Math 322 Fall 2016
Number Theory HW 9 Solutions
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 $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$.

   Solution: We see that $n, n+1, n+2, n+3$ are all different equivalence classes modulo 4. But there are only four equivalence classes modulo 4, so there is some $0 \leq i \leq 3$ such that $4|n+i$. But then $n+i$ is divisible by a square of a prime, so $\mu(n+i) = 0$.

   Thus $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3)$ is a product of four numbers, at least one of which is zero, so the product is zero.

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 $\log(a^k b^\ell) = k\log(a) + \ell\log(b)$).

   Solution:

   Let $n = \prod_{i=1}^{n} p_i^{k_i}$. Then for any i n has exactly k_i divisors that are a nonzero power of p_i: these divisors are $p_i, p_i^2, \ldots, p_i^k$. And we know that $\Lambda(d) = 0$ for any divisor

d that does not have this form. Thus

$$\begin{aligned}\sum_{d|n}\Lambda(d) &= \sum_{i=1}^{n}\left(\sum_{j=1}^{k_i}\Lambda(p_i^j)\right)\\ &= \sum_{i=1}^{n}\left(\sum_{j=1}^{k_i}\log(p_i)\right)\\ &= \sum_{i=1}^{n}k_i\log(p_i) = \sum_{i=1}^{n}\log(p_i^{k_i})\\ &= \log\left(\prod_{i=1}^{n}p_i^{k_i}\right) = \log(n).\end{aligned}$$

(b) Use Möbius inversion to show that

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

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

Solution: Suppose $n = 1$. Then $\Lambda(1) = 0$ and $-\sum_{d|1}\mu(d)\log(d) = -\mu(1)\log(1) = -1\cdot 0 = 0$.

Now suppose $n > 1$. In part (a) we proved that $\log(n)$ is the summatory function of $\Lambda(n)$. Thus by Möbius inversion we have

$$\begin{aligned}\Lambda(n) &= \sum_{d|n}\mu(d)\log(n/d) = \sum_{d|n}\mu(d)\left(\log(n)-\log(d)\right)\\ &= \sum_{d|n}\mu(d)\log(n) - \sum_{d|n}\mu(d)\log(d)\\ &= \log(n)\sum_{d|n}\mu(d) - \sum_{d|n}\mu(d)\log(d).\end{aligned}$$

But we proved the summatory function of μ is zero when $n \neq 1$ (that is, ι from problem (1) is the summatory function of μ), and thus the left hand sum is zero. So we have

$$\begin{aligned}\Lambda(n) &= \log(n)\cdot 0 - \sum_{d|n}\mu(d)\log(d)\\ &= -\sum_{d|n}\mu(d)\log(d)\end{aligned}$$

as desired.

3. (a) Compute $\mathrm{ord}_{11}\,3$

Solution: $\phi(11) = 10$ so the order must divide 10. So we check

$$\begin{aligned} 3^1 &= 3 \equiv 3 \mod 11 \\ 3^2 &= 9 \equiv 9 \mod 11 \\ 3^5 &= 9^2 \cdot 3 \equiv (-2)^2 \cdot 3 = 12 \equiv 1 \mod 11 \end{aligned}$$

so $\operatorname{ord}_{11} 3 = 5$.

(b) Compute $\operatorname{ord}_{10} 7$ **Solution:** $\phi(10) = 4$ so we know the order must divide 4. We compute

$$\begin{aligned} 7^1 &= 7 \equiv 7 \mod 10 \\ 7^2 &= 49 \equiv 49 \equiv -1 \mod 10 \end{aligned}$$

Thus the only option left is 4, so $\operatorname{ord}_{10} 7 = 4$. We can also check this by hand, to see

$$7^4 = 49^2 \equiv (-1)^2 \equiv 1 \mod 10$$

or

$$7^4 = 2401 \equiv 1 \mod 10.$$

(c) Show that 5 is a primitive root of 6. **Solution:** We see that $\phi(6) = 2$, so we need to find an element of order 2. We see that $\operatorname{ord}_6 1 = 1$, but

$$\begin{aligned} 5^1 &= 5 \equiv 5 \mod 6 \\ 5^2 &= 25 \equiv 1 \mod 6 \end{aligned}$$

so $\operatorname{ord}_6 5 = 2$ as desired. 5 is a primitive root modulo 6.

