CSE 16
Homework Assignment 7
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 7 (page 155): 24
If $a \in \mathbb{Z}$, then $4 \nmid (a^2 - 3)$.

Proof:
There are four cases to consider, corresponding to the possible remainders upon division by 4.

(1) $a = 4k$ (for some $k \in \mathbb{Z}$): Then $a^2 = (4k)^2 = 4(4k^2)$, whence $a^2 \equiv 0 \pmod 4$.
(2) $a = 4k+1$ (for some $k \in \mathbb{Z}$): Then $a^2 = (4k+1)^2 = 4(4k^2+2k)+1$, so $a^2 \equiv 1 \pmod 4$.
(3) $a = 4k+2$ (for some $k \in \mathbb{Z}$): Then $a^2 = (4k+2)^2 = 4(4k^2+4k)$, so $a^2 \equiv 0 \pmod 4$.
(4) $a = 4k+3$ (for some $k \in \mathbb{Z}$): Then $a^2 = (4k+3)^2 = 4(4k^2+6k+2)+1$, so $a^2 \equiv 1 \pmod 4$.

Thus, for any $a \in \mathbb{Z}$, there are only two possibilities: $a^2 \equiv 0 \pmod 4$ or $a^2 \equiv 1 \pmod 4$. In particular, for no a do we have $a^2 \equiv 3 \pmod 4$. In other words $4 \mid (a^2-3)$ is impossible. Therefore $4 \nmid (a^2-3)$ for every $a \in \mathbb{Z}$. ■

Chapter 7 (page 155): 30
Let $a, b, p \in \mathbb{Z}$, and suppose p is prime. Prove that if $p \mid ab$, then either $p \mid a$ or $p \mid b$. (Hint: use the proposition on page 152, which says $\gcd(u, v) = ux + vy$ for some $x, y \in \mathbb{Z}$.)

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

Case 1: $p \mid a$
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 $p \mid b$.

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