HW3 Solutions

1.89 Consider the congruence $ax \equiv b \bmod m$ when $\gcd(a, m) = d$. Show that $ax \equiv b \bmod m$ has a solution if and only if $d \mid b$.

Solution. If x_0 is a solution of $ax \equiv b \bmod m$, then $ax_0 - b = my$ for some integer y. Now $a = da'$ and $m = dm'$, by hypothesis, and so $da'x_o - b = dm'y$. It follows that $d \mid b$.

Conversely, suppose that $b = db'$. Then the congruence is

$$da'x \equiv db' \bmod dm'.$$

Note that $(a', m') = (a/d, m/d) = 1$, because d is the gcd (a, m). Therefore, the congruence $a'x \equiv b' \bmod m'$ has a solution, say, u, and hence du is a solution of the original congruence.

1.92 Find the smallest positive integer which leaves remainder 4, 3, 1 after dividing by 5, 7, 9, respectively.

Solution. That the desired integer x satisfies three congruences:

$$x \equiv 4 \bmod 5; \quad x \equiv 3 \bmod 7; \quad x \equiv 1 \bmod 9.$$

By the Chinese remainder theorem, the first two congruences give

$$x \equiv 24 \bmod 35.$$

Now use the Chinese remainder theorem for the system

$$x \equiv 24 \bmod 35$$
$$x \equiv 1 \bmod 9$$

(which is possible because $(35, 9) = 1$. We obtain $x \equiv 199 \bmod 315$. Thus, 199 is the smallest such solution.

1.97 On a desert island, five men and a monkey gather coconuts all day, then sleep. The first man awakens and decides to take his share. He divides the coconuts into five equal shares, with one coconut left over. He gives the extra one to the monkey, hides his share, and goes to sleep. Later, the second man awakens and takes his fifth from the remaining pile; he too finds one extra and gives it to the monkey. Each of the remaining three men does likewise in turn. Find the minimum number of coconuts originally present.

Solution. Here are the equations arising from the story. Let C be the number of coconuts.

$$C = 5a + 1 \tag{1}$$
$$4a = 5b + 1 \tag{2}$$
$$4b = 5c + 1 \tag{3}$$
$$4c = 5d + 1 \tag{4}$$
$$4d = 5e + 1 \tag{5}$$

We work from the bottom up. Since $4d$ occurs in the last equation and $5d$ occurs in equation (4) above it, rewrite the latter as

$$16c = 5 \cdot 4d + 4.$$

Hence,

$$16c = 5 \cdot (5e + 1) + 4 = 25e + 9.$$

Now go up to the next equation (3), which we multiply by 16:

$$64b = 5(16c) + 16 = 5(25e + 9) + 16 = 125e + 61.$$

Go up again after multiplying by 64:

$$256a = 5(64b) + 64 = 5(125e + 61) + 64 = 625e + 369.$$

Finally, multiply equation (1) by 256 to get

$$256C = 5(256a) + 256 = 5(625e + 369) + 256 = 3125e + 2101.$$

Thus,

$$256C \equiv 2101 \bmod 3125.$$

Were the hint, "Try -4 coconuts," not given, one would proceed to solve this congruence, taking note of the fact that $(256, 3125) = 1$. But $C = -4$ is a solution of this congruence, and so $C \equiv -4 \bmod 3125$; that is, every number of the form $3125k - 4$ is a solution. The minimum value for C is thus 3121 coconuts.