LECTURE 4: CHINESE REMAINDER THEOREM AND MULTIPLICATIVE FUNCTIONS

1. The Chinese Remainder Theorem

We now seek to analyse the solubility of congruences by reinterpreting their solutions modulo a composite integer m in terms of related congruences modulo prime powers.

Theorem 1.1 (Chinese Remainder Theorem)**.** *Let $m_1, \dots, m_r$ denote positive integers with $(m_i, m_j) = 1$ for $i \neq j$, and let $a_1, \dots, a_r \in \mathbb{Z}$. Then the system of congruences*

$$x \equiv a_i \pmod{m_i} \quad (1 \leqslant i \leqslant r) \tag{1.1}$$

is soluble simultaneously for some integer x. If x_0 is any one such solution, then x is a solution of (1.1) if and only if $x \equiv x_0 \pmod{m_1 m_2 \dots m_r}$.

Proof. Let $m = m_1 m_2 \dots m_r$, and $n_j = m/m_j$ $(1 \leqslant j \leqslant r)$. Then for each $j = 1, \dots, r$ one has $(m_j, n_j) = 1$, whence there exists an integer b_j with

$$n_j b_j \equiv 1 \pmod{m_j}.$$

Moreover,

$$n_j b_j = \left(\frac{m_1 \cdots m_r}{m_j m_i} b_j \right) m_i \equiv 0 \pmod{m_i}$$

whenever $i \neq j$. Then if we put

$$x_0 = n_1 b_1 a_1 + \cdots + n_r b_r a_r,$$

we find that

$$x_0 \equiv n_i b_i a_i \equiv a_i \pmod{m_i}$$

for $1 \leqslant i \leqslant r$. Thus we may conclude that x_0 is a solution of (1.1).

In order to establish uniqueness, suppose that x and y are any two solutions of (1.1). Then one has

$$x \equiv y \pmod{m_i}, \ \ 1 \leqslant i \leqslant r, \quad \text{and} \quad (m_i, m_j) = 1, \ \ i \neq j.$$

Then it follows that $x \equiv y \pmod{[m_1, \dots, m_r]}$. Since m_i's are coprime, $[m_1, \dots, m_r] = m_1 \dots m_r$. □

Example 1.2. Find the set of solutions to the system of congruences

$$4x \equiv 1 \pmod 3, \quad x \equiv 2 \pmod 5, \quad 2x \equiv 5 \pmod 7.$$

We first convert this into a form where the leading coefficients are all 1. Thus, multiplying the final congruence through by 4 (the multiplicative inverse of 2 modulo 7), we obtain the equivalent system

$$x \equiv 1 \pmod 3, \quad x \equiv 2 \pmod 5, \quad x \equiv 6 \pmod 7.$$

We next put $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, so that $(m_i, m_j) = 1$ for $i \neq j$. Define $m = 3 \cdot 5 \cdot 7 = 105$, and $n_1 = 105/3 = 35$, $n_2 = 105/5 = 21$, $n_3 = 105/7 = 15$. We compute integers b_j with $n_j b_j \equiv 1 \pmod{m_j}$ $(j = 1, 2, 3)$ by means of the Euclidean Algorithm (or directly, if the numbers are small enough). Thus we find that

$$35b_1 \equiv 1 \pmod 3 \Rightarrow 2b_1 \equiv 1 \pmod 3 \Rightarrow b_1 \equiv 2 \pmod 3,$$
$$21b_2 \equiv 1 \pmod 5 \Rightarrow b_2 \equiv 1 \pmod 5,$$
$$15b_3 \equiv 1 \pmod 7 \Rightarrow b_3 \equiv 1 \pmod 7.$$

So take

$$\begin{aligned} x_0 &= 35 \cdot 2 \cdot 1 + 21 \cdot 1 \cdot 2 + 15 \cdot 1 \cdot 6 \\ &= 70 + 42 + 90 = 202 \equiv 97 \pmod{105}. \end{aligned}$$

Then we find that $x_0 = 97$ satisfies the given congruences, and the complete set of solutions is given by $x = 97 + 105k$ $(k \in \mathbb{Z})$.

