Worksheet 16

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

1. (a) Let b, n, k be integers with $\gcd(b, n) = 1$ and $\gcd(k, \varphi(n)) = 1$. Prove that the congruence $x^k \equiv b \bmod n$ has a unique solution mod n. Explicitly, what is the solution?
   (b) Solve $x^{17} \equiv 11 \bmod 29$.
2. (a) Prove the function $f : (\mathbb{Z}/29\mathbb{Z})^\times \to (\mathbb{Z}/29\mathbb{Z})^\times$ given by $f([x]) = [x]^{17}$ is bijective.
   (b) Reinterpret your result from problem 1 as a statement about the k-th power map on $(\mathbb{Z}/n\mathbb{Z})^\times$.

The next few problems explore the structure of $(\mathbb{Z}/61\mathbb{Z})^\times$. Find a generator a of $(\mathbb{Z}/61\mathbb{Z})^\times$ and make a table of all the powers of a mod 61. (You won't have to try that hard to find a generator!)

2. Use your table to solve the following equations in $\mathbb{Z}/61\mathbb{Z}$:
   (a) $x^2 = [22]$
   (b) $x^3 = [23]$
3. How many perfect squares are there in $(\mathbb{Z}/61\mathbb{Z})^\times$? Perfect cubes? 5th powers?
4. How many elements of $(\mathbb{Z}/61\mathbb{Z})^\times$ have order 2? 3? 4? 5? 6? 7? Do you see a pattern?
5. Since $\varphi(100) = 40$, Euler's theorem says $a^{40} \equiv 1 \bmod 100$ for all integers a with $\gcd(a, 100) = 1$. Prove that you can do better, by showing that $a^{20} \equiv 1 \bmod 100$ for all a with $\gcd(a, 100) = 1$.
6. Let a, b, n be integers with $\gcd(a, n) = \gcd(b, n) = 1$ and $n > 1$.
   (a) $(*)$ Suppose that $\operatorname{ord}_n(a) = m$ and $\operatorname{ord}_n(b) = \ell$ and $\gcd(m, \ell) = 1$. Prove that $\operatorname{ord}_n(ab) = m\ell$.
   (b) More generally, is it true that $\operatorname{ord}_n(ab) = \operatorname{lcm}(\operatorname{ord}_n(a), \operatorname{ord}_n(b))$?