Math 322 Fall 2016
Number Theory HW 9
Due Friday, November 17

You may *not* discuss the starred problem with classmates, though you should of course feel free to discuss it with me as much as you like. Linguistic precision is important for this problem.

($\star$) **Starred Problem:** Let b be an inverse of a modulo n. Prove that $\operatorname{ord}_n a = \operatorname{ord}_n b$.

For the remainder of these problems, I encourage you to collaborate with your classmates, as well as to discuss them with me.

1. Prove that if n is a natural number, then $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$.

2. **Definition 1.** The *von Mangoldt function* Λ is defined by

$$\Lambda(n) = \begin{cases} \log p & n = p^k \text{ for } p \text{ prime}, k \in \mathbb{N} \\ 0 & \text{otherwise} \end{cases}$$

   (a) Show that $\sum_{d|n} \Lambda(d) = \log n$ for any natural number n.
   (Hint: recall $\log(a^k b^\ell) = k \log(a) + \ell \log(b)$).

   (b) Use Möbius inversion to show that

$$\Lambda(n) = -\sum_{d|n} \mu(d) \log d.$$

   (Hint: treat the case $n = 1$ separately).

3. (a) Compute $\operatorname{ord}_{11} 3$
   (b) Compute $\operatorname{ord}_{10} 7$
   (c) Show that 5 is a primitive root of 6.
   (d) Show that 12 has no primitive roots.

4. Let p be a prime with $p \equiv 1 \mod 4$. Let r be a primitive root modulo p. Prove that $-r$ is also a primitive root modulo p.

   (Hint: Observe that if $p \equiv 1 \mod 4$ then $4|\phi(p)$).

5. Find an example of a prime $q \equiv 3 \mod 4$ and a primitive root r modulo q such that $-r$ is not a primitive root modulo q.

6. Fix natural numbers n and $a > 1$, and set $m = a^n - 1$. Prove that $\mathrm{ord}_m\, a = n$. Conclude that $n|\phi(m)$.

7. Find a complete set of incongruent primitive roots of 17.

8. Let $p > 2$ be a prime and

$$f(x) = (x-1)(x-2)\dots(x-p+1) - x^{p-1} + 1 = 1 - x^{p-1} + \prod_{i=1}^{p-1}(x-i).$$

   Use Lagrange's theorem to show that every coefficient of this polynomial is divisible by p (i.e. the polynomial is 0 mod p).

   (Hint: What is the coefficient of the x^{p-1} term? What degree does this polynomial really have? How many roots does it have modulo p?)