MAT 311: Number Theory
Spring 2006

HW4 - Solutions

1. (Davenport, pp.217, ex. 2.03) We aim to find the smallest positive integer which leaves remainders $1, 2, \dots, 9$ respectively when divided by $2, 3, \dots, 10$. Stating it in the language of congruences, this amounts to solving

$$\begin{array}{rcll} x & \equiv & 1 & \text{mod } 2 \\ x & \equiv & 2 & \text{mod } 3 \\ \dots & & \dots & \\ x & \equiv & 9 & \text{mod } 10. \end{array}$$

For aesthetical reasons we prefer to write the above congruences as:

$$\begin{array}{rcll} x & \equiv & -1 & \text{mod } 2 \\ x & \equiv & -1 & \text{mod } 3 \\ \dots & & \dots & \\ x & \equiv & -1 & \text{mod } 10. \end{array}$$

This system of equations indeed has an obvious solution $\text{lcm}(2, 3, \dots, 10) - 1 = 2519$. This is the smallest positive solution, because any two solutions x, y differ by a multiple of $\text{lcm}(2, 3, \dots, 10)$, (because then we would have $x \equiv y \mod 2, 3, \dots, 10$, so $x - y$ is divisible by any number which is divisible by all of $2, 3, \dots, 10$).

Alternatively, one could use the fact that the congruence $a \equiv b \mod dm$ implies $a \equiv b \mod m$ in order to reduce this system to the case where the moduli are mutually coprime (for instance, the congruence $x \equiv -1 \mod 5$ is redundant because $x \equiv -1 \mod 10$ already implies that).

2. (Davenport, p.217, ex.2.04) We want to solve the congruence $97x \equiv 13 \mod 105$. Since 105 and 97 are coprime, we know that the system has indeed a (unique) solution $\mod 105$. By euclidian algorithm, it is easy to see that $-12 \cdot 105 + 13 \cdot 97 = 1$. Taking this modulo 105, we see that $97 \cdot 13 \equiv 1 \mod 105$. Thus, multiplying the given congruence above by 13, gives $97 \cdot 13 \cdot x \equiv 13 \cdot 13 \mod 105 \Rightarrow x \equiv 169 \equiv 64 \mod 105$.

3. Using the Chinese remainder theorem, explain (only) how to add and how to multiply 784 and 813 on a computer with word size 100: There are several ways of doing this. Choose sufficiently many *mutually coprime* moduli whose product exceeds $784 \cdot 813$. It is up to you how to choose those moduli (as long as they are mutually coprime). If you like working with large moduli, you may take 99, 98, 97. Note that they are mutually coprime and their product is (by inspection) greater than $784 \cdot 813$ (think like this: $784 \cdot 813 << 1000 \cdot 1000 = 10^6$, but $99 \cdot 98 \cdot 97$ is *closer* to $100 \cdot 100 \cdot 100 = 10^6$). Next, find the remainders of 784 and 813 modulo 99, 98, 97. An easy calculation shows:

$$\begin{array}{lcll lcll c lcll} 784 & \equiv & 91 & \text{mod } 99 & 813 & \equiv & 21 & \text{mod } 99 & \Rightarrow & 784 \cdot 813 & = & 30 & \text{mod } 99 \\ 784 & \equiv & 0 & \text{mod } 98 & 813 & \equiv & 29 & \text{mod } 98 & \Rightarrow & 784 \cdot 813 & = & 0 & \text{mod } 98 \\ 784 & \equiv & 8 & \text{mod } 97 & 813 & \equiv & 37 & \text{mod } 97 & \Rightarrow & 784 \cdot 813 & = & 5 & \text{mod } 97. \end{array}$$

Since the moduli are mutually coprime, the Chinese remainder theorem gives us an algorithm to find the (unique) number congruent to $784 \cdot 813$ modulo $99 \cdot 98 \cdot 97$. Since $99 \cdot 98 \cdot 97 > 784 \cdot 813$, the number we find must be indeed $784 \cdot 813$.

You can do the same method with smaller moduli (but, then of course you have to take a lot more moduli so that their product exceed $784 \cdot 813$).

Calculation of $784 + 813$ via Chinese remainder theorem is similar.