Problem Set 3

Student handout

Totients, divisor sums, and exact periods

8 problems | 100 points + 10 optional challenge points | Suggested time: 3–4 hours

Preparation. Course packet Sections 5.3–5.9; modular inverses and CRT from Chapter 4. Posets, complex numbers, and field extensions are not required.

Name: _____ **Due:** _____

Instructions. Write on separate paper. Show the arithmetic and justify each proof. You may use unique factorization, Bézout, CRT, Euler's theorem, and Möbius inversion. When asked to prove a statement, give the argument rather than citing that same statement from the book. Computation may check examples; it does not replace a proof.

Notation. All divisors are positive. $\tau(n) = \sum_{d|n} 1$, $\sigma(n) = \sum_{d|n} d$, $\mathbf{1}(n) = 1$, and $\mathrm{id}(n) = n$. The function ε is 1 at $n = 1$ and zero otherwise. Convolution means $(f * g)(n) = \sum_{d|n} f(d)g(n/d)$.

I. Prime powers and reversible arithmetic

1. A small table, several different rules [12 points]

(a) Compute $\varphi(n), \tau(n), \sigma(n), \mu(n)$ for $n = 1, 16, 27, 30, 180$. Show the prime-power calculations for 180. (8)

(b) Give counterexamples showing that φ, τ, and μ are not completely multiplicative. State the hypothesis under which they are multiplicative. (4)

2. Euler needs a unit [12 points]

(a) Use extended Euclid to find an integer certificate for the inverse of 7 modulo 40. Give the inverse between 0 and 39. (4)

(b) Compute $\varphi(40)$ using $40 = 8 \cdot 5$. Explain why multiplying $\varphi(4)$ and $\varphi(10)$ would not be justified. (3)

(c) Use Euler's theorem to compute $7^{2026} \pmod{40}$, then check the result separately modulo 8 and 5. (3)

(d) Does Euler's theorem imply $2^{16} \equiv 1 \pmod{40}$? Identify the failed hypothesis and compute the actual remainder. (2)

3. Why convolution preserves multiplicativity [12 points]

Let f, g be multiplicative functions, and let $\gcd(m, n) = 1$.

(a) Prove that every divisor of mn is uniquely ab with $a \mid m$ and $b \mid n$. (4)

(b) Use this correspondence to prove that $h = f * g$ is multiplicative, including the condition at 1. Indicate both places coprimality is used. (6)

(c) Taking $f = g = \mathbf{1}$, use $630 = 18 \cdot 35$ to compute $\tau(630)$ without listing its divisors. (2)

II. Recover the exact contribution

4. A gcd partition explains the totient sum [12 points]

(a) Partition $\{1, \dots, n\}$ according to $\gcd(r, n)$ and prove $\sum_{d \mid n} \varphi(d) = n$. Explain the term $\varphi(1)$. (6)

(b) Apply Möbius inversion to recover a formula for $\varphi(n)$. Use it to compute $\varphi(84)$, displaying every nonzero term. (6)

5. Recover a hidden arithmetic function [14 points]

Suppose $F(n) = \sum_{d \mid n} f(d)$ and the recorded data are

n	1	2	3	6	9	18
$F(n)$	2	5	6	16	16	45

(a) Recover f at these six inputs by successive subtraction. Check $f(18)$ independently by Möbius inversion. (6)

(b) Now assume the rule is $F(n) = \sigma(n) + \tau(n)$ for every n. Find and prove a formula for $f(n)$ valid for all positive integers. (6)

(c) Is the resulting f multiplicative? Does your answer affect the validity of inversion? (2)

6. Convolve Möbius with itself [12 points]

Put $h = \mu * \mu$.

(a) For a prime p, determine $h(p^k)$ for every $k \geq 0$. Use $p^0 = 1$. (5)

(b) Use Problem 3 to compute $h(30), h(180), h(8)$. (3)

(c) An integer is *cubefree* if no prime cube divides it. Give a formula for $h(n)$ in terms of whether n is cubefree and the number of primes occurring to exponent exactly 1. (4)

III. Two counting applications

7. Words and necklaces of length ten [14 points]

Let $P(n)$ count binary labeled words of length n whose least rotational period is n. Necklaces identify words that differ by a rotation; reflections are not identified.

(a) Explain why $2^n = \sum_{d|n} P(d)$ and derive the inversion formula for $P(n)$. (4)

(b) Compute $P(d)$ for $d = 1, 2, 5, 10$. Count the necklaces of full period 10. (5)

(c) Count all binary necklaces of length 10, including shorter periods. Explain why dividing 2^{10} by 10 is invalid. (5)

8. Count squarefree integers without testing them one by one [12 points]

Recall that squarefree means no prime square divides the integer.

(a) Prove the indicator identity $\mu(n)^2 = \sum_{d^2|n} \mu(d)$. *Hint:* examine the primes whose squares divide n. (5)

(b) Let $Q(N)$ count squarefree integers in $\{1, \dots, N\}$, including 1. Exchange finite sums to prove

$$Q(N) = \sum_{1 \le d \le \sqrt{N}} \mu(d) \left\lfloor \frac{N}{d^2} \right\rfloor.$$

Use this formula to compute $Q(50)$. (7)

Optional challenge: a two-coordinate totient [10 extra points]

Let $J_2(n)$ count ordered pairs (u, v) with $1 \le u, v \le n$ and $\gcd(u, v, n) = 1$, where the gcd is taken over all three integers.

(a) Group all n^2 pairs by $\gcd(u, v, n)$ to prove $n^2 = \sum_{d|n} J_2(d)$. (4)

(b) Invert the sum and factor the result to prove

$$J_2(n) = n^2 \prod_{p|n} (1 - p^{-2}).$$

Compute $J_2(12)$. (6)