

CS3441/9441 Tutorial 2

Review of Modular Arithmetic

For integers x, y and $n > 0$, write $x \equiv y \pmod n$ if there exists an integer k such that $x = kn + y$

1. Show that equivalence $\pmod n$ is an equivalence relation, i.e., is reflexive, symmetric and transitive.
2. Show that if $x \equiv x' \pmod n$ and $y \equiv y' \pmod n$ then
 - (a) $x + y \equiv x' + y' \pmod n$
 - (b) $x \cdot y \equiv x' \cdot y' \pmod n$
 - (c) $x^y \equiv (x')^y \pmod n$
 - (d) it does *not* follow that $x^y \equiv x^{y'} \pmod n$ (Try $x = 2, y = 1, y' = 4, n = 3$)
3. a is a generator $\pmod n$ if $a, a^2, a^3, \dots, a^{n-1}$ includes all numbers $1, 2, 3, \dots, n-1 \pmod n$. For each $n = 3, 4, 5, 6, 7$, determine which numbers are generators $\pmod n$.
4. Prove that if q is prime then generators $\pmod q$ exist.
5. Which numbers $\pmod{30}$ are relatively prime to 30?
6. Solve the following equations using Euclid's Algorithm
 - (a) $7x \equiv 4 \pmod{30}$
 - (b) $11x \equiv 23 \pmod{30}$
7. From first principles, compute $\phi(n)$ and $a^{\phi(n)} \pmod n$ for the pairs $(a, n) = (5, 6), (7, 10), (11, 15)$. Compare with the theorems given in class.