Worksheet 18

Problems marked with a $(*)$ are "key results".

1. $(*)$ Let $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ be a non-constant polynomial of degree d. Prove that $f(x)$ has at most d roots in $\mathbb{Z}/p\mathbb{Z}$.

2. (a) $(*)$ Let $d \mid p-1$, and let $N_p(d)$ denote the number of elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order d. Prove that if $N_p(d) > 0$, then $N_p(d) = \varphi(d)$. That is to say, if there is an element of order d then there are precisely $\varphi(d)$ of them.

   (b) Suppose I tell you that 5 is a generator mod 73. Compute the total number of generators mod 73 and write down a full list of generators.

3. (a) Let $p > 2$ be a prime. Show that a is a generator mod p if and only if $a^{(p-1)/q} \not\equiv 1 \bmod p$ for all prime divisors q of $p-1$.

   (b) Use part (a) to prove that 3 is a generator mod 31.

4. (a) Find generators of $(\mathbb{Z}/13\mathbb{Z})^\times$ and $(\mathbb{Z}/17\mathbb{Z})^\times$.

   (b) Solve the congruence equation $x^3 \equiv 5 \bmod 13$.

   (c) Solve the congruence equation $4^x \equiv 13 \bmod 17$.

5. Show that $x^2 \equiv 2 \bmod 7^n$ has a solution for all $n \geq 1$.