6.C. The Chinese Remainder Theorem

We shall begin with the standard Long Division Property of the integers: *Let a and b be positive integers with $b \geq 2$. Then there are unique nonnegative integers q* (the quotient) *and r* (the remainder) *such that*

$$a \quad = \quad bq \ + \ r$$

where $0 \leq r < b$.

We may then state the Chinese Remainder Problem as follows:

Let $p, q \geq 2$ be relatively prime (no common divisors except ± 1), and let a and b be nonnegative integers. Find all positive integers n such that n leaves remainders of a and b after long division by p and q.

For example, we might take $p = 3$ and $q = 5$, with $a = 2$ and $b = 3$.

Congruences

The most efficient way of solving such problems involves the notion of *congruence* for integers.

Definition. Let $m \geq 2$ be an integer, and let u and v be arbitrary integers. Then u and v are said to be congruent modulo m, writteh $u \equiv v \ (m)$ if and only if $u - v$ is (evenly) divisible by m (with zero remainder). This concept has the following properties:

(1) If r is the remainder of u after long division by m, then $u \equiv r \ (m)$.

(2) If $0 \leq r_1 < r_2 < m$, then $r_1 \not\equiv r_2 \ (m)$.

(3) If $a \equiv b \ (m)$ then $b \equiv a \ (m)$.

(4) If $a \equiv b \ (m)$ and $b \equiv c \ (m)$, then $a \equiv c \ (m)$.

(5) If $a \equiv a' \ (m)$ and $b \equiv b' \ (m)$, then $a + b \equiv a' + b' \ (m)$ and $ab \equiv a'b' \ (m)$.

(6) If c is relatively prime to m, then there is a positive integer d such that $dc \equiv 1 \ (m)$.

The last property is particularly important for the Chinese Remainder Problem, for it implies that we can find integers d and k such that $cd = 1 + km$. For small values of m and c one can often find d and k by trial and error. For example, if $m = 20$ and $c = 7$, then we can take $d = 3$. Similarly, if $m = 7$ and $c = 5$, then we can take $d = 3$, and if $m = 5$ and $c = 7$, then we can take $d = 4$. We shall begin by looking at examples of c, m where it is easy to find d, and at the end we shall discuss the general method for finding d in more complicated cases.

Simple examples

1. In the setting of the preceding paragraph, find d if $m = 7$ and $c = 6$, likewise if $m = 6$ and $c = 7$.

SOLUTION. We have $d = 6$ in the first case and $d = 7$ in the second (verify these claims).■

2. The example at the beginning of this document can be rewritten to ask for all integers n such that $n \equiv 2 \ (3)$ and $n \equiv 3 \ (5)$.

SOLUTION. We are interested in finding all integers of the form $3p + 2$ such that $3p + 2 \equiv 3 \ (5)$. Subtracting 2 from each side we obtain the equivalent congruence $3p \equiv 1 \ (5)$, and $p = 2$ is one solution. More generally, every integer $p = 5k + 2$ is a solution and this yields all solutions. Therefore the solutions to the original system are given by integers of the form

$$n \quad = \quad 3 \cdot (5k+2) \; + \; 2 \quad = \quad 15k \; + \; 8$$

and conversely it is easy to verify that each integer of this form solves the original problem. Therefore we may write the solution in the form $n \equiv 8\ (15)$.■

3. Suppose we modify the example to add a third condition: Find all integers n such that $n \equiv 2\ (3)$, $n \equiv 3\ (5)$, and $n \equiv 5\ (7)$.

SOLUTION. One begins by solving the problem with the first two conditions, which yields $n \equiv 8\ (15)$, and proceeding to solve a problem involving the result of the first step plus the third condition $n \equiv 5\ (7)$. To complete the final step we need to find all solutions of the congruence $15k + 8 \equiv 5\ (7)$.

