

Problem 1

For this problem just state the requested results; no proofs required.

- (i) State the Moebius Inversion Formula. Be sure to include any assumptions and any necessary quantifiers (e.g., “for all $n \in \mathbb{N}$ ”).

Solution: The Moebius Inversion formula states: “If $f(n) = \sum_{d|n} g(d)$ for all $n \in \mathbb{N}$, then $g(n) = \sum_{d|n} \mu(d)f(n/d)$ for all $n \in \mathbb{N}$.”

Remark: The quantifier “for all $n \in \mathbb{N}$ ” on each side of the implication is necessary. Without it, the statement would become false: If the formula $f(n) = \sum_{d|n} g(d)$, holds for a *particular* n -value, it does not follow that the corresponding formula on the other side, $g(n) = \sum_{d|n} \mu(d)f(n/d)$ holds for the same n -value.

- (ii) State the Primitive Root Theorem (which characterizes those positive integers that have a primitive root).

Solution: The positive integers that have a primitive root are exactly those of the form $1, 2, 4, p^\alpha$, and $2p^\alpha$ (where p is a prime and α a positive integer).

- (iii) Write down a perfect number that is divisible by $2^{11213} - 1$. (Hint: $2^{11213} - 1$ is a (very famous) prime.)

Solution: The given number is a Mersenne prime, $2^p - 1$. By Euler’s characterization of even perfect numbers, the number $2^{p-1}(2^p - 1) = \boxed{2^{11212}(2^{11213} - 1)}$ is perfect.

Problem 2

- (i) Compute the Legendre symbol $\left(\frac{28}{151}\right)$. (Show all work; for the key steps, indicate which rule/property of the Legendre symbol you are using. Note that 151 is prime.)

Solution: $\left(\frac{28}{151}\right) = \left(\frac{2^2 \cdot 7}{151}\right) \stackrel{\text{mult.}}{=} \left(\frac{2^2}{151}\right) \left(\frac{7}{151}\right) \stackrel{\text{squares}}{=} \left(\frac{7}{151}\right) \stackrel{\text{QR}}{=} (-1) \left(\frac{151}{7}\right) \stackrel{\text{period.}}{=} -\left(\frac{4}{7}\right) = -\left(\frac{2^2}{7}\right) \stackrel{\text{squares}}{=} \boxed{-1}$.

- (ii) Determine, with explanation, whether there exists an integer n such that $n^2 + 2$ is divisible by 2011. (Note that 2011 is prime.)

Solution: The given divisibility condition is equivalent to the congruence $n^2 \equiv -2 \pmod{2011}$. This congruence has a solution if and only if the Legendre symbol $\left(\frac{-2}{2011}\right)$ is equal to 1. Now, $\left(\frac{-2}{2011}\right) = \left(\frac{-1}{2011}\right) \left(\frac{2}{2011}\right)$, and by the formulas for $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$, we have $\left(\frac{-1}{2011}\right) = -1$ (since $2011 \equiv 3 \pmod{4}$), and $\left(\frac{2}{2011}\right) = -1$ (since $2011 \equiv 3 \pmod{8}$). Hence $\left(\frac{-2}{2011}\right) = (-1)(-1) = 1$, so there is an n with $n^2 + 2$ divisible by 2011.

- (iii) Suppose p is a prime greater than 7 such that 3, 5, and 7 are all quadratic nonresidues modulo p . Determine, with explanation, which (if any) of the integers $15(= 3 \cdot 5)$, $21(= 3 \cdot 7)$, $35(= 5 \cdot 7)$, $105(= 3 \cdot 5 \cdot 7)$ are quadratic residues modulo p , and which (if any) are quadratic nonresidues modulo p .

Solution: (This is a variation on Problem 24 from HW 7.) By the multiplicativity of the Legendre symbol, the product of two quadratic nonresidues is a residue (since $(-1)(-1) = 1$), while the product of three quadratic nonresidues is a nonresidue (since $(-1)(-1)(-1) = -1$). Of the given integers, 105 is a product of three quadratic nonresidues (namely, 3, 5, 7), while 15, 21, 35 are products of two quadratic nonresidues. Hence $\boxed{15, 21, 35}$ are **quadratic residues**, while $\boxed{105}$ is a **quadratic nonresidue**.

Problem 3

Given that 3 is a primitive root modulo 31, determine the following. (Be sure to show work; an answer alone without adequate justification, or with incorrect reasoning, will not earn credit.)

- (i) An integer a in the range $3 < a < 31$ that is also a primitive root modulo 31. (Only one such integer is needed, but it must be in the given range.)

