PRIME PROBLEMS:
PRIMITIVE ROOTS AND ARITHMETIC FUNCTIONS

Problem 1.
(a) Find a primitive root mod 13.
(b) Find all primitive roots mod 13.

Solution. (a) We need to find a \( \in \mathbb{Z} \) with order \( \varphi(13) = 12 \), so it suffices to find a \( \in \mathbb{Z} \) coprime to 13 with \( a^4 \not\equiv 1 \mod 13 \) and \( a^8 \not\equiv 1 \mod 13 \). We compute \( 2^4 \equiv 3 \mod 13 \) and \( 2^8 \equiv -1 \mod 13 \), so 2 works. 
(b) From a homework ord(\( \alpha^n \)) = ord(\( \alpha \))/gcd(e, ord(\( \alpha \))). Thus, the primitive roots are 2, 2\(^5\), 2\(^7\), 2\(^{11}\), and indeed we know there must be \( \varphi(12) = 2 \cdot 2 = 4 \) elements of order 12. Evaluating the powers, these 

Problem 2. What is the order of 6 mod 19?

Solution. Let \( d = \text{ord}_9 (2) \) be the order of 6 mod 19. \( \varphi(19) = 18 = 2 \cdot 3^2 \), so \( d = 2, 3, 6, 9, 18 \). \( 6^6 \equiv (-2)^3 \equiv -8 \), so \( d = 9 \) and \( 6^9 \equiv (-8) \cdot (-2) \cdot 6 \equiv -18 \equiv 1 \). Thus, \( d = 9 \).

Problem 3. Find a primitive root mod 11\(^{100}\).

Solution. We know for an odd prime \( p \) that: (a) there is some \( a \in \mathbb{Z} \) that is a primitive root mod \( p \); (b) if \( a \in \mathbb{Z} \) is a primitive root mod \( p \), either \( a \) or \( a + p \) is a primitive root mod \( p^2 \); (c) if \( a \in \mathbb{Z} \) is a primitive root mod \( p^2 \) then it is a primitive root mod \( p^e \) for all \( e \geq 2 \). Thus, we compute: (a) 2 is primitive mod 11 since \( 2^2 \not\equiv 1 \mod 11 \) and \( 2^5 \not\equiv 1 \mod 11 \); (b) \( \text{ord}_{11^2} (2) \) is either 10 or 110, and since \( 2^{110} \equiv 128 \cdot 8 \equiv 7 \cdot 8 \not\equiv 1 \mod 11^2 \), 

Problem 4. Suppose we have distinct \( \alpha, \beta \in (\mathbb{Z}/n)^* \). Show that ord(\( \alpha \beta \))| lcm(ord(\( \alpha \)), ord(\( \beta \))). Must we have equality?

Solution. Let \( d = \text{lcm}(\text{ord}(\alpha), \text{ord}(\beta)) \). Certainly \( \alpha^d = 1 = \beta^d \), so \( (\alpha \beta)^d = 1 \) and thus \( \text{ord}(\alpha \beta)|d \). If \( \alpha \) is not of order 2, then \( \beta = \alpha^{-1} \not\equiv \alpha \), and ord(\( \alpha \beta \)) = 1.

Problem 5. Find all solutions to \( x^5 \equiv -1 \mod 11^2 \)

Solution. Substituting \( x = 2^d \), and using the fact that \(-1 = 2^{55}\) (which we know because \( 2^{55} \) must have order 2) the congruence is equivalent to \( 5d \equiv 55 \mod 110 \), so we must have \( d \equiv 11 \mod 22 \), and the 5 solutions mod 110 are 11, 11 + 22, 11 + 2 · 22, 11 + 3 · 22, 11 + 4 · 22 = 11, 33, 55, 77, 99. Thus, the solutions to \( x^5 \equiv -1 \mod 11^2 \) are \( 2^{11}, 2^{33}, 2^{55}, 2^{77}, 2^{99} \). If we really wanted to we could evaluate these to be 112, -1, -1, -1, -1.

Problem 6. Find all solutions to \( x^4 \equiv 5 \mod 2^{100} \)

Solution. Recall that 5 has order \( 2^{e-2} \mod 2^e \), and that every invertible residue class mod \( 2^e \) can be written as \( \pm 5^d \). Therefore substituting \( x = \pm 5^d \), the equation implies \( 4d \equiv 1 \mod 8 \), which has no solutions.

Problem 7. Find all solutions to \( x^2 \equiv 16 \mod 77 \) (you may use the fact that 3, 2 are primitive roots mod 7, 11 respectively).

