Chapter 3
Counting Solutions of Congruences

In this chapter we shall use the results obtained in the preceding chapter to count solutions of certain linear and other congruences in \( s \) unknowns. By a solution of a congruence, with modulus \( r \), we mean a solution \((\text{mod } r)\), i.e., an ordered \( s \)-tuple of integers \((x_1, \ldots, x_s)\) that satisfies the congruence, with two \( s \)-tuples \((x_1, \ldots, x_s)\) and \((x'_1, \ldots, x'_s)\) that satisfy the congruence counted as the same solution if and only if \( x_i \equiv x'_i \pmod{r} \) for \( i = 1, \ldots, s \).

We shall count either all the solutions or all the solutions that are restricted in some way. For example, we might consider those solutions \((x_1, \ldots, x_s)\) such that \((x_i, r) = 1\) for \( i = 1, \ldots, s \).

We begin by counting the unrestricted solutions of the general linear congruence.

**Proposition 3.1.** The congruence

\[
n \equiv a_1 x_1 + \ldots + a_s x_s \pmod{r}
\]

has a solution if and only if

\[
d \mid n, \text{ where } d = (a_1, \ldots, a_s, r).
\]

If it does have a solution, then it has \( dr^{s-1} \) solutions.

**Proof.** The condition that \( d \mid n \) is certainly necessary for the congruence to have a solution.

P. J. McCarthy, *Introduction to Arithmetical Functions*
© Springer-Verlag New York Inc. 1986
On the other hand, suppose that $d \mid n$. We shall show, by induction on $s$, that the congruence has $dr^{s-1}$ solutions.

Suppose that $s = 1$. The congruence

$$\frac{n}{d} \equiv \frac{a_1}{d} x_1 \pmod{\frac{r}{d}}$$

has a unique solution $x_1$: hence $n \equiv a_1 x_1 \pmod{r}$ has exactly $d$ solutions, to wit, $x_1, x_1 + \frac{r}{d}, x_1 + 2\frac{r}{d}, \ldots, x_1 + (d - 1)\frac{r}{d}$.

Now suppose that $s > 1$ and that the assertion is true for linear congruences with $s-1$ unknowns. Let $e = (a_2, \ldots, a_s, r)$. Since $d = (a_1, e) \mid n$, the congruence $n \equiv a_1 x_1 \pmod{e}$ has $d$ solutions. Hence, in every complete residue system $(\pmod{r})$ there are $(r/e)d$ solutions of this congruence.

Let $x_1$ be a solution of $n \equiv a_1 x_1 \pmod{e}$ and consider the congruence

$$n - a_1 x_1 \equiv a_2 x_2 + \ldots + a_s x_s \pmod{r}.$$ 

Since $e \mid n - a_1 x_1$, it has $e r^{s-2}$ solutions. Therefore, the congruence with $s$ unknowns has $(r/e)dr^{s-2} = dr^{s-1}$ solutions.

Now consider the congruence

$$(*) \quad n \equiv x_1 + \ldots + x_s \pmod{r}.$$ 

We wish to count the solutions $\langle x_1, \ldots, x_s \rangle$ of this congruence for which the greatest common divisors $(x_i, r)$, $i = 1, \ldots, s$, are restricted in various ways. (See Exercise 3.1.)