Solution: Since 3 has order $\varphi(31) = 30$, 3^i has order $30/(30, i)$ (by the power order formula). Thus, 3^i will be a primitive root if and only if $(30, i) = 1$. In particular, $i = 7$ satisfies this condition, giving the primitive root 3^7 . Reducing mod 31 we get $3^7 \equiv 27^2 \cdot 3 \equiv (-4)^2 \cdot 3 \equiv 48 \equiv \boxed{17}$.

- (ii) An integer a in the range $1 < a < 31$ whose order modulo 31 is 4; if no such integer exists, explain why.

Solution: No such integer exists, since an order must be a divisor of $\varphi(31) = 30$, and 4 does not divide 30.

- (iii) An integer a in the range $1 < a < 31$ whose order modulo 31 is 10; if no such integer exists, explain why.

Solution: Since 10 is a divisor of $\varphi(31) = 30$, there exist integers of order 10. To find one, use the power order formula: Since 3 has order $\varphi(31) = 30$, 3^i has order $30/(30, i)$, which is equal to 10 if and only if $(30, i) = 3$. Taking $i = 3$ gives an integer with order 10, namely $3^i = \boxed{27}$.

Problem 4

- (i) Let f and g be an arithmetic functions and let $h = f \star g$ be the Dirichlet product of f and g . Write down an *explicit* formula for $h(12)$ in terms of the values $f(1), f(2), \dots, g(1), g(2), \dots$ (“Explicit” means a “plug-in ready” formula such as $f(1) + g(11) + f(3) + g(9) + f(5) + g(7)$, with all terms explicitly listed.)

Solution: $h(12) = \sum_{d|12} f(d)g(n/d) = \boxed{f(1)g(12) + f(2)g(6) + f(3)g(4) + f(4)g(3) + f(6)g(2) + f(12)g(1)}$.

- (ii) Characterize the positive integers n that have exactly 453 positive divisors. (Note that $453 = 3 \cdot 151$, and 151 is prime. Be sure to show work, include any conditions/constraints needed.)

Solution: (This is essentially Problem 31 from HW 5.) Writing n in the standard prime factorization $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ with distinct primes p_i and $\alpha_i \in \mathbf{N}$, the number of divisors of n is given by $\nu(n) = (\alpha_1 + 1) \dots (\alpha_r + 1)$. This equals $453 = 3 \cdot 151$ if and only if either $r = 1$ and $\alpha_1 + 1 = 453$, or $r = 2$ and $(\alpha_1 + 1, \alpha_2 + 1) = (3, 151)$ or $(151, 3)$. Thus the integers n with 453 positive divisors are those of the form $\boxed{n = p_1^{452}}$ or $\boxed{n = p_1^2 p_2^{150}}$ (where p_1 and p_2 are distinct primes).

- (iii) Let $f = g \star \mu$, where g is the arithmetic function defined by $g(n) = n$ for all $n \in \mathbf{N}$. Evaluate $f(10^{10})$. (Don’t try this by brute force. With the right approach, this requires only minimal amount of numerical calculation. Explain any non-obvious steps (e.g., by citing an appropriate theorems/formulas/properties.)

Solution: Note that $g = \mathbf{id}$, the identity function. By **Gauss’ Identity**, $\mathbf{id} = \varphi \star \mathbf{1}$. Hence $f = (\varphi \star \mathbf{1}) \star \mu = \varphi \star (\mathbf{1} \star \mu) = \varphi \star \delta = \varphi$, by the properties of the Dirichlet product. Therefore, by the multiplicativity of φ , $f(10^{10}) = \varphi(10^{10}) = \varphi(2^{10}5^{10}) = 2^9(2-1)5^9(5-1) = \boxed{2^{11}5^9}$.

- (iv) **Extra Credit:** Characterize, with proof, the squarefree positive integers for which the sum of all positive divisors is a power of 2 (i.e., $2^1, 2^2, \dots$). (A squarefree integer is one that is not divisible by the square or a higher power of a prime. continue on back of page.)

Solution: Since $\sigma(1) = 1$, and 1 is not a power of 2 we may restrict to squarefree integers $n \geq 2$. Writing n as $n = p_1 p_2 \dots p_r$ with distinct primes p_i , we have $\sigma(n) = (p_1 + 1)(p_2 + 1) \dots (p_r + 1)$. This is equal to a power of 2 if and only if, for each prime factor p_i , $p_i + 1$ is a power of 2, i.e., if and only if each prime factor p_i is of the form (*) $p_i = 2^{k_i} - 1$ with some $k_i \in \mathbf{N}$. But primes of the form (*) are exactly the Mersenne primes. Hence $\sigma(n)$ is a power of 2 if and only if $\boxed{n \text{ is a product of distinct Mersenne primes}}$.