Homework Set 7 (Lecture 25)

Problem 6

Example 7. What are the multiplicative orders of 2 and 4 modulo 7?

Solution. Since $\phi(7)=6$, the possible orders of residues modulo 7 are $1,2,3,6$.
Since $2^2=4\not\equiv 1$, $2^3\equiv 1 \pmod 7$, the multiplicative order of $2 \pmod 7$ is 3.
Since $4^2\equiv 2\not\equiv 1$, $4^3\equiv 1 \pmod 7$, the multiplicative order of $4 \pmod 7$ is 3.
Alternatively. For the second part, we could have also used that, if $x \pmod m$ has (multiplicative) order k, then x^a has order $\frac{k}{\gcd(k,a)}$. Therefore, $4=2^2$ has multiplicative order $\frac{3}{\gcd(3,3)}=3$ modulo 7.

Problem 7

Example 8. Suppose 4 has multiplicative order 17 modulo m. What is the multiplicative order of 64 modulo m?

Solution. Recall that, if $x \pmod m$ has (multiplicative) order k, then x^a has order $\frac{k}{\gcd(k,a)}$.
Therefore, $64=4^3$ has multiplicative order $\frac{17}{\gcd(17,3)}=17$ modulo m.

Problem 8

Example 9. Suppose 2 has multiplicative order 21 modulo m. What is the multiplicative order of 8 modulo m?

Solution. Recall that, if $x \pmod m$ has (multiplicative) order k, then x^a has order $\frac{k}{\gcd(k,a)}$.
Therefore, $8=2^3$ has multiplicative order $\frac{21}{\gcd(21,3)}=7$ modulo m.

Armin Straub
straub@southalabama.edu