Worksheet 19

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

1. $(*)$ Prove that $\sum_{d|n} \varphi(d) = n$. *(Hint: start by proving it for primes first.)*
2. $(*)$ Recall from worksheet 18 that for prime p and positive integer d, $N_p(d)$ denotes the number of elements of order d in $(\mathbb{Z}/p\mathbb{Z})^\times$. Prove that $N_p(p-1) > 0$, i.e. $(\mathbb{Z}/p\mathbb{Z})^\times$ always has a generator.

One important consequence of always having a generator mod p is as follows. Fix a prime p and let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Then for any $[a] \in (\mathbb{Z}/p\mathbb{Z})^\times$, we have $a \equiv g^k \bmod p$ for integer $k \geq 0$. By what we know about orders, there is a unique such choice of k with $0 \leq k \leq p-1$. The **logarithm** of $[a]$ relative to g is denoted $\log_g(a)$ and is defined by $\log_g(a) = k$.

3. Let p be a prime and let g be a generator mod p. Prove the following properties of logarithms:
   (a) $\log_g(1) = 0$.
   (b) $\log_g(ab) \equiv \log_g(a) + \log_g(b) \bmod p-1$.
   (c) $\log_g(a^k) \equiv k \cdot \log_g(a) \bmod p-1$.
4. (a) Show that 3 is a generator mod 17, and create a table of $\log_3(a)$ for $[a] \in (\mathbb{Z}/17\mathbb{Z})^\times$. Use your table of logarithms to help you solve the congruence $6x^{12} \equiv 11 \bmod 17$.
   (b) Solve the congruence $7^x \equiv 6 \bmod 17$.
5. Solve problems 7 and 5 from worksheets 17 and 18 respectively if you haven’t done so already. They’ll be very helpful for Wednesday!