Example 1.3. Find the set of solutions, if any, to the system of congruences

$$x \equiv 1 \pmod{15}, \quad x \equiv 2 \pmod{35}.$$

In this example, the moduli of the two congruences are not coprime, since $(35, 15) = 5$. In order to determine whether or not the system is soluble, we therefore need to examine the underlying congruences, extracting as a modulus this greatest common divisor. Thus we find that any potential solution x of the system must satisfy

$$x \equiv 1 \pmod{15} \quad \Rightarrow \quad x \equiv 1 \pmod 3 \quad \text{and} \quad x \equiv 1 \pmod 5,$$

and at the same time

$$x \equiv 2 \pmod{35} \quad \Rightarrow \quad x \equiv 2 \pmod 5 \quad \text{and} \quad x \equiv 2 \pmod 7.$$

But then one has $x \equiv 1 \pmod 5$ and $x \equiv 2 \pmod 5$, two congruence conditions that are plainly incompatible. We may conclude then that there are no solutions of the simultaneous congruences $x \equiv 1 \pmod{15}$ and $x \equiv 2 \pmod{35}$.

2. Multiplicative functions

We wish to investigate further the properties of the Euler totient function, and so pause to introduce the concept of a multiplicative function.

Definition 2.1. (i) We say that a function $f : \mathbb{N} \to \mathbb{C}$ is an **arithmetical function**;
(ii) An arithmetical function f is said to be **multiplicative** if (a) f is not identically zero, and (b) whenever $(m, n) = 1$, one has $f(mn) = f(m)f(n)$;
(iii) An arithmetical function g is said to be **totally multiplicative** if for all natural numbers m and n, one has $g(mn) = g(m)g(n)$.

Note that if $f(n)$ is multiplicative, then necessarily one has $f(1) = 1$.

Theorem 2.2. *The function $\phi(n)$ is multiplicative. Thus, whenever $(m,n)=1$, one has $\phi(mn)=\phi(m)\phi(n)$. Moreover, if n has canonical prime factorisation $n=\prod_{i=1}^t p_i^{r_i}$, then*

$$\phi(n)=\prod_{i=1}^t p_i^{r_i-1}(p_i-1)=n\prod_{p|n}(1-1/p).$$

Proof. Let m and n be natural numbers with $(m,n)=1$. Let R_m and R_n be reduced residue systems modulo m and n respectively. Let us consider the set

$$R=\{an+bm:\ a\in R_m, b\in R_n\}.$$

We observe that if

$$an+bm\equiv a'n+b'm \pmod{mn}$$

for some $a,a'\in R_m$ and $b,b'\in R_n$, then $an\equiv a'n \pmod{m}$, and since $(n,m)=1$, $a\equiv a' \pmod{m}$, so that $a=a'$. Similarly, we also deduce that $b=b'$. Hence, all the numbers $an+bm$ with $a\in R_m$ and $b\in R_n$ are district, and $|R|=|R_m||R_n|$.

We claim that R is a reduced residue system modulo mn. This will immediately imply that $\phi(mn)=\phi(m)\phi(n)$. We note that the above argument already shows that

$$an+bm\not\equiv a'n+b'm \pmod{mn}$$

for $(a,b)\neq(a',b')\in R_m\times R_n$. Moreover, whenever $(a,m)=(b,n)=1$, one has

$$(an+bm,n)=(bm,n)=1 \quad\text{and}\quad (an+bm,m)=(an,m)=1,$$

whence $(an+bm,mn)=1$. Therefore, all $r\in R$ satisfy $(r,mn)=1$.

We next seek to establish that whenever $(c,mn)=1$, then there exist $a\in R_m$ and $b\in R_n$ with $c\equiv an+bm \pmod{mn}$. But $(m,n)=1$, so by the Euclidean Algorithm, there exist integers x and y with $xm+yn=1$. It is clear from this equation that $(x,n)=1$, so that $(cx,n)=1$. Hence there exists $a\in R_n$ satisfying $a\equiv cx \pmod{n}$. Similarly, $(y,m)=1$, $(cy,m)=1$, and there exists $b\in R_m$ satisfying $b\equiv cy \pmod{m}$. Then

$$an+bm\equiv(cx)n+(cy)m\equiv c \pmod{mn}.$$

This completes the proof that R is a reduced residue system modulo mn and establishes that the Euler ϕ-function is multiplicative.

In order to complete the proof of the theorem, we observe next that when p is a prime number, one has $\phi(p^r)=p^r-p^{r-1}$, since the total number of residues modulo p^r is p^r, of which precisely the p^{r-1} divisible by p are not reduced. In this way, the final assertions of the theorem follow by making use of the multiplicative property of ϕ. □

Useful properties of $\phi(n)$ that will be employed later stem easily from its multiplicative property. Before establishing one such property, we establish a general result for multiplicative functions.