(d) Show that 12 has no primitive roots. **Solution:** We compute $\phi(12) = 4$, so we want to show no element has order 4 modulo 12. We only need to check the numbers relatively prime to 12 and less than 12, which are 1, 5, 7, 11. We see

$$\begin{aligned} 1^1 &= 1 \equiv 1 \mod 12 \\ 5^2 &= 25 \equiv 1 \mod 12 \\ 7^2 &= 49 \equiv 1 \mod 12 \\ 11^2 &= 121 \equiv 1 \mod 12 \end{aligned}$$

so every integer relatively prime to 12 has order either 1 or 2 modulo 12; thus there are no primitive roots modulo 12.

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 $4|\phi(p)$).

Solution: We know that $\operatorname{ord}_p r = \phi(p) = p - 1$ is divisible by 4. We see that $(-r)^{p-1} = (-1)^{p-1} r^{p-1} = r^{p-1} \equiv 1 \mod p$.

Now set $n = \text{ord}_p(-r)$; we see that $n|p-1$. We have $(-1)^n r^n \equiv (-r)^n \equiv 1 \mod p$, and since $(-1)^n \equiv \pm 1 \mod p$ we know that $(r)^n \equiv \pm 1 \mod p$.

Suppose $r^n \equiv (-1)^n \equiv -1 \mod p$. Then $r^{2n} \equiv 1 \mod p$, so we must have $2n = \text{ord}_p r = p-1$. But then n is even, so $(-1)^n \equiv 1 \mod p$ which is a contradiction.

So suppose $r^n \equiv (-1)^n \equiv 1 \mod p$. Then $p-1|n$, and since $n|p-1$ we must have $n = p-1 = \phi(p)$ as desired.

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.

   Solution: 3 is a prime equivalent to 3 modulo 4 (clearly). $\phi(3) = 2$, and we see that $2^1 \not\equiv 1 \mod 3, 2^2 \equiv 1 \mod 3$ so $\text{ord}_3 2 = 2$ and 2 is a primitive root modulo 3.

   But $-2 \equiv 1 \mod 3$, and $\text{ord}_3 1 = 1 \neq 2$ so -2 is not a primitive root modulo 3.

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

   Solution: We see that $m|a^n - 1$ so $a^n \equiv 1 \mod m$. Suppose $1 \leq m < n$. Then $1 < a^m < a^n - 1 = m$, so $a^m \not\equiv 1 \mod m$. Thus by definition $\text{ord}_m a = n$.

   But by theorem we know that $\text{ord}_m a|\phi(m)$, so we must have $n|\phi(m)$.

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

   Solution: We first compute that, say, 3 is a primitive root of 17. We see that

$$\begin{aligned} 3^1 &\equiv 3 \not\equiv 1 \mod 17 \\ 3^2 &\equiv 9 \not\equiv 1 \mod 17 \\ 3^4 &\equiv 81 \equiv 13 \not\equiv 1 \mod 17 \\ 3^8 &\equiv 169 \equiv -1 \not\equiv 1 \mod 17 \end{aligned}$$

   and since $\text{ord}_{17} 3|\phi(17) = 16$ we must have $\text{ord}_{17} 3 = 16$ and thus 3 is a primitive root modulo 17.

   Now we know that the complete set of primitive roots is just 3 raised to all the powers relatively prime to 16. Thus the set of primitive roots is

$$\begin{aligned} 3^1 &\equiv 3 \mod 17 & 3^3 &\equiv 10 \mod 17 \\ 3^5 &\equiv 5 \mod 17 & 3^7 &\equiv 11 \mod 17 \\ 3^9 &\equiv 14 \mod 17 & 3^{11} &\equiv 7 \mod 17 \\ 3^{13} &\equiv 12 \mod 17 & 3^{15} &\equiv 6 \mod 17. \end{aligned}$$

   (We can compute these residues by hand, or by multiplying each previous residue by $3^2 = 9$).

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?)

Solution: Notice that the coefficient of x^{p-1} is actually 0, so f has degree $n-2$ at most. But for any $1 \leq n \leq p-1$ we have

$$f(n) = 0 - n^{p-1} + 1 \equiv -1 + 1 \equiv 0 \mod p$$

by Fermat's little theorem. Thus f has at least $p-1$ roots modulo p.

Suppose f has some coefficient not divisible by p. Then we can write a polynomial $g(x) = a_k x^k + \dots + a_0$ with $p \not| a_k$ and $k < p-1$, such that the coefficients of g equivalent to the coefficients of f modulo p, so that $g(x) \equiv f(x) \mod p$ for any x. Then g also has at least $p-1$ roots, but by Lagrange's theorem we know that g has at most $k < p-1$ roots, which is a contradiction. Thus all of f's coefficients are divisible by p.