

Homework 6

Due at the *beginning* of class on Nov. 14

When you are asked to compute a result “by hand”, you may use a calculator to perform multiplication/division but you may not use a special-purpose computer program.

1. Exercise 7.6.
2. Exercise 7.8.
3. The following exercises concern modular arithmetic. Answer them by hand:
 - (a) Compute $[46^{-1} \bmod 51]$, using the extended Euclidean algorithm.
 - (b) Solve for x in the following equation: $46x = 49 \bmod 51$.
 - (c) Compute $\gcd(45, 51)$ using the Euclidean algorithm. Does 45 have an inverse modulo 51?
 - (d) The equation $45x = 39 \bmod 51$ has the solution $x = 2$. Does this contradict your result from part (c)?
4. Let $N = 55 = 5 \cdot 11$. Answer the following by hand:
 - (a) What is $\varphi(N)$?
 - (b) Say $e = 3$. Find d such that $(x^e)^d = x \bmod N$ for all $x \in \mathbb{Z}_N^*$.
 - (c) Find an $x \in \mathbb{Z}_N^*$ such that $x^e = 2 \bmod N$. How many $x \in \mathbb{Z}_N^*$ satisfy this equation?
5. The following exercises concern the group $\mathbb{Z}_{17}^*$. Answer them by hand.
 - (a) Prove that 2 is not a generator of $\mathbb{Z}_{17}^*$.
 - (b) Show that 3 is a generator of $\mathbb{Z}_{17}^*$.
 - (c) Compute $\log_3 10$.
6. Exercise 7.13.