Problem Set D – Partial Solutions

Shishir Agrawal

Problem 1. Students learning algebra for the first time will sometimes assert things like $(a+b)^2 = a^2 + b^2$. This, of course, is just not true! (Take $a = b = 1$ for a counterexample.) However, it *is* true that

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

for $a, b \in \mathbb{Z}$ and any prime number p. Prove this fact.

Solution. There are at least two (closely related) proofs: one using Fermat's little theorem, the other using the binomial theorem.

First, let's do the proof using Fermat's little theorem, which tells us that $x^p \equiv x \pmod{p}$ for any x. Applying this with $x = a, b, a+b$ shows that $a^p \equiv a, b^p \equiv b, (a+b)^p \equiv a+b \pmod{p}$. Thus

$$(a+b)^p \equiv a+b \equiv a^p + b^p \pmod{p}.$$

Next, let's do the proof using the binomial theorem. We know that

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} + b^p.$$

Note that

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

must be divisible by p for any $1 \leq k \leq p-1$. This is because p shows up as a prime factor of the numerator but it does not show up in the denominator since none of the terms in either $k!$ or in $(p-k)!$ is divisible by p. Thus all of the terms in the summation above corresponding to $k = 1, \ldots, p-1$ are divisible by p, so

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} + b^p \equiv a^p + b^p \pmod{p}.$$

Problem 3. Show that $(p+1)^p \equiv 1 \pmod{p^2}$ for any prime p.

Solution. By the binomial theorem, we have

$$(p+1)^p = p^p + \binom{p}{1}p^{p-1} + \cdots + \binom{p}{p-2}p^2 + \binom{p}{p-1}p + 1.$$

Clearly $p^2 \mid p^k$ for all $k \geq 2$, so all the terms except for the last 2 are congruent to 0 mod p^2. Moreover, $\binom{p}{p-1} = p$, so the second-to-last term $\binom{p}{p-1}p = p^2$ is also congruent to 0 mod p^2. Thus

$$(p+1)^p \equiv 1 \pmod{p^2}.$$

Problem 5. Prove that, if $\gcd(a,b) = 1$, then

$$a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}.$$

Solution. Note that

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

where we use the fact that any power of b is congruent to 0 mod b for the first congruence, and Euler's theorem for the second congruence. Similarly, we also have

$$a^{\phi(b)} + b^{\phi(a)} \equiv b^{\phi(a)} \equiv 1 \pmod{b}.$$

By the Chinese remainder theorem, we know that the system of congruences

$$\begin{aligned} x &\equiv 1 \pmod{a} \\ x &\equiv 1 \pmod{b} \end{aligned}$$

has a unique solution modulo ab. Since $x = 1$ and $x = a^{\phi(a)} + b^{\phi(a)}$ are both solutions to this system of congruences, it must be that

$$a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$$

using the uniqueness assertion of the Chinese remainder theorem.