The congruence in the preceding sentence can be rewritten in the form $k+1 \equiv 5\ (7)$, and from this we see that $k \equiv 4\ (7)$ or $k = 7m + 4$. Therefore the general solution has the form

$$n = 15k \; + \; 8 \quad = \quad 15(7m+4) \; + \; 8 \quad = \quad 105m \; + \; 68$$

or equivalently $n \equiv 68\ (105)$. Obviously we can handle systems of four or more congruences similarly, provided that the numbers by which we divide are pairwise relatively prime.■

4. Find all integers n such that $n \equiv 7\ (8)$ and $n \equiv 3\ (9)$.

SOLUTION. We need to find all solutions to $8p + 7 \equiv 3\ (9)$. This reduces to $8p \equiv \ -4 \equiv 5\ (9)$. Now $8 \cdot 8 \equiv 1\ (9)$, so the last congruence implies that $p \equiv 8 \cdot 8p \equiv 8 \cdot 5 \equiv 4\ (9)$. Therefore $p = 9q+4$, so that

$$n \quad = \quad 8(9q+4) \; + \; 7 \;\; 72q \; + \; 39$$

or $n \equiv 39\ (72)$.■

5. Find all integers n such that $n \equiv 13\ (27)$ and $n \equiv 7\ (16)$.

SOLUTION. We need to find all solutions to $27p+13 \equiv 7\ (16)$. This reduces to $27p \equiv -6 \equiv 10\ (16)$, and we may rewrite this as $11p \equiv 10\ (16)$. Now $11 \cdot 3 = 33 \equiv 1\ (16)$, so we have

$$p \quad \equiv \quad 3 \cdot 11p \quad \equiv \quad 30 \quad \equiv \quad 14\ (16)$$

so that $n = 27(16q + 14) + 13 \;\; = \;\; 432q + 391$, or equivalently $n \equiv 391\ (432)$.■

Solving $cd \equiv 1\ (m)$ systematically

In the preceding examples we were fortunate enough to be able to solve the congruence problem by trial and error for suitable choices of c and m. Obviously we need something which is more reliable, particularly if we are given more complicated problems. Specifically, we need the following:

THEOREM. *Suppose that a and b are relatively prime positive integers greater than* 1. *Then there exist integers s and t such that $sa + tb = 1$. In fact, we can always find a pair of such integers for which s is positive.*

Proof. The process of finding s and t is called the *Euclidean algorithm*; not surprisingly, it appears in Euclid's *Elements*. Let's suppose that $a > b$. Then by long division we may write $a = bq_1 + r_1$

where $0 < r_1 < b$; we know that the remainder is positive because a and b are relatively prime. We now recursively define integers q_i and r_i as follows until we reach an integer k such that $r_{k+1} = 0$:

$$\begin{array}{lcl}
b & = & r_1 q_2 \ + \ r_2 \ , \quad \text{where} \quad 0 \ < \ r_2 \ < \ r_1 \\
r_1 & = & r_2 q_3 \ + \ r_3 \ , \quad \text{where} \quad 0 \ < \ r_3 \ < \ r_2 \\
\cdots & & \\
r_{k-2} & = & r_{k-1} q_k \ + \ r_k \ , \quad \text{where} \quad 0 \ < \ r_k \ < \ r_{k-1} \\
r_{k-1} & = & r_k q_{k+1} \ + \ 0
\end{array}$$

In other words, r_k is the last positive remainder in the sequence. Let's define $r_0 = b$ and $r_{-1} = a$ because that will allow us to add $a = bq - 1 = r_1$ at the top of this list and express all the equations with uniform notational conventions.

A recursive argument now shows that each remainder r_j (where $-1 \leq j \leq k$) can be written in the form $s_j a + t_j b$ for suitable integers s_j, t_j, and furthermore a backward recursive argument shows that r_k divides each remainder r_j (where $k \geq j \geq -1$). The first of these shows that $r_k = sa + tb$, while the second shows that r_k divides $a = r_{-1}$ and $b = r_0$. Since a and b are relatively prime, it follows that r_k must be equal to 1.

