CSE 16
Homework Assignment 6
Solutions to Selected Problems

Chapter 5 (page 136): 18
If $a, b \in \mathbb{Z}$, then $(a+b)^3 \equiv a^3 + b^3 \pmod 3$.

Proof:
Observe $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 = (a^3 + b^3) + 3(a^2b + ab^2)$, so that

$$(a+b)^3 - (a^3 + b^3) = 3(a^2b + ab^2).$$

Thus $3 \mid \big((a+b)^3 - (a^3 + b^3)\big)$, whence $(a+b)^3 \equiv a^3 + b^3 \pmod 3$. ■

Chapter 5 (page 136): 24
Let $a, b, c, d \in \mathbb{Z}$. If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $ac \equiv bd \pmod n$.

Proof:
Assume $a \equiv b \pmod n$ and $c \equiv d \pmod n$, whence $n|(a-b)$ and $n|(c-d)$. Therefore there exist $k_1, k_2 \in \mathbb{Z}$ such that $a - b = k_1 n$ and $c - d = k_2 n$. Now observe

$$\begin{aligned} ac - bd &= ac - bc + bc - bd \\ &= c(a-b) + b(c-d) \\ &= ck_1 n + bk_2 n \\ &= (ck_1 + bk_2)n, \end{aligned}$$

showing that $n|(ac - bd)$. Therefore $ac \equiv bd \pmod n$, as required. ■

Chapter 6 (page 144): 6
If $a, b \in \mathbb{Z}$, then $a^2 - 4b - 2 \neq 0$.

Proof:
Assume, to get a contradiction, that $a^2 - 4b - 2 = 0$. Then $a^2 = 4b + 2 = 2(2b+1)$. This shows $2|a^2$, and by a result proved in class, we have $2|a$. Therefore $a = 2k$ for some $k \in \mathbb{Z}$, and

$$\begin{aligned} & (2k)^2 = 2(2b+1) \\ \therefore \quad & 4k^2 = 2(2b+1) \\ \therefore \quad & 2k^2 = 2b + 1. \end{aligned}$$

But the left hand side of this equation is even, while the right hand side is odd, which is impossible. This contradiction shows our assumption was false, and therefore $a^2 - 4b - 2 \neq 0$, as claimed. ■

Chapter 7 (page 155): 30

Let $a, b, p \in \mathbb{Z}$, and suppose p is prime. Prove that if $p|ab$, then either $p|a$ or $p|b$. (Hint: use the proposition on page 152, which says $\gcd(u, v) = ux + vy$ for some $x, y \in \mathbb{Z}$.)

Proof:

Assume $p|ab$, whence $ab = pk$ for some $k \in \mathbb{Z}$. Either p divides a, or it does not.

Case 1: $p|a$

In this case we are done.

Case 2: $p \nmid a$

Since p is prime, the divisors of p are $\{1, p\}$. The only common divisor of p and a is therefore 1, hence $\gcd(p, a) = 1$. By the hint (a fact that was proved in class), we have $px + ay = 1$, for some $x, y \in \mathbb{Z}$. Multiplying this last equation by b, we have

$$b = b(px + ay) = pbx + aby = pbx + pky = p(bx + ky),$$

showing that $p|b$.

Since at least one of these cases must hold, we have either $p|a$ or $p|b$, as required. ■