SKETCH OF SOLUTIONS (HOMEWORK V)

4.- a) $37 \mod 187$, b) $23 \mod 30$

12.- We have to solve the system:

$$x \equiv 1 \mod 2 \tag{1}$$
$$x \equiv 2 \mod 3 \tag{2}$$
$$x \equiv 3 \mod 4 \tag{3}$$
$$x \equiv 4 \mod 5 \tag{4}$$
$$x \equiv 5 \mod 6 \tag{5}$$
$$x \equiv 0 \mod 7 \tag{6}$$

We *can not* use the Chinese remainder theorem directly since the moduli are not relatively prime. If we solve the system involving equations (2), (3), (4) and (6) the answer is $119 \mod 420$. Notice that this also solves the first and fifth congruences.

22.- The system we must solve is:

$$x \equiv 3 \mod 17 \tag{7}$$
$$x \equiv 10 \mod 16 \tag{8}$$
$$x \equiv 0 \mod 15 \tag{9}$$

Using the Chinese remainder theorem we get $x = 3930$

24.- Take a set of numbers (each < 100) whose product is greater than the product of 784 and 813 and such that they are pairwise relatively prime. And use the Chinese remainder theorem. Example: Take $97, 98, 99$, and let $x = 784$, $y = 813$ then:

$$\begin{array}{rclcrcl} x & \equiv & 8 \mod 97 & & y & \equiv & 37 \mod 97 \\ x & \equiv & 0 \mod 98 & & y & \equiv & 29 \mod 98 \\ x & \equiv & 91 \mod 99 & & y & \equiv & 21 \mod 99 \end{array}$$

Using the Chinese remainder theorem we solve the equations

$$\begin{array}{rclclcrclcl} x+y & \equiv & 8+37 & \equiv & 45 \mod 97 & & xy & \equiv & 8*37 & \equiv & 5 \mod 97 \\ x+y & \equiv & 0+29 & \equiv & 29 \mod 98 & & xy & \equiv & 0*29 & \equiv & 0 \mod 98 \\ x+y & \equiv & 91+21 & \equiv & 13 \mod 99 & & xy & \equiv & 91*21 & \equiv & 30 \mod 99 \end{array}$$

Therefore $x + y = 1597$ and $xy = 637392$

Section 4.4

1.- a) $x = 1, 2$ b) $x = 8, 37$ c) $x = 132, 211$ (assuming the equation is $x^2 + 4x + 2 = 0$ the solution is $106, 233$)

10.- Three, namely: $6, 51$ and 123

Section 4.5

2.- a) $y = n, x = 6 + 2n$ b) no solutions

4.-

$$\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}$$

8.- b)

$$\begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix}$$

14.- Let k and l be integers between 0 and $n^2 - 1$. Suppose that they fall into the same entry (i, j) of the matrix. Then we have:

$$\begin{aligned} a + ck + e[k/n] &\equiv a + cl + e[l/n] \mod n \\ b + dk + f[k/n] &\equiv b + dl + f[l/n] \mod n \end{aligned} \tag{10}$$

This system is equivalent to:

$$\begin{aligned} c(k-l) + e([k/n] - [l/n]) &\equiv 0 \mod n \\ c(k-l) + e([k/n] - [l/n]) &\equiv 0 \mod n \end{aligned}$$

Since the matrix

$$\begin{pmatrix} c & e \\ d & f \end{pmatrix}$$

has determinant $cf - de$ which by hypothesis is relatively prime to n there is exactly one solution to the system, namely $(0, 0)$. Therefore $k \equiv l \mod n$ and $[k/n] \equiv [l/n] \mod n$ Since $0 \leq k, l \leq n^2 - 1$ we must have $0 \leq k/n, l/n \leq n - 1/n$ Thus $|k - l| < n$. Then, since $k \equiv l \mod n$ we have that $k = l$