

Problem 1 (15 points)

(True/false questions) For each of the following statements, say if it is true or false, and provide a brief justification for your claim. Credit on these questions is based on your justification. *A simple true/false answer, without justification, or with an incorrect justification, won't earn credit.*

For true statements, a justification typically consists of citing and applying an appropriate theorem, if necessary stating why the cited theorem can be applied. Be specific; e.g., say “Since $(453, 347) = 1$, Euler’s Theorem with $a = 453$ and $b = 347$ applies and guarantees the existence of a solution ...” rather than something like “true by Euler’s Theorem”.

For false statements, usually a specific counterexample may be enough. Note, however, that a different strategy is required to disprove statements asserting something for *infinitely many* (rather than *all*) integers.

- (i) There exist infinitely many solutions $x, y \in \mathbf{Z}$ to the equation $2x + 5y = 3$.

Solution: TRUE The statement is equivalent to the assertion that the congruence $2x \equiv 3 \pmod{5}$ has infinitely many solutions. Since $(2, 5) = 1$, and $1 \mid 3$, the theorem on the existence of solutions to a linear congruence shows that this equation has a single solution x modulo 5, and hence infinitely many integer solutions.

- (ii) If $a, b, c \in \mathbf{N}$ are such that $a + b \mid c$, then $a \mid c$ and $b \mid c$.

Solution: FALSE A counterexample is given by $a = 1, b = 3, c = 4$ (there are many others): $1 + 3 \mid 4$, but $3 \nmid 4$.

- (iii) If n is composite, then n does **not** divide $2^{n-1} - 1$.

Solution: FALSE The statement is equivalent to the statement that if $2^{n-1} \equiv 1 \pmod{n}$, then n is prime. The latter would be the converse to Fermat’s theorem, which, however, does not hold: There exists composite integers n (“pseudoprimes”) satisfying $2^{n-1} \equiv 1 \pmod{n}$. One example is $n = 561$, a Carmichael number.

Problem 2 (15 points)

(Definitions and theorems) The following problems test your knowledge of theorems and definitions: Simply state the theorem or definition requested; be sure to include any necessary hypotheses, and be careful with details (e.g., “for all $a, b \in \mathbf{Z}$ ” versus “for all $a, b \in \mathbf{N}$ ” or for all “ $a, b \in \mathbf{N}$ such that $(a, b) = 1$ ”):

- (i) State the Goldbach conjecture.

Solution: The Goldbach Conjecture asserts the following: *Every even integer ≥ 4 is expressible as a sum of two prime numbers.*

- (ii) State the Prime Number Theorem (be sure to define/explain any notation involved).

Solution: The Prime Number Theorem asserts that

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \log x} = 1,$$

where $\pi(x)$ denotes the number of primes $\leq x$.

- (iii) State the Moebius inversion formula.

Solution: In Dirichlet product notation, the Moebius inversion formula is as follows:

$$\text{If } f = g \star \mathbf{1}, \text{ then } g = f \star \mu = \mu \star f.$$

Equivalently, the Moebius inversion formula states the following:

$$\text{If } f \text{ and } g \text{ are arithmetic functions such that } f(n) = \sum_{d|n} g(d) \text{ holds for all } n \in \mathbf{N}, \text{ then} \\ g(n) = \sum_{d|n} f(d)\mu(n/d) = \sum_{d|n} \mu(d)f(n/d) \text{ holds for all } n \in \mathbf{N}.$$

Problem 3 (15 points)

(Short computations) Evaluate each of the following quantities.

- (i) The gcd $(4a^2