Math Circles - Elementary Number Theory - Fall 2023

Exercises

1. Compute the following:
   (a) $5 + 7 \mod 8$
   (b) $18 - 21 \mod 30$
   (c) $3 \cdot 7 \mod 15$
   (d) $7 \cdot -9 \mod 11$
2. Compute the following multiplicative inverses:
   (a) $5^{-1} \mod 7$
   (b) $14^{-1} \mod 19$
   (c) $33^{-1} \mod 47$
3. Compute the following:
   (a) $3 \div 5 \mod 7$
   (b) $9 \div 14 \mod 19$
   (c) $1 \div 33 \mod 47$
4. Let a, b, c, d, and n be integers. Prove the following:
   (a) If $a \equiv b \mod n$ and $c \equiv d \mod n$ then $a + c \equiv b + d \mod n$.
   (b) If $a \equiv b \mod n$ and $c \equiv d \mod n$ then $ac \equiv bd \mod n$.
   (c) If $a \equiv b \mod n$ and $b \equiv c \mod n$ then $a \equiv c \mod n$.
5. Let p be prime. Prove that the multiplicative inverse of every integer in $\{1, \ldots, p-1\}$ is unique.
6. Let a, b, and c be integers, and let p be prime. Prove that if $ab \equiv ac \mod p$ then $b \equiv c \mod p$. (This is called the "cancellation law").
7. Prove that if x is a perfect square (i.e., there exists an integer y such that $y^2 = x$) then either $x \equiv 0 \mod 4$ or $x \equiv 1 \mod 4$.