MATH 113: DISCRETE STRUCTURES
FRIDAY WEEK 12 HANDOUT

Question 1. Solve the system of congruences

$$2x \equiv 5 \pmod 7$$
$$3x \equiv 4 \pmod 8.$$

Problem 2. What is the remainder when you divide 135^3 by 1728? (*Hint*: $1728 = 64 \cdot 27$.)

Recall that the Fermat-Euler Theorem is a generalization of Fermat's Little Theorem which states that

$$a^{\phi(n)} \equiv 1 \pmod n$$

when $\gcd(a, n) = 1$. We will prove a special case of this theorem in which n is the product of k distinct primes, $n = p_1 p_2 \cdots p_k$. In this case, $\phi(n) = (p_1 - 1)(p_2 - 1) \cdots (p_k - 1)$. Let $q_i = \phi(n)/(p_i - 1)$ for $i = 1, 2, \ldots, k$. Then

$$a^{\phi(n)} = (a^{p_i - 1})^{q_i} \equiv 1^{q_i} \equiv 1 \pmod{p_i}$$

for all i. We see then that $x = a^{\phi(n)}$ is a simultaneous solution of the congruences

$$x \equiv 1 \pmod{p_1},\ x \equiv 1 \pmod{p_2},\ \ldots,\ x \equiv 1 \pmod{p_k}.$$

But $x = 1$ is another solution! By Sunzi's theorem, it follows that $a^{\phi(n)} \equiv 1 \pmod n$. □

Problem 3. How can the above argument be extended to the case in which $n = p_1^{a_1} \cdots p_k^{a_k}$ where the p_i are distinct primes and $a_i \geq 1$?