To complete the proof we only need to show that we can choose s, t such that $s > 0$. To see this, start by writing $1 = s^* a + t^* b$ for some integers s^*, t^*. If $s^* > 0$ we are done, but if not we can find some positive integer K such that $s = s^* + Kb$ is positive (write $-s^* = ub + v$ where $0 \leq v < b$, so that $0 = ub + v + s^* < (u+1)v + s^*$). If we now take $t = t^* - Ka$ then it follows that $sa + tb = 1$.■

EXAMPLE. Suppose that $a = 77$ and $b = 52$. Then we obtain the following sequence of long divisions:

$$\begin{array}{lcl}
77 & = & 52 \cdot 1 \ + \ 25 \\
52 & = & 25 \cdot 2 \ + \ 2 \\
25 & = & 2 \cdot 12 \ + \ 1
\end{array}$$

In the notation of the display we have

$$r_{-1} \ = \ a \ = \ 77, \quad r_0 \ = \ b \ = \ 52 \ , \quad r_1 \ = \ 25 \ , \quad r_2 \ = \ 2, \quad r_3 = 1$$

$$q_1 \ = \ 1 \ , \quad q_2 \ = \ 2 \ , \quad q_3 \ = \ 12 \ .$$

We also have the recursive relation $r_{j-2} - r_{j-1} q_j \ = \ r_j$ for all $j \geq 1$, and this yields the following chain of identities:

$$25 \ = \ r_1 \ = \ 77 \cdot 1 \ + \ 52 \cdot (-1)$$

$$2 \ = \ r_2 \ = \ r_0 \ - \ q_2 r_1 \ = \ 52 \ - \ 2 \cdot (77 \cdot 1 \ + \ 52 \cdot (-1)) \ = \ 52 \cdot 3 \ + \ 77 \cdot (-2)$$

$$1 \ = \ r_3 \ = \ r_1 - q{-}3 r_2 \ = \ (77 \cdot 1 \ + \ 52 \cdot (-1)) \ - \ 12 \cdot (52 \cdot 3 \ + \ 77 \cdot (-2)) \ = \ 77 \cdot 25 \ + \ 52 \cdot (-37)$$

We can check the accuracy of these calculuations by computing the products $77 \times 25 = 1925$ and $52 \times 37 = 1924$. Thus we have shown that $24 \times 77 \equiv 1$ (52) and also $37 \times 52 \equiv -1$ (77), which is equivalent to $1 \equiv -37 \times 52 \equiv 40 \cdot 52$ (77).■

STILL MORE EXAMPLES

Here are some more examples.

Problem 6. Find all integers n such that $n = 5p + 2$ and $n = 7q + 5$ where p and q are integers.

SOLUTION. We need to find p such that $5p + 2 \equiv 5$ modulo 7, which is equivalent to $5p \equiv 3$ (7). To proceed, we need to find y such that $5y \equiv 1$ (7); we can do this easily because $5 \cdot 3 = 14 + 1$. Therefore we have $p \equiv 15p = 3 \cdot 5p \equiv 3 \cdot 3 \equiv 2$ (7) so that $p = 7z + 2$ for some z and $n = 5(7z + 2) + 2 = 35z + 10 + 2 = 35z + 12$.■

Problem 7. Find all integers n such that $0 < n < 200$ and n can be written as $n = 11p + 6$ and $n = 17q + 8$ where p and q are integers.

SOLUTION. We need to find p such that $11p+6 \equiv 8$ modulo 17, which is equivalent to $11p \equiv 2$ (17). To proceed, we need to find y such that $11y \equiv 1$ (17); we can do this easily because $11 \cdot -3 = -34 + 1 = (-2) \cdot 17 + 1$. Multiplying the congruence on the first line by -3, we find that

$$p \quad \equiv \quad -33p \quad \equiv \quad (-3) \cdot 11p \quad \equiv \quad (-3) \cdot 2 \quad \equiv \quad -6$$

mod 17, so that $p = 17w + 11$ for some w. Substituting in this value, we obtain

$$n \quad = \quad 11(17w + 11) \ + \ 6 \quad = \quad 187w \ + \ 121 \ + \ 6 \quad = \quad 187w \ + \ 127 \ .$$

By construction $n \equiv 6$ (11) and the other congruence follows because $127 = (9 \cdot 17) + 8$. Since $187w + 127$ is not between 0 and 200 if $w \neq 0$, it follows that $n = 127$ is the only solution.■