Number Theory – HW 4-5

Number-Theoretic Functions

Problem 1 *Find all positive integers n with $\sigma(n) = 24$.*

Problem 2 *Let σ_k be the number-theoretic function*

$$\sigma_k(n) = \sum_{d|n} d^k.$$

(a) *Simplify*

$$\sum_{d|n} \mu(d)\sigma_k(n/d).$$

Hint: *Remember Mobius Inversion Formula.*

(b) *Prove that the following function is multiplicative:*

$$S_k(n) = \sum_{d|n} \mu(d)\sigma_k(d)$$

Hint:

(H1) We know that μ is multiplicative.

(H2) Show $\sigma_k(n)$ is multiplicative.

(H3) We know that if $f(n)$ is multiplicative, then $\sum_{d|n} f(d)$ is multiplicative.

Problem 3 (a) *Show that the number-theoretic function $f(n) = (-1)^{n-1}$ is multiplicative.*

(b) *Let g be the number-theoretic function*

$$g(n) = \sum_{d|n} \mu(d)f(d).$$

Prove that $g(n) = 0$ if n is not a power of 2.

Euler ϕ-Function and Euler's Generalization of Fermat's Little Theorem

Problem 4 *Find all positive integers n such that $\phi(n)$ is odd.*

Problem 5 *We showed in class that there is no positive integer n such that $\phi(n) = 14$. Find the smallest integer $m > 14$ such that no positive integer n exists satisfying $\phi(n) = m$. Explain your reasoning.*

Learning outcomes: Problems 1, 3, 4, 9 and 11 are due 11/14. Problems 12, 13,15, 16 and 17 are due 11/21.

Problem 6 *Show that if $n > 1$, then*

$$\prod_{p|n} p \geq \frac{n}{\phi(n)}.$$

Hint:

(H1) $\phi(n) = n \cdot \prod_{p|n}(1 - \frac{1}{p})$ *where p is always prime.*

(H2) $\frac{1}{p} \leq 1 - \frac{1}{p}$ *if p is prime.*

Problem 7 *Find all positive integers n such that $\phi(n) \mid 3n$.*

Hint:

(H1) *Can n be odd?*

(H2) *If $n = 2^k \cdot m$ for odd m, what can you say about $n/\phi(n)$? Hence, what can you say about m?*

(H3) *Do you know any prime number that divides m?*

Problem 8 (a) *Show $\phi(2m) = \phi(m)$ if m is odd.*

(b) *Show $\phi(3m) = \phi(2m)$ if m is even and not divisible by 3.*

(c) *Use previous results to show that, for any given k, if the equation $\phi(n) = k$ has exactly one solution n, then $36 \mid n$.*

(d) *Can you give two integers m and n such that $36 \mid m$, n and $\phi(m) = \phi(n)$?*
(If you can, this shows that the converse of the previous result is not true.)

Problem 9 *Suppose that $m = pq$, and $\phi = (p - 1)(q - 1)$ where p, q are real numbers. Find a formula for p and q, in terms of m and ϕ. Supposing that $m = 39,247,771$ is the product of two distinct primes p and q, deduce the factors of m from the information that $\phi(m) = 39,233,944$.*
Remark: A nice Cryptogtaphy problem!

Problem 10 *Let N be a perfect number. Show that*

$$\prod_{\substack{p|N \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right) < \frac{1}{2}.$$

Hint:

(H1) *A perfect number is a number sum of whose divisors is equal to itself. That is, $\sigma(n) = n$.*

(H2) *You might want to check equivalent definition(s) of σ from your book.*

Problem 11 *Let $p > 0$ be an odd prime and $n = 3^p + 1$. Let q be an odd prime divisor of n.*

(a) *What is the order of 3 modulo n?*

(b) *Show that q is of the form $q = 2kp + 1$ for some integer $k > 0$.*

Problem 12 *Use Fermat's Little Theorem to find a very short calculation of*

$$3^{37,123,878,237,982,731,602} \pmod{101}$$

Problem 13 (a) *Write 1234 in base 2.*

(b) *Calculate $2^2, 2^4, \ldots, 2^k \pmod{789}$ where $2^k \leq 1234$ and $2^{k+1} > 1234$.*

(c) *Use $(a), (b)$ to calculate $2^{1234} \pmod{789}$.*

(d) *Calculate $\phi(789)$.*

(e) *Use parts $(b), (d)$ and a similar idea to (a) to obtain the same result a lot faster.*

Problem 14 *Let n be an integer with $n > 6$. Show that*

$$\phi(n) > \sqrt{n}.$$

Hint:

(H1) You may want to deal with two cases: $n = 2m$ where m is odd and all other cases.

(H2) When is $k - 1 > k/2$?

(H3) When is $p - 1 > \sqrt{p}$?

(H4) When is $p - 1 > \sqrt{2p}$?

Primite Roots

Problem 15 *Describe all primes p such that*

$$x^4 + x^3 + x^2 + 2 + 1 \equiv 0 \pmod{p}$$

Hint: *Can you multiple the given polynomial and obtain $x^m - 1$ for some m? If yes, you can then use the fact that m must divide $\phi(p)$.*

Problem 16 (a) *Use the fact that 3 is a primitive root modulo the prime 79 to find all x satisfying*

$$x^{40} \equiv 2 \pmod{79}.$$

Hint:

(H1) What can you say about the order of x modulo 79?

(H2) Test all possibilities for the order of x. Make sure that your solution for each order actually have the desired order.

(b) *Is 2 a primitive root modulo 79?*

Problem 17 *Factor* $n = 2^{30} - 1$ *completely.*

Hint:

(H1) First, calculate all odd m *such that* $\phi(m) \mid 30$.

(H2) If m *is odd, then* $(m, 2) = 1$ *and hence* $m \mid n$. *The least common multiple of all such* m *is a divisor of* n. *Let's call this LCM* ℓ.*(Why not even* m*?)*

(H3) Calculate prime numbers $q < \sqrt{n/\ell}$ *such that* $30 \mid (q-1)$. *(You do not really need to calculate* $\sqrt{n/\ell}$. *Instead try to use* $2^{15}/2^k$ *such that* 2^k *is largest integer less than* ℓ.*)*

(H4) Test whether $2^{30} \equiv 1 \pmod{q}$ *for each prime obtained in the previous step. If yes, then* $q \mid n$.

Here, we use the theorem "If order of m modulo n is k and $m^s \equiv 1 \pmod{n}$ then $k \mid s$."