Chapter 5

The Chinese Remainder Theorem

5.1 Coprime moduli

Theorem 5.1. *Suppose* $m, n \in \mathbb{N}$, *and*

$$\gcd(m, n) = 1.$$

Given any remainders $r \bmod m$ *and* $s \bmod n$ *we can find* N *such that*

$$N \equiv r \bmod m \text{ and } N \equiv s \bmod n.$$

Moreover, this solution is unique $\bmod mn$.

Proof. We use the pigeon-hole principle. Consider the mn numbers

$$0 \leq N < mn.$$

For each N consider the remainders

$$r = N \bmod m,\ s = N \bmod n,$$

where r, s are chosen so that

$$0 \leq r < m,\ 0 \leq s < n.$$

We claim that these pairs r, s are different for different $N \in [0, mn)$. For suppose $N < N'$ have the same remainders, ie

$$N' \equiv N \bmod m \text{ and } N' \equiv N \bmod n.$$

Then

$$m \mid N' - N \text{ and } n \mid N' - N.$$

Since $\gcd(m, n) = 1$, it follows that

$$mn \mid N' - N.$$

But that is impossible, since

$$0 < N' - N < mn.$$

□

Example: Let us find N such that

$$N \equiv 3 \bmod 13,\ N \equiv 7 \bmod 23.$$

One way to find N is to find a, b such that

$$\begin{aligned} a \equiv 1 \bmod m,\ a \equiv 0 \bmod n, \\ b \equiv 0 \bmod m,\ b \equiv 1 \bmod n. \end{aligned}$$

For then we can take

$$N = 3a + 7b.$$

Note that

$$a = 1 + sm = tn.$$

We are back to the Euclidean Algorithm for $\gcd(m, n)$:

$$\begin{aligned} 23 &= 2 \cdot 13 - 3, \\ 13 &= 4 \cdot 3 + 1, \end{aligned}$$

giving

$$\begin{aligned} 1 &= 13 - 4 \cdot 3 \\ &= 13 - 4(2 \cdot 13 - 23) \\ &= 4 \cdot 23 - 7 \cdot 13. \end{aligned}$$

Thus we can take

$$a = 4 \cdot 23 = 92,\ b = -7 \cdot 13 = -91.$$

giving

$$N = 3 \cdot 92 - 7 \cdot 91 = 276 - 637 = -361.$$

Of course we can add a multiple of mn to N; so we could take

$$N = 13 \cdot 23 - 361 = 299 - 361 = -62,$$

if we want the smallest solution (by absolute value); or

$$N = 299 - 62 = 237,$$

for the smallest positive solution.

5.2 The modular ring

We can express the Chinese Remainder Theorem in more abstract language.

Theorem 5.2. *If* $\gcd(m, n) = 1$ *then the ring* $\mathbb{Z}/(mn)$ *is isomorphic to the product of the rings* $\mathbb{Z}/(m)$ *and* $\mathbb{Z}/(n)$*:*

$$\mathbb{Z}/(mn) = \mathbb{Z}/(m) \times \mathbb{Z}/(n).$$

Proof. We have seen that the maps

$$N \mapsto N \bmod m \text{ and } N \mapsto N \bmod n$$

define ring-homomorphisms

$$\mathbb{Z}/(mn) \to \mathbb{Z}/(m) \text{ and } \mathbb{Z}/(mn) \to \mathbb{Z}/(n).$$

These combine to give a ring-homomorphism

$$\mathbb{Z}/(mn) \to \mathbb{Z}/(m) \times \mathbb{Z}/(n),$$

under which

$$r \bmod mn \mapsto (r \bmod m, r \bmod n).$$

But we have seen that this map is bijective; hence it is a ring-isomorphism. □

5.3 The totient function

Proposition 5.1. *Suppose* $\gcd(m,n) = 1$. *Then*

$$\gcd(N, mn) = \gcd(N, m) \cdot \gcd(N, n).$$

Proof. Let

$$d = \gcd(N, mn).$$

Suppose

$$p^e \parallel d.$$

Then

$$p^e \parallel m \text{ or } p^e \parallel n.$$

Thus the prime-power divisors of d are divided between m and n □

Corollary 5.1. *If* $\gcd(m,n) = 1$ *and* $N \in \mathbb{Z}$ *then*

$$\gcd(N, mn) = 1 \iff \gcd(N, m) = 1 \text{ and } \gcd(N, n) = 1.$$

From this we derive

Theorem 5.3. *Euler's totient function is multiplicative, ie*

$$\gcd(m,n) = 1 \implies \phi(mn) = \phi(m)\phi(n).$$

This gives a simple way of computing $\phi(n)$.