Solution. This is equivalent to solving \( x^2 \equiv 16 \mod 7 \) and \( x^2 \equiv 16 \mod 11 \). Both of these have the solution \( \pm 4 \), so there are 4 solutions mod 77 given by solving \( x \equiv \pm 4 \mod 7 \) and \( x \equiv \pm 4 \mod 11 \). \( x \equiv \pm 4 \mod 77 \) work, and so do \( x \equiv \pm 18 \mod 77 \) since \( 18 \equiv 4 \mod 7 \) and \( 18 \equiv -4 \mod 11 \). Note we didn’t even have to use primitive roots explicitly.
Problem 8. How many solutions does \( x^{11} \equiv -1 \mod 23^{1000000000} \) have?

Solution. There are clearly solutions because \( x \equiv -1 \) is a solution. The number of solutions is then \( \gcd(11, \varphi(n)) \) for \( n = 23^{1000000000} \), and since \( \varphi(23^{1000000000}) = 23^{999999999} \cdot 22 \), there are 11 solutions. Note we could have easily seen from our criterion that there are solutions since \((-1)^{\varphi(n)/\gcd(11, \varphi(n))} \equiv 1 \).

Problem 9. Show that there are no solutions to \( x^n \equiv -1 \mod 2^e \) for \( e \geq 3 \) and \( n \) even.

Solution. We know every invertible residue mod \( 2^e \) is congruent to \( \pm 5^d \) for a unique choice of \( \pm \) and \( d \) with \( 0 \leq d < 2^{e-2} \). Setting \( x = \pm 5^d \) and plugging in, we must have \( 5^ad \equiv -1 \mod 2^e \). By uniqueness, we can never write \(-1 \) as \( +5^d \), so there cannot be any solutions.

Problem 10. Suppose we have two functions \( f, g : \mathbb{N} \to \mathbb{C} \) with \( f(n) = \sum_{d|n} g(d) \), and suppose further that \( f(n) \) is zero if \( n \) is divisible by a nontrivial square (i.e. \( m^2 \) for \( m > 1 \)). Show that \( g(n) \) is zero for \( n \) divisible by a nontrivial cube.

Solution. By Möbius inversion, 
\[
g(n) = \sum_{de=n} f(d) \mu(e)
\]
If \( n \) is divisible by \( m^3 \) for \( m > 1 \), then for any factorization \( de = n \), either \( m^2|d \) or \( m^2|e \) in which case either \( f(d) = 0 \) or \( \mu(e) = 0 \).

Problem 11. Define a function \( f : \mathbb{N} \to \mathbb{C} \) implicitly by \( n^2 = \sum_{d|n} f(d) \). What is \( f(p^e q^f) \) for \( p, q \) distinct primes?

Solution. By Möbius inversion, \( f(n) = \sum_{d|n} d^2 \mu(n/d) \), so evaluating \( f(p^e) = (p^{e-1})^2(-1) + (p^e)^2 = p^{2e-2}(p^2-1) \), and similarly for \( f(q^f) \). The Dirichlet product of two multiplicative functions is multiplicative, so
\[
f(p^e q^f) = f(p^e) f(q^f) = p^{2e-2} q^{2f-2}(p^2 - 1)(q^2 - 1)
\]

Problem 12. Recall that \( \tau(n) = \sum_{d|n} 1 \). Express \( \sum_{d|n} \tau(d) \varphi(n/d) \) in terms of \( \sigma(n) = \sum_{d|n} d \).

Solution. This is easiest using the notion of Dirichlet product. Let \( u(n) = 1 \) for all \( n \in \mathbb{N} \) and \( N(n) = n \). Then \( \tau = u * u \) and we know \( N = u * \varphi \), so \( \tau * \varphi = u * u * \varphi = u * N = \sigma \).

Problem 13. Recall that \( \sigma_k(n) = \sum_{d|n} d^k \) for \( k \in \mathbb{Z} \). Show that \( n^k \sigma_{-k}(n) = \sigma(n) \).

Solution. We know if \( g(n) \) is multiplicative then \( f(n) = \sum_{d|n} g(d) \) is too. Thus, \( \sigma_k(n) \) is multiplicative for all \( k \), as is \( \rho_k(n) = n^k \sigma_{-k}(n) \). We just need to show that \( \rho_k \) and \( \sigma_k \) agree on prime powers:
\[
\rho_k(p^r) = (p^r)^k (1 + p^{-k} + (p^2)^{-k} + \cdots + (p^r)^{-k}) = (p^{r+k})^k + (p^{r-1+k})^k + (p^{r-2+k})^k + \cdots + 1 = \sigma_k(p^r)
\]