Worksheet 15

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

1. For $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$, let f be the function f from Monday's worksheet. That is, $f([x]) = [a]\cdot[x]$ for $[x] \in (\mathbb{Z}/n\mathbb{Z})$.

   (a) What can you say about the products $\prod_{[b]\in(\mathbb{Z}/n\mathbb{Z})^\times} [b]$ and $\prod_{[b]\in(\mathbb{Z}/n\mathbb{Z})^\times} f([b])$?

   (b) $(*)$ Let a, n be integers with $\gcd(a, n) = 1$ and $n > 1$. Prove that $a^{\varphi(n)} \equiv 1 \bmod n$. *(Hint: use the previous part.)*

   (c) Let p be a prime. Prove that for any positive integer a with $p \nmid a$, $a^{p-1} \equiv 1 \bmod p$.

2. For any integers a, n with $\gcd(a, n) = 1$ and $n > 1$, what does the result of 1(b) tell you about the size of $\mathrm{ord}_n(a)$?

3. $(*)$ Let a, n be integers with $\gcd(a, n) = 1$ and $n > 1$. Prove that for integers ℓ, k we have $a^k \equiv a^\ell \bmod n$ if and only if $k \equiv \ell \bmod \mathrm{ord}_n(a)$.

4. (Some various computations)

   (a) Compute $3^{201} \bmod 11$.

   (b) Compute $2^{2^{15}} \bmod 23$.

   (c) Without running the Euclidean algorithm, find the inverse of 3 mod 118.

   (d) Find all primes p such that $\mathrm{ord}_p(3) = 12$.

5. Let a, n be integers such that $\gcd(a, 91) = \gcd(n, 91) = 1$. Prove that $n^{12} - a^{12}$ is divisible by 91. *(Note that $91 = 7 \cdot 13$.)*

6. (a) Find all solutions to $x^5 \equiv 11 \bmod 18$. *(Hint: what does 1(b) tell you?)*

   (b) Suppose you have a congruence of the form $x^k \equiv b \bmod n$. What conditions do you have to impose on k, b, n to generalize you method from part (a)? Come up with a conjecture, and try to prove it!