Contents

Chapter 6

The Chinese Remainder Theorem

6.1 Coprime moduli

Theorem 6.1. *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

$$0 \le N < mn.$$

For each N consider the remainders

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

where r, s are chosen so that

$$0 \le r < m, \; 0 \le s < n.$$

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

$$a \equiv 1 \bmod m, \; a \equiv 0 \bmod n,$$
$$b \equiv 0 \bmod m, \; b \equiv 1 \bmod n.$$

For then we can take

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

Note that

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

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

$$23 = 2 \cdot 13 - 3,$$
$$13 = 4 \cdot 3 + 1,$$

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.

6.2 The modular ring

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

Theorem 6.2. *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. □

6.3 The totient function

Proposition 6.1. *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 6.1. *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 6.3. *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 6.2. *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 6.1. $\phi(p^e) = p^{e-1}(p - 1)$.

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.

6.4 The multiplicative group

Theorem 6.4. *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.

6.5 Multiple moduli

The Chinese Remainder Theorem extends to more than two moduli.

Proposition 6.3. *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

$$\begin{aligned} n_1 \equiv 1 \bmod 5,\ n_1 \equiv 0 \bmod 56, \\ n_2 \equiv 1 \bmod 7,\ n_2 \equiv 0 \bmod 40, \\ n_3 \equiv 1 \bmod 8,\ n_3 \equiv 0 \bmod 35, \end{aligned}$$

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.

Exercise 6

In exercises 1–10 find the smallest simultaneous solution $n \geq 0$ of the given congruences, or else show that there is no such solution.

** 1. $n \equiv 1 \bmod 4,\ n \equiv 2 \bmod 7$

** 2. $n \equiv 2 \bmod 5,\ n \equiv 5 \bmod 8$

** 3. $n \equiv 2 \bmod 3,\ n \equiv 3 \bmod 4$

** 4. $n \equiv 2 \bmod 5,\ n \equiv 3 \bmod 7,\ n \equiv 1 \bmod 8$

** 5. $n \equiv 3 \bmod 4,\ n \equiv 5 \bmod 7,\ n \equiv 2 \bmod 9$

** 6. $n \equiv 1 \bmod 5,\ n \equiv 3 \bmod 6,\ n \equiv 2 \bmod 7$

** 7. $n \equiv 2 \bmod 4,\ n \equiv 4 \bmod 5,\ n \equiv 3 \bmod 7$

** 8. $n \equiv 2 \bmod 4,\ n \equiv 3 \bmod 6,\ n \equiv 4 \bmod 7$

** 9. $n \equiv 4 \bmod 7,\ n \equiv 6 \bmod 11,\ n \equiv 9 \bmod 11$

** 10. $n \equiv 1 \bmod 9,\ n \equiv 2 \bmod 10,\ n \equiv 3 \bmod 11$

*** 11. How many positive integers $x \leq 10,000$ are there such that the difference $2^x - x^2$ is not divisible by 7?

*** 12. Show that

$$\phi(n) \to \infty$$

as $n \to \infty$.

**** 13. Find an odd integer k such that $k \cdot 2^n - 1$ is composite for all $n \geq 1$.

**** 14. Is there a 9-digit number

$$N = d_1 d_2 \cdots d_9$$

with the following properties: the 9 digits are distinct, and for each $k \in [1, 9]$ the number

$$d_1 d_2 \ldots d_k$$

is divisible by k?