Lemma 2.3. *Suppose that f is multiplicative, and define $g(n) = \sum_{d|n} f(d)$. Then g is a multiplicative function.*

Proof. Suppose that m and n are natural numbers with $(m, n) = 1$, and suppose that $d \mid mn$. Write $d_1 = (d, m)$ and $d_2 = (d, n)$. Then $d = d_1 d_2$ and $(d_1, d_2) = 1$. Thus we obtain

$$g(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) = \left(\sum_{d_1|m} f(d_1) \right) \left(\sum_{d_2|n} f(d_2) \right),$$

whence $g(mn) = g(m)g(n)$. This completes the proof that g is multiplicative. □

Corollary 2.4. *One has $\sum_{d|n} \phi(d) = n$.*

Proof. Observe that for each prime number p, and every natural number r, one has

$$\sum_{d|p^r} \phi(d) = \sum_{h=0}^{r} \phi(p^h) = 1 + \sum_{h=1}^{r} (p^h - p^{h-1}) = p^r.$$

Thus, owing to the multiplicative property of ϕ established in Theorem 2.2, it follows from Lemma 2.3 that $\sum_{d|n} \phi(d)$ is a multiplicative function, and when $n = \prod_{t=1}^{t} p_i^{r_i}$

$$\sum_{d|n} \phi(d) = \prod_{i=1}^{t} \left(\sum_{d|p^{r_i}} \phi(d) \right) = \prod_{i=1}^{t} p^{r_i} = n.$$

□

To conclude this section, we examine the set of solutions of a polynomial congruence.

Definition 2.5. Let $f \in \mathbb{Z}[x]$, and suppose that $r_1, \ldots, r_m$ is a complete residue system modulo m. Then we say that the **number of solutions** of the congruence $f(x) \equiv 0 \pmod{m}$ is the number of residues r_i with $f(r_i) \equiv 0 \pmod{m}$.

Theorem 2.6. *Suppose that $f \in \mathbb{Z}[x]$, and denote by $N_f(m)$ the number of solutions of the congruence $f(x) \equiv 0 \pmod{m}$. Then $N_f(m)$ is a multiplicative function of m, so that when $m = \prod_{t=1}^{t} p_i^{r_i}$,*

$$N_f(m) = \prod_{i=1}^{t} N_f(p^{r_i}).$$

Proof. Suppose that m_1 and m_2 are natural numbers with $m = m_1 m_2$ and $(m_1, m_2) = 1$. Let $\{r_1, \ldots, r_{m_1}\}$, $\{s_1, \ldots, s_{m_2}\}$ and $\{t_1, \ldots, t_m\}$ be complete residue systems modulo m_1, m_2 and m, respectively. Suppose that some t_k satisfies $f(t_k) \equiv 0 \pmod{m}$. Then there exist unique r_i and s_j with

$$t_k \equiv r_i \pmod{m_1} \text{ and } t_k \equiv s_j \pmod{m_2},$$

and they satisfy

$$f(r_i) \equiv 0 \pmod{m_1} \text{ and } f(s_j) \equiv 0 \pmod{m_2}.$$

Further, if t_k and t_ℓ satisfy

$$t_k \equiv t_\ell \equiv r_i \pmod{m_1} \text{ and } t_k \equiv t_\ell \equiv s_j \pmod{m_2},$$

then, by the Chinese Remainder Theorem $t_k \equiv t_\ell \pmod{m}$, so that $t_k = t_\ell$. Thus we have defined an injective map from the set of solutions modulo m to the set of pairs of solutions modulo m_1 and m_2.

In the other direction, whenever there exist residues r_i and s_j with

$$f(r_i) \equiv 0 \pmod{m_1} \text{ and } f(s_j) \equiv 0 \pmod{m_2},$$

then by the Chinese Remainder Theorem there exists unique t_k with

$$t_k \equiv r_i \pmod{m_1} \text{ and } t_k \equiv s_j \pmod{m_2},$$

so that

$$f(t_k) \equiv 0 \pmod{m_i},\ i = 1, 2.$$

But since $(m_1, m_2) = 1$, it follows that

$$f(t_k) \equiv 0 \pmod{m}.$$

There is therefore an injective map from pairs of solutions (r_i, s_j) modulo m_1 and m_2 respectively, to solutions modulo m.

Collecting together the above conclusions, we find that the solutions modulo m, and pairs of solutions modulo m_1 and m_2, are in bijective correspondence, whence $N_f(m) = N_f(m_1)N_f(m_2)$ whenever $(m_1, m_2) = 1$. The desired conclusion now follows on considering the prime factorisation of m. $\square$