Homework Set 9

MATH 221 — WINTER 2016

Do not turn in.

PROBLEM 9.1. a) Compute $10\%7, 100\%7, 1000\%7, 10000\%7, 100000\%7, 1000000\%7$.

b) Use part a) to quickly determine $9001073\%7$.

PROBLEM 9.2. Use the extended Euclidean algorithm to compute $\gcd(342, 232)$; show each intermediate step in the algorithm and use this to find integers $x$ and $y$ such that $342x + 232y = \gcd(342, 232)$. Do the same for $\gcd(1714, 1814)$.

PROBLEM 9.3. An element $k$ of $\mathbb{Z}_n$ is invertible if there is an $a \in \mathbb{Z}_n$ such that $ka \equiv 1 \mod n$. Find the inverses of all the invertible elements of $\mathbb{Z}_{26}$.

PROBLEM 9.4. Do there exist integers $x$ and $y$ such that $4x + 6y = 2$? Either find a solution or say why none exists.

PROBLEM 9.5. Do there exist integers $x$ and $y$ such that $4x + 6y = 3$? Either find a solution or say why none exists.

PROBLEM 9.6. Compute $\phi(n)$ for $n = 2, 3, 4, 5, 6, 27, 30, 100, 400, 100000$.

PROBLEM 9.7. Prove or disprove: $\phi(ab) = \phi(a)\phi(b)$ for all integers $a, b > 1$.

PROBLEM 9.8. Let $p$ be a prime. Note that $D(p^2) = \{\pm 1, \pm p, \pm p^2\}$.

a) Determine the set of integers $\{k \in \mathbb{Z} : \gcd(k, p^2) = p \text{ and } 1 \leq k < p^2\}$.

b) Determine the set of integers $\{k \in \mathbb{Z} : \gcd(k, p^2) = 1 \text{ and } 1 \leq k < p^2\}$.

c) Use part (b) to show that $\phi(p^2) = p^2 - p$.


PROBLEM 9.10. Euler’s generalization of Fermat’s little theorem says that $a^{\phi(n)} \equiv 1 \mod n$ if $\gcd(a, n) = 1$. Use this to find the last 5 digits of $7^{40000}$. 