Worksheet 8

Problems marked with a $(*)$ are "key results".

The first few problems deal with the basic properties of modular arithmetic, and show that it has very similar properties to usual arithmetic.

1. $(*)$ Prove that there is a unique choice of r with $0 \le r < n$ such that $a \equiv r \bmod n$.
2. $(*)$ Let $a, b, c \in \mathbb{Z}$ be arbitrary, and fix $n > 1$. Prove the following:
   (a) $a \equiv a \bmod n$
   (b) If $a \equiv b \bmod n$ then $b \equiv a \bmod n$.
   (c) If $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $a \equiv c \bmod n$.
3. $(*)$ For any $a, a', b, b' \in \mathbb{Z}$ and fixed $n > 1$, prove the following:
   (a) If $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$ then $a \pm b \equiv a' \pm b' \bmod n$.
   (b) If $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$ then $ab \equiv a'b' \bmod n$.
   (c) If $a \equiv b \bmod n$ and $d \mid n$, then $a \equiv b \bmod d$.
4. $(*)$ Fix $n > 1$. For any $a, b \in \mathbb{Z}$ and $k \ge 1$, prove that if $a \equiv b \bmod n$ then $a^k \equiv b^k \bmod n$.

The remaining problems deal with computations using the above properties of modular arithmetic, to help you get a feeling for how they go.

5. Reduce the following mod n:
   (a) $9284756 \bmod 8$
   (b) $-181374 \bmod 29$
   (c) $2357 \cdot (9453 + 1294) - 3284 \bmod 7$
6. Show that 41 divides $2^{20} - 1$ by following these steps. Explain why each step is true.
   i. $2^5 \equiv -9 \bmod 41$.
   ii. $(2^5)^4 \equiv (-9)^4 \bmod 41$.
   iii. $2^{20} \equiv 81^2 \bmod 41 \equiv (-1)^2 \bmod 41$.
   iv. $2^{20} - 1 \equiv 0 \bmod 41$.
7. Reduce $2^{50} \bmod 7$.
8. Show that 39 divides $17^{48} - 5^{24}$.
9. Find an integer x such that $5x \equiv 1 \bmod 7$. Can you find x such that $6x \equiv 1 \bmod 8$?