Math 580/780I Notes 9

Supplement on Calculating Inverses:

- **Basic Thoughts:** One reason to use the Chinese Remainder Theorem in certain problems is that it allows you to take advantage of using smaller moduli in your work. For this reason, it is good to know how to compute inverses for smaller moduli. We describe three approaches here. In each case, we are interested in computing an $x \in \mathbb{Z}$ such that $ax \equiv 1 \pmod{n}$, where a and n are given integers with $n > 1$. Further, we suppose $\gcd(a, n) = 1$, since otherwise an inverse for a (that is, an x satisfying $ax \equiv 1 \pmod{n}$) will not exist.

- **Approach 1: Exhausting the Possibilities.** Under the conditions above, there is an inverse $x \in \{1, 2, \ldots, n-1\}$. Furthermore, the x is unique (that is, there is exactly one such x). Try each such x one at a time until you get one that satisfies $ax \equiv 1 \pmod{n}$.

- **Approach 2: Focusing on the Moduli.** Instead of looking at multiples of a (numbers of the form ax), look at multiples of n (numbers of the form kn). For $k = 1, 2, 3, \ldots$, consider $kn + 1$. If $kn + 1$ is divisible by a, then let $x = (kn + 1)/a$ so that $ax = kn + 1 \equiv 1 \pmod{n}$.

- **Approach 3: Negatives Playing a Positive Role.** Proceed as in Approach 2, except consider both $kn + 1$ and $kn - 1$. If $kn + 1$ is divisible by a, do the same as before. If $kn - 1$ is divisible by a, then let $x = -(kn - 1)/a$ so that $ax = -(kn - 1) \equiv 1 \pmod{n}$.

- **What works best?** You should do what you feel comfortable with, but there is a reason for mentioning Approach 2 and Approach 3. We know $ax \equiv 1 \pmod{n}$ has a solution (since we are considering the case that $\gcd(a, n) = 1$). If x is the smallest positive solution that you get from Approach 1, then $ax \leq a(n-1)$. So in Approach 2, we can find k so that

$$kn + 1 = ax \leq a(n-1) < an \implies k < a.$$

Moreover, note that $kn + 1 = ax$ itself implies $k < (a/n)x$. This means that if a is small, then it is really to your advantage to think of using Approach 2 instead of Approach 1. In Approach 1, you might have to try $n - 1$ different values of x before you get one that satisfies $ax \equiv 1 \pmod{n}$. Since $k < (a/n)x$, you necessarily will have only a/n times as many choices for k to consider. In Approach 3, the number of k to consider is decreased by a factor of 2 over Approach 2 (more-or-less, though this is certainly not true if $n = 2$). However, for each k, there are two numbers to ponder, both $kn + 1$ and $kn - 1$. A slight advantage of Approach 3 over Approach 2 is that the multiples of n one looks at are kept smaller in Approach 3.

- **Examples.**

(1) Solve $3x \equiv 1 \pmod{19}$. Approach 1 requires that we check $x = 1, 2, \ldots, 13$. We can stop at 13 since then $3 \cdot 13 = 39 \equiv 1 \pmod{19}$. For Approach 2, we check $19 + 1 = 20$ and $2 \cdot 19 + 1 = 39$. Since 39 is divisible by 3, we stop and compute $x = 39/3 = 13$. For Approach 3, we check $19 + 1 = 20$ and $19 - 1 = 18$. Since 18 is divisible by 3, we get $x = -18/3 = -6$ (which is the same as 13 modulo 19).

(2) Solve $51x \equiv 1 \pmod{22}$. First, we observe that $51 \equiv 7 \pmod{22}$. The problem then is equivalent to solving $7x \equiv 1 \pmod{22}$. Approach 1 requires that we check $x = 1, 2, \ldots, 19$. We stop at 19 since $7 \cdot 19 = 133 \equiv 1 \pmod{22}$. For Approach 2, we check $22+1, 2 \cdot 22+1, \ldots, 5 \cdot 22+1$ and $6 \cdot 22 + 1$. Since $6 \cdot 22 + 1 = 133$ is divisible by 7, we stop there and get $x = 133/7 = 19$.

For Approach 3, we check $22+1$ and $22-1$. Since $22-1=21$ is divisible by 7, we obtain $x=-21/7=-3$ (which is the same as 19 modulo 22).

Homework:

(1) Solve $5x \equiv 1 \pmod{18}$. Use each of the approaches mentioned.

(2) Solve $4x \equiv 1 \pmod{49}$ using any approach you want. Check your work by checking directly to see if the x you obtained satisfies $4x \equiv 1 \pmod{49}$.

(3) Solve $67x \equiv 1 \pmod{16}$ using any approach you want.