Math 345 – Monday 11/13/17

Exercise 42. Recall, for an integer a with $\gcd(a, n) = 1$, the *order* of $a \pmod{n}$, written $|a|$ or $|a|_n$, is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$. We call a a *primitive root* (mod n) if $|a|_n = \phi(n)$.

(a) Compute the orders of a for $1 \leq a < n$ with $\gcd(a, n) = 1$, for $n = 4, 8$, and 13.
(b) Define $\psi_n(k) = \#\{1 \leq a < p \mid |a| = k\}$ (as in class). Compute $\psi_n(k)$ for $1 \leq k \leq \phi$ for $p = 13$ and $p = 37$ (use a computer to generate data).
(c) Prove that if $k \nmid \phi(n)$, then $\psi_n(k) = 0$.
(d) List the primitive roots modulo 13.
For each primitive root ξ, for which k is ξ^k also a primitive root (mod 13)?
(e) List the primitive roots modulo 37.
For each primitive root ξ, for which k is ξ^k also a primitive root? (mod 37)
(f) For each of $n = 8$, 10, and 12, answer the following: Are there any primitive roots modulo n? If so, list them. If not, what is the largest order occurring modulo n?

Exercise 43. A function $f(n)$ that satisfies the multiplication formula $f(mn) = f(m)f(n)$ for all numbers m and n with $\gcd(m, n) = 1$ is called a *multiplicative function.* For example, we have seen that Eulers phi function $\phi(n)$ is multiplicative and that $F(n) = \sum_{d|n} \phi(n)$ is multiplicative. Now suppose that $f(n)$ is any multiplicative function, and define a new function

$$g(n) = f(d_1) + f(d_2) + \cdots + f(d_r),$$

where $1 = d_1 < d_2 < \cdots < d_{r-1} < d_r = n$ are the divisors of n.

Prove that $g(n)$ is a multiplicative function.

Exercise 44. Define $\lambda(n)$ by factoring n into a product of primes,

$$n = p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell},$$

with $p_1 < p_2 < \cdots < p_\ell$ prime, and then setting

$$\lambda(n) = (-1)^{k_1+k_2+\cdots+k_\ell}, \qquad \text{with} \quad \lambda(1) = 1.$$

For example, since $1728 = 2^6 \cdot 3^3$, we have $\lambda(1728) = (-1)^{6+3} = (-1)^9 = -1$.

(a) Compute $\lambda(30)$ and $\lambda(504)$.
(b) Prove that $\lambda(n)$ is a multiplicative function.
(c) We now define a new function $G(n)$ by the formula

$$G(n) = \lambda(d_1) + \lambda(d_2) + \cdots + \lambda(d_r),$$

where $1 = d_1 < d_2 < \cdots < d_{r-1} < d_r = n$ are the divisors of n.

Explicitly compute $G(n)$ for each $1 \leq n \leq 18$.
(d) Use your computations to make a guess as to the value of $G(n)$. Use your guess to find the value of G(62141689) and G(60119483). (You can find the factorizations of these large numbers on wolframalpha.com.)
(e) Prove that your guess in (d) is correct. (Use Exercise 43.)