CSE 16
Homework Assignment 6
Solutions to Selected Problems

Chapter 5 (p. 136): #30
If $a \equiv b(\mathrm{mod}\ n)$, then $\gcd(a, n) = \gcd(b, n)$.

Proof:
Since $a \equiv_n b$ we have $n|(a - b)$ and hence $a - b = kn$ for some $k \in \mathbb{Z}$. Thus, for any $d \in \mathbb{Z}$ we have

$$d|a \wedge d|n \;\Rightarrow\; d|(a - kn) \wedge d|n \;\Rightarrow\; d|b \wedge d|n$$

and

$$d|b \wedge d|n \;\Rightarrow\; d|(b + kn) \wedge d|n \;\Rightarrow\; d|a \wedge d|n.$$

Hence $d|a \wedge d|n \;\Leftrightarrow\; d|b \wedge d|n$, for any integer d. It follows that

$$\{\text{common divisors of } a \text{ and } n\} = \{\text{common divisors of } b \text{ and } n\}$$

Since these sets are equal, their greatest elements must also be equal, i.e. $\gcd(a, n) = \gcd(b, n)$. ■

Chapter 7 (p. 155): #10
If $a \in \mathbb{Z}$, then $a^3 \equiv a(\mathrm{mod}\ 3)$.

Proof:
Every 3rd integer is divisible by 3, and hence any sequence of three consecutive integers contains one term that is divisible by 3. In particular, for any $a \in \mathbb{Z}$, exactly one of $a - 1$, a, $a + 1$ is divisible by 3, whence $3|a(a - 1)(a + 1) = a(a^2 - 1) = a^3 - a$. Thererfore $a^3 \equiv a(\mathrm{mod}\ 3)$ as required. ■

Chapter 7 (p. 155): #34
If $\gcd(a, c) = \gcd(b, c) = 1$, then $\gcd(ab, c) = 1$. [Hint: use the following proposition from page 152 of the text, and from page 4 in the class notes from 7-26-22: $\gcd(d, e) = dn + em$ for some $n, m \in \mathbb{Z}$.]

Proof:
Utilizing the hint, there exist integers n, m, k, l such that $an + cm = 1$ and $bk + cl = 1$. Multiplying these two equations gives

$$1 = (an + cm)(bk + cl)$$

$$1 = abnk + cbmk + canl + c^2ml$$

$$1 = ab(nk) + c(bmk + bml + cml).$$

Since $\gcd(ab, c)$ divides both ab and c, the last equation implies $\gcd(ab, c)|1$, and hence $\gcd(ab, c) = 1$, as claimed. ■

Chapter 10 (p. 195): #24
Prove (by induction) that for any $n \geq 1$

$$\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}.$$

Note: we gave two non-inductive proofs of this fact in the solutions to hw4.

Proof:

I. Let $n = 1$. Then the LHS is $\sum_{k=1}^{1} k\binom{1}{k} = 1 \cdot \binom{1}{1} = 1$, while the RHS equals $1 \cdot 2^0 = 1 \cdot 1 = 1$, which establishes the base case.

II. Let $n \geq 1$ be arbitrary, and assume $\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}$. We must show that

$$\sum_{k=1}^{n+1} k\binom{n+1}{k} = (n+1)2^n$$

Pascal's identity gives us

$$\sum_{k=1}^{n+1} k\binom{n+1}{k} = \sum_{k=1}^{n+1} k\left[\binom{n}{k-1} + \binom{n}{k}\right]$$

$$= \sum_{k=1}^{n+1} k\binom{n}{k-1} + \sum_{k=1}^{n+1} k\binom{n}{k}$$

(replace k by $k+1$ in the first sum, peel off the last term in the second sum)

$$= \sum_{k=0}^{n} (k+1)\binom{n}{k} + \sum_{k=1}^{n} k\binom{n}{k} + (n+1)\binom{n}{n+1}$$

(distribute $\binom{n}{k}$ in the first sum, split into two sums, peel off 1st term)

$$= 0 \cdot \binom{n}{0} + \sum_{k=1}^{n} k\binom{n}{k} + \sum_{k=0}^{n} \binom{n}{k} + \sum_{k=1}^{n} k\binom{n}{k} + (n+1)\binom{n}{n+1}$$

(delete the outer terms since they are zero, combine first and third sums)

$$= \sum_{k=0}^{n} \binom{n}{k} + 2 \cdot \sum_{k=1}^{n} k\binom{n}{k}$$

(use $\sum_{k=0}^{n} \binom{n}{k} = 2^n$, and the <u>induction hypothesis</u>)

$$= 2^n + 2 \cdot n2^{n-1}$$

$$= 2^n + n2^n$$

$$= (n+1)2^n.$$

The result follows for all $n \geq 1$ by the 1st Principle of Mathematical Induction. ■