

Outline notes for PS08
Math 126

Definitions. (Ch. 20) Multiplicative function. (Ch. 21) Order of a modulo p , primitive root modulo p .

Problem outlines.

18.2(a). *Assume:* $m = pq$, p, q prime, $ed \equiv 1 \pmod{\varphi(m)}$, $a \in \mathbb{Z}$. (e is encoding exponent, d is decoding exponent.)

Conclude: $(a^e)^d \equiv a \pmod{m}$.

Suggestion: Chinese Remainder Theorem.

20.2. (a) *Assume:* $m, n \in \mathbb{Z}$, $\gcd(m, n) = 1$.

Conclude: $\lambda(mn) = \lambda(m)\lambda(n)$.

Suggestion: FTA.

(b) *Assume:* $f(n)$ multiplicative, $g(n) = f(d_1) + \cdots + f(d_r)$, where d_1, \dots, d_r are the divisors of n . $m, n \in \mathbb{Z}$, $\gcd(m, n) = 1$.

Conclude: $g(mn) = g(m)g(n)$.

21.2. (b) *Assume:* $m, a \in \mathbb{Z}$, $\gcd(a, m) = 1$.

Conclude: $e_m(a)$ divides $\varphi(m)$.

Suggestion: Try contradiction.