Math 113 — Problem Set 11 — William Guss

(P189. 1) We will see later that the multiplicitive group of nonzero elements of a finite field is cyclic. Find a generator for this group for the finite field $\mathbb{Z}_7$.

Proof. The multiplicitive group of nonzero elements of $\mathbb{Z}_7$ is $G = \langle\{1, \cdots, 6\}, \cdot_7\rangle$. If an element a generates G for every coprime of 6, (there must be 6 elements) Then a^5 must also generate the group. Thus the generators are $\{5\}$ and by $\{3\}$ because

$$[5^n]_{n=0}^{20} = [1, 5, 4, 6, 2, 3, 1, 5, 4, 6, 2, 3, 1, 5, 4, 6, 2, 3, 1, 5]$$
$$[3^n]_{n=0}^{20} = [1, 3, 2, 6, 4, 5, 1, 3, 2, 6, 4, 5, 1, 3, 2, 6, 4, 5, 1, 3]$$

□

(P189. 4) Using Fermat's theorem compute the remainder of 3^{47} when it is divided by 23.

Proof. Although a is not divisible by 23, Fermat's theorem says that if 3 is not divisible by 23, then $3^{22} = 1 \mod 23$. Thus $3^{22\times2+3} = 3^{22}\times3^{22}\times3^3 \mod 23 = 1\times1\times3^3 \mod 23$. Computing $3^3 = 27 = 4 \mod 23$ we get $3^{47} = 4 \mod 23$. □