Quiz1109@Tan&znlady

Pre-class-Quiz Name: ID:

Answer:

1. $3^{201} \bmod 11 = ?$
2. $a \equiv 9794 \pmod{73}$, $a \in [0, 72]$ $a = ?$
3. **Chinese Remainder theorem** $x \equiv 2 (\bmod 3)$, $x \equiv 3 (\bmod 5)$, $x \equiv 2 (\bmod 7)$ $x = ?$
4. If $\gcd(r, n) = 1$ and if $\phi(n)$ is the **order** of *a*, then a is called **a primitive root** modulo n. Find all primitive roots of 25.
5. $7^{1000} \equiv a \pmod{10}$, $a \in [0, 9]$, $a = ?$
6. **Generators** in $\mathbb{Z}_{13}^*$ are ?
7. How much is the **inverse** of 550 in $\mathbb{Z}_{1759}$, i.e. $550^{-1} \bmod 1759 = ?$
8. What is the **order** of 2 in $\mathbb{Z}_{35}^*$? i.e. $2^x = 1 \bmod 25$, $x = ?$

Post-class-Quiz Name: ID:

Answer:

1. $\phi(440) = ?$
2. $x^{85} \equiv 6 \pmod{29}$, $x \in [0, 28]$, $x = ?$
3. $14x \equiv 26 (\bmod 38)$ $x = ?$
4. **Chinese Remainder theorem** $x \equiv 2 (\bmod 3)$ $x \equiv 1 (\bmod 5)$, $x \equiv 6 (\bmod 7)$ $x = ?$
5. What is the **5th root** of 2 in $\mathbb{Z}_{19}$? (i.e. $2^{1/5} \bmod 19 = ?$)
6. $x^2 - 4x - 16 \equiv 0 (\bmod 29)$ $x = ?$
7. Compute a^{75} by **repeated squaring algorithm**, how many multiplications do you need?
8. What is the discrete log of 6 base 2 in $\mathbb{Z}_{13}$? (i.e. $D\log_2 6 \bmod 13 = ?$)