Dartmouth College
Mathematics 17

Assignment 4
due Wednesday, February 1

1. Let's consider a special case of the Chinese Remainder Theorem (CRT). Let $m, n > 1$ be coprime integers, and let a, b be arbitrary integers. Then the system of congruences:

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

has a unique solution modulo mn.

   (a) Give a proof of the CRT using the following generous hint. Since $\gcd(m, n) = 1$, Bezout says there exists $u, v \in \mathbb{Z}$ so that $mu + nv = 1$. Show that the number $bmu + anv$ is a solution to the system, and then prove it is unique modulo mn.

   (b) Explain how to use this version of the CRT to solve a system $x \equiv a \pmod{m}$, $\equiv b \pmod{n}$, $x \equiv c \pmod{\ell}$ where $m, n, \ell > 1$ are integers which are coprime in pairs.

   (c) Solve the system $x \equiv 2 \pmod{15}$, $x \equiv 3 \pmod{7}$ using the CRT.

2. This problem focuses on two means to compute the least non-negative residue of $5^{1030} \pmod{153}$ in an efficient manner.

   (a) In this first approach, use the fact that $153 = 9 \cdot 17$ together with the CRT and Euler's theorem, to find the least non-negative residue.

   (b) Use the method of fast exponentiation described in class (via the binary expansion of 1030) to compute this residue.

3. Recall that the Euler phi-function, $\phi(n)$, is defined by:
$\phi(n) = |U_n| = \#\{k \mid 1 \leq k \leq n \text{ with } \gcd(k, n) = 1\}$ We have observed that for a prime p, $\phi(p) = p - 1$.

   (a) Let p be a prime. Determine the value of $\phi(p^r)$ for any positive integer r. Hint: It may be easier to count the number of elements of $a \in \mathbb{Z}_{p^r}$ which are not relatively prime to p^r and use that to determine the value of the function. Of course be sure to check your answer against a few examples you can compute by hand.

   (b) It is easy to show that in general $\phi(mn) \neq \phi(m)\phi(n)$, but what is remarkable is the when $\gcd(m, n) = 1$, $\phi(mn) = \phi(m)\phi(n)$. The function ϕ is an example of a *multiplicative* function in number theory. Perhaps more surprising is that this is another consequence of the CRT. Give a proof that ϕ is multiplicative using the following idea: Let $\gcd(m, n) = 1$. Show that there is a bijection between the sets: U_{mn} and $U_m \times U_n$ (ordered pairs (a, b) with $a \in U_m$, $b \in U_n$. Let the map $F : U_{mn} \to U_m \times U_n$ be given by $F([a]_{mn}) = ([a]_m, [a]_n)$. You need to show this map is well-defined, one-to-one, and onto. Then deduce the result.

Some of these words may be new to you, so here are some definitions.

- We have encountered the term well-defined before. In this context it means that if $[a]_{mn} = [b]_{mn}$, then $F([a]) = F([b])$.
- A map is one-to-one (injective) if $F([a]) = F([b])$ implies $[a]_{mn} = [b]_{mn}$.
- A map is onto (surjective) if given $([b]_m, [c]_n) \in U_m \times U_n$, there exists $[a]_{mn} \in U_{mn}$ so that $F([a]) = ([b], [c])$.
- A map is bijective if it is one-to-one and onto.
- If $f : S \to T$ is a bijection, then S and T are said to have the same cardinality (size), and the result you are to prove is simply that when $\gcd(m, n) = 1$, the size of U_{mn} and $U_m \times U_n$ is the same.