4.1 Divisibility and Modular ARITHMETIC

(19.) $f(x) = \begin{cases} x \bmod m & \text{if } x \bmod m \le \lceil m/2 \rceil \\ (x \bmod m) - m & \text{if } x \bmod m > \lceil m/2 \rceil \end{cases}$

(37.) a) if $ac \equiv bc \pmod m$, where a, b, c and m are integers with $m \geq 2$, then $a \equiv b \pmod m$ –
– to show that this does not hold, we need to find an example in which $ac \equiv bc \pmod m$, but $a \equiv b \pmod m$. let $m = 4$ and $C = 2$. Let $a = 0$, and $b = 2$ then $ac = 0$ and $bc = 4$, so $ac \equiv bc \pmod 4$, but $0 \not\equiv 2 \pmod 4$

b) if $a \equiv b \pmod m$ and $c \equiv d \pmod m$, where a, b, c, d and m are integers with c and d positive and $m \geq 2$, then $a^c \equiv b^d \pmod m$
– to show that this will not hold, we need an example where $a \equiv b \pmod m$ and $c \equiv d \pmod m$, but $a^c \not\equiv b^d \pmod m$.

Let $m = 5$, $a = 3$, $b = 3$, $C = 1$, $d = 6$. $a^c = 3$, $b^d = 729 \equiv 4 \pmod 5$
so $3 \not\equiv 3^6 \pmod 5$, even though $3 \equiv 3 \pmod 5$ and $1 \equiv 6 \pmod 5$.

(41) Since $a \equiv b \pmod m$, then $a \cdot a \equiv b \cdot b \pmod m$, i.e. $a^2 \equiv b^2 \pmod m$. Since $a \equiv b \pmod m$ and $a^2 \equiv b^2 \pmod m$, then $a^3 \equiv b^3 \pmod m$.
After $k-1$ applications, we will obtain $a^k \equiv b^k \pmod m$