**Example:** Let $m = 3$ and $n = 4$. Then

$$S_{12}^* = \{1, 5, 7, 11\}$$
$$T_{3,4}^* = \{(1, 1), (1, 3), (2, 1), (2, 3)\}$$
Now define $f_{m,n}^*: S_{mn}^* \to T_{m,n}^*$ the same way we did before: for $x \in S_{mn}^*$ define

$$f_{m,n}^*(x) := (\lnr(x,m), \lnr(x,n)).$$

Here is a quick example when $m = 3$ and $n = 4$:

$$f_{3,4}^*(1) = (1, 1)$$
$$f_{3,4}^*(5) = (2, 1)$$
$$f_{3,4}^*(7) = (1, 3)$$
$$f_{3,4}^*(11) = (2, 3)$$

Notice that in this example that for all $x \in S_{12}^*$, $f_{3,4}^*(x) \in T_{3,4}^*$, not just in $T_{3,4}$. This is not a coincidence!

**Exercise**: Let $a, m \in \mathbb{Z}$ with $m > 0$. Prove that $\gcd(a, m) = 1$ if and only if $\gcd(\lnr(a, m), m) = 1$.

**Corollary 5.** Let $m$ and $n$ be positive integers and $x \in S_{mn}$. Then $f_{m,n}(x) \in T_{mn}^*$, if and only if $x \in S_{mn}^*$.

**Proof.** Let $f_{m,n}(x) = (a, b)$, where $a = \lnr(x, m)$ and $b = \lnr(x, n)$. Suppose first that $x \in S_{mn}^*$. Then $\gcd(x, mn) = 1$, which implies $\gcd(x, m) = 1$ and $\gcd(x, n) = 1$. By the Exercise above, this means $\gcd(a, m) = \gcd(x, m) = 1$ and $\gcd(b, n) = \gcd(x, n) = 1$. Thus, $(a, b) \in T_{m,n}^*$. Conversely, suppose $(a, b) \in T_{m,n}^*$. This means that $\gcd(a, m) = 1$ and $\gcd(b, n) = 1$. Again by the lemma above, we have that $\gcd(x, m) = 1$ and $\gcd(x, n) = 1$. Clearly, this implies $\gcd(x, mn) = 1$ and so $x \in S_{mn}^*$.

**Theorem 6.** Let $m$ and $n$ be relatively prime positive integers. Then $f_{m,n}^*: S_{mn}^* \to T_{m,n}^*$ is one-to-one and onto.

**Proof.** We will use the fact that the function $f_{m,n}: S_{mn} \to T_{m,n}^*$ is one-to-one and onto. Suppose $f_{m,n}^*(x) = f_{m,n}^*(y)$ for some $x, y \in S_{mn}^*$. Then certainly $f_{m,n}(x) = f_{m,n}(y)$. Since $f_{m,n}$ is one-to-one, we must have $x = y$. Thus, $f_{m,n}^*$ is also one-to-one.

Now let $(a, b) \in T_{m,n}^*$. As $(a, b) \in T_{m,n}^*$ and $f_{m,n}$ is onto, there exists an $x \in S_{mn}$ such that $f_{m,n}(x) = (a, b)$. But by the Corollary, this implies that $x \in S_{mn}^*$. Thus, $f_{m,n}^*$ is onto.

As an immediate corollary, we get the following:

**Corollary 7.** Let $m$ and $n$ be relatively prime positive integers. Then $\phi(mn) = \phi(m)\phi(n)$.

**Proof.** By the theorem above, since $f^*: S_{mn}^* \to T_{m,n}^*$ is one-to-one and onto, we have that $S_{mn}^*$ and $T_{m,n}^*$ have the same number of elements. But, by definition of the Euler $\phi$-function, the number of elements in $S_{mn}^*$ is $\phi(mn)$ and the number of elements in $T_{m,n}^*$ is $\phi(m)\phi(n)$. Therefore, $\phi(mn) = \phi(m)\phi(n)$.

Finally, we obtain our promised formula for the Euler $\phi$-function:

**Theorem 8.** Let $a = p_1^{m_1}p_2^{m_2} \cdots p_k^{m_k}$ be the prime factorization of $a$, where $p_1, \ldots, p_k$ are distinct primes. Then

$$\phi(a) = \phi(p_1^{m_1})\phi(p_2^{m_2}) \cdots \phi(p_k^{m_k}) = (p_1^{m_1} - p_1^{m_1-1})(p_2^{m_2} - p_2^{m_2-1}) \cdots (p_k^{m_k} - p_k^{m_k-1}).$$
Proof. We use induction on the number $k$ of primes in the prime factorization of $a$. Suppose $k = 1$. Then $a = p^n$ for some prime $p$. An integer between 1 and $p^n$ is relatively prime to $p^n$ if and only if it is not a multiple of $p$. Let’s count how many multiples of $p$ there are between 1 and $p^n$. Well, we can list all of them in an orderly way: $p$, $2p$, $3p$, ..., $(p^{n-1})p$. Counting, we see there are $p^{n-1}$ multiples of $p$ in this range. Thus, the number of integers from 1 to $p^n$ which are relatively prime to $p^n$ is $p^n - p^{n-1}$.

Now let’s assume $k > 1$ and we know theorem is true for positive integers with at most $k - 1$ distinct prime factors. Let $c = p_k^{m_k}$ and $b = p_1^{m_1} \cdots p_{k-1}^{m_{k-1}}$. Then $a = bc$ and gcd($b, c$) = 1. Further, the number of distinct primes in the factorizations for $b$ and $c$ are each less than $k$. Using the Corollary above, we have $\phi(a) = \phi(bc) = \phi(b)\phi(c) = \phi(b)\phi(p_k^{m_k})$. By our inductive hypothesis, we know $\phi(b) = \phi(p_1^{m_1}) \cdots \phi(p_{k-1}^{m_{k-1}})$. Thus,

$$\phi(a) = \phi(p_1^{m_1}) \cdots \phi(p_k^{m_k}).$$

This proves the first equality. By the $k = 1$ case, we know $\phi(p_i^{k_i}) = p_i^{k_i} - p_i^{k_i-1}$ for each $i$. Thus, the second equality holds also. $\square$

Homework:

1. Compute $\phi(43659)$.

2. Find the unique integer $x$ between 0 and 104 such that $x \equiv 1 \pmod{3}$, $x \equiv 3 \pmod{5}$ and $x \equiv 3 \pmod{7}$.

3. Let $p$ and $q$ be primes with $p > q$ and let $n = pq$. Find a formula for $p$ and $q$ in terms of $n$ and $\phi(n)$. (Hint: first show $p + q = n - \phi(n) + 1$ and $p - q = \sqrt{(p + q)^2 - 4n}$.)