NAME (Printed): _____

Math 330-3 Number Systems Fall 2022 Quiz 10 Feingold

SHOW ALL WORK NECESSARY TO JUSTIFY YOUR ANSWERS.

Def: For any $n \in \mathbb{N}^+$ define $U(n) = \{[a]_n \in \mathbb{Z}_n \mid gcd(a, n) = 1\}$ and let $\phi(n) = |U(n)|$ be the number of equivalence classes in $U(n)$. Example: $U(8) = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ so $\phi(8) = 4$.

Th: $U(n)$ is a finite group under multiplication mod n, with identity element $[1]_n$.

Th: (Fermat's Little Th) For p prime and $a \in \mathbb{Z}$ with $gcd(a, p) = 1$, we have $a^{p-1} \equiv 1 \pmod{p}$.

Th: (Euler's Theorem) For $n \in \mathbb{N}^+$ and $a \in \mathbb{Z}$ with $gcd(a, n) = 1$, we have $a^{\phi(n)} \equiv 1 \pmod{n}$.

Use these results to efficiently answer the following questions. Do not just take powers until you find the smallest power that gives the equivalence class of 1.

---

1. (10 points) Find the unique integer c, $1 \leq c < 13$ such that $3^{4370} \equiv c \pmod{13}$.

---

2. (10 points) Find the unique integer d, $1 \leq d < 20$ such that $7^{1950} \equiv d \pmod{20}$.

Math 330-3 Number Systems Fall 2022 Quiz 10 Solutions Feingold

Def: For any $n \in \mathbb{N}^+$ define $U(n) = \{[a]_n \in \mathbb{Z}_n \mid gcd(a,n) = 1\}$ and let $\phi(n) = |U(n)|$ be the number of equivalence classes in $U(n)$. Example: $U(8) = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ so $\phi(8) = 4$.

Th: $U(n)$ is a finite group under multiplication mod n, with identity element $[1]_n$.

Th: (Fermat's Little Th) For p prime and $a \in \mathbb{Z}$ with $gcd(a,p) = 1$, we have $a^{p-1} \equiv 1 \pmod{p}$.

Th: (Euler's Theorem) For $n \in \mathbb{N}^+$ and $a \in \mathbb{Z}$ with $gcd(a,n) = 1$, we have $a^{\phi(n)} \equiv 1 \pmod{n}$.

Use these results to efficiently answer the following questions. Do not just take powers until you find the smallest power that gives the equivalence class of 1.

---

1. (10 points) Find the unique integer c, $1 \le c < 13$ such that $3^{4370} \equiv c \pmod{13}$.

Solution: Since 13 is prime and $gcd(3,13) = 1$, Fermat's Little Theorem says $3^{12} \equiv 1 \pmod{13}$. By simple arithmetic, $4370 = (12)(364) + 2$ so

$$3^{4370} = (3^{12})^{364}\, 3^2 \equiv 1^{364}\, 3^2 \equiv 9 \pmod{13} \quad \text{gives} \quad c = 9.$$

---

2. (10 points) Find the unique integer d, $1 \le d < 20$ such that $7^{1950} \equiv d \pmod{20}$.

Solution: Since $gcd(7,20) = 1$, Euler's Theorem says $7^{\phi(20)} \equiv 1 \pmod{20}$. We check that $U(20)$ consists of the eight equivalence classes mod 20 of the numbers $1, 3, 7, 9, 11, 13, 17, 19$, so $\phi(20) = 8$ so $7^8 \equiv 1 \pmod{20}$. By simple arithmetic, $1950 = (8)(243) + 6$ so

$$7^{1950} = (7^8)^{243}\, 7^6 \equiv 1^{243}\, 7^6 \equiv 7^6 \pmod{20}.$$

We also know that $7^2 = 49 \equiv 9 \pmod{20}$ so $7^3 \equiv (9)(7) = 63 \equiv 3 \pmod{20}$, so $7^6 = (7^3)^2 \equiv 3^2 \equiv 9 \pmod{20}$ so $d = 9$.