Proposition 5.2. *If*

$$n = \prod_{1 \le i \; er} p_i^{e_i},$$

where the primes $p_1, \ldots, p_r$ *are different and each* $e_i/ge1$. *Then*

$$\phi(n) = \prod p_i^{e_i - 1}(p_i - 1).$$

Proof. Since $\phi(n)$ is multiplicative,

$$\phi(n) = \prod_i \phi(p_i^{e_i}).$$

The result now follows from

Lemma 5.1. $\phi(p^e) = p^{e-1}(p-1)$.

Proof. The numbers $r \in [0, p^e)$ is *not* coprime to p^r if and only if it is divisible by p, ie

$$r \in \{0, p, 2p, \ldots, p^e - p\}.$$

There are

$$[p^e/p] = p^{e-1}$$

such numbers. Hence

$$\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1).$$

□

□

Example: Suppose $n = 1000$.

$$\begin{aligned}\phi(1000) &= \phi(2^3 5^3) \\ &= \phi(2^3)\phi(5^3) \\ &= 2^2(2-1)\ 5^2(5-1) \\ &= 4 \cdot 1 \cdot 25 \cdot 4 \\ &= 400;\end{aligned}$$

there are just 400 numbers coprime to 1000 between 0 and 1000.

5.4 The multiplicative group

Theorem 5.4. *If* $\gcd(m, n) = 1$ *then*

$$(\mathbb{Z}/mn)^\times = (\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times.$$

Proof. We have seen that the map

$$r \bmod mn \mapsto (r \bmod m, r \bmod n) : \mathbb{Z}/(mn) \to \mathbb{Z}/(m) \times \mathbb{Z}/(n)$$

maps r coprime to mn to pairs (r, s) coprime to m, n respectively. Thus the subset $(Z/mn)^\times$ maps to the product of the subsets $(\mathbb{Z}/m)^\times$ and $(\mathbb{Z}/n)^\times$, from which the result follows. □

In effect, this is an algebraic expression of the fact that the totient function is multiplicative.

5.5 Multiple moduli

The Chinese Remainder Theorem extends to more than two moduli.

Proposition 5.3. *Suppose $n_1, n_2, \ldots, n_r$ are pairwise coprime, ie*

$$i \neq j \implies \gcd(n_i, n_j) = 1;$$

and suppose we are given remainders $a_1, a_2, \ldots, a_r$ moduli $n_1, n_2, \ldots, n_r$, respectively. Then there exists a unique $N \bmod n_1 n_2 \cdots n_r$ such that

$$N \equiv a_1 \bmod n_1,\ N \equiv a_2 \bmod n_2, \ldots, N \equiv a_r \bmod n_r.$$

Proof. This follows from the same pigeon-hole argument that we used to establish the Chinese Remainder Theorem.

Or we can prove it by induction on r; for since

$$\gcd(n_1 n_2 \cdots n_i, n_{i+1}) = 1,$$

we can add one modulus at a time,

Thus if we have found N_i such that

$$N_i \equiv a_1 \bmod n_1,\ N_i \equiv a_2 \bmod n_2, \ldots, N_i \equiv a_i \bmod n_i$$

then by the Chinese Remainder Theorem we can find N_{i+1} such that

$$N_{i+1} \equiv N_i \bmod n_1 n_2 \cdots n_i \text{ and } N_{i+1} \equiv a_{i+1} \bmod n_{i+1}$$

and so

$$N_{i+1} \equiv a_1 \bmod n_1,\ N_{i+1} \equiv a_2 \bmod n_2, \ldots, N_{i+1} \equiv a_{i+1} \bmod n_{i+1},$$

establishing the induction. □

Example: Suppose we want to solve the simultaneous congruences

$$n \equiv 4 \bmod 5,\ n \equiv 2 \bmod 7,\ n \equiv 1 \bmod 8.$$

There are two slightly different approaches to the task.

Firstly, we can start by solving the first 2 congruences. As is easily seen, the solution is

$$n \equiv 9 \bmod 35.$$

The problem is reduced to two simultaneous congruences:

$$n \equiv 9 \bmod 35,\ n \equiv 1 \bmod 8,$$

which we can solve with the help of the Euclidean Algorithm, as before.

Alternatively, we can find solutions of the three sets of simultaneous congruences

$$\begin{aligned} n_1 &\equiv 1 \bmod 5,\ n_1 \equiv 0 \bmod 7,\ n_1 \equiv 0 \bmod 8, \\ n_2 &\equiv 0 \bmod 5,\ n_2 \equiv 1 \bmod 7,\ n_2 \equiv 0 \bmod 8, \\ n_3 &\equiv 0 \bmod 5,\ n_3 \equiv 0 \bmod 7,\ n_3 \equiv 1 \bmod 8, \end{aligned}$$

ie

$$n_1 \equiv 1 \bmod 5,\ n_1 \equiv 0 \bmod 56,$$
$$n_2 \equiv 1 \bmod 7,\ n_2 \equiv 0 \bmod 40,$$
$$n_3 \equiv 1 \bmod 8,\ n_3 \equiv 0 \bmod 35,$$

which we can solve by our previous method. The required solution is then

$$n = 4n_1 + 2n_2 + n_3,$$

where the coefficients 4,2,1 are the required residues.

5.6 Multiplicative functions

We have seen that $\phi(n)$ is multiplicative. There are several other multiplicative functions that play an important role in number theory, for example:

1. The number $d(n)$ of divisors of n, eg
$$d(2) = 1,\ d(12) = 3,\ d(32) = 5.$$
2. The sum $\sigma(n)$ of the divisors of n, eg
$$\sigma(2) = 3,\ \sigma(12) = 28,\ \sigma(32) = 63.$$
3. The Möbius function
$$\mu(n) = \begin{cases} (-1)^e & \text{if } n \text{ is square-free and has } e \text{ prime factors,} \\ 0 & \text{if } n \text{ has a square factor } n = p^2 m. \end{cases}$$
4. The function $(-1)^n$.
5. The function
$$\theta(n) = \begin{cases} 1 & \text{if } n \equiv 1 \bmod 4, \\ -1 & \text{if } n \equiv 3 \bmod 4, \\ 0 & \text{if } n \text{ is even.} \end{cases}$$

5.7 Perfect numbers

Definition 5.1. *We say that $n \in \mathbb{N}$ is* perfect *if it is the sum of all its divisors, except for n itself.*

In other words,

$$n \text{ is perfect } \iff \sigma(n) = 2n.$$

Theorem 5.5. *If $M(p) = 2^p - 1$ is prime then*

$$n = 2^{p-1} M(p)$$

is perfect. Moreover, every even *perfect number is of this form*

Remark: Euclid showed that every number of this form is perfect; Euler showed that every even perfect number is of this form.

Proof. Note that

$$\sigma(n) = n + 1 \iff n \text{ is prime.}$$

For if $n = ab$ (where $a, b > 1$) then $\sigma(n) \geq n + 1 + a$.

Also

$$\sigma(2^e) = 1 + 2 + 2^2 + \cdots + 2^e = 2^{e+1} - 1.$$

Thus if $n = 2^{p-1}M(p)$, where $P = M(p)$ is prime, then (since 2^e and $M(p)$ are coprime)

$$\begin{aligned}\sigma(n) &= \sigma(2^{p-1})\sigma(M(p)\\ &= (2^p - 1)(M(p) + 1)\\ &= (2^p - 1)(2^p)\\ &= 2n.\end{aligned}$$

Conversely, suppose n is an even perfect number. Let $n = 2^e m$, where m is odd. Then

$$\sigma(n) = \sigma(2^e)\sigma(m) = 2n,$$

ie

$$(2^{e+1} - 1)\sigma(m) = 2^{e+1}m.$$

Thus $2^{e+1} - 1 \mid m$, say

$$m = (2^{e+1} - 1)x.$$

Then

$$\sigma(m) = 2^{e+1}x = m + x.$$

But x is a factor of m. So if x is not 1 or m then

$$\sigma(m) \geq m + x + 1.$$

Hence $x = 1$ or m If $x = m$ then $2^{e+1} - 1 = 1 \implies e = 0$, which is not possible since n is even.

It follows that $x = 1$, so that

$$m = 2^{e+1} - 1 = M(e + 1).$$

Also

$$\sigma(m) = m + 1.$$

Thus $m = M(e + 1)$ is prime (and therefore $e + 1 = p$ is prime), and

$$n = 2^{p-1}M(p),$$

as stated. □

But what if n is odd? *It is not known if there are any odd perfect numbers.* This is one of the great unsolved problems of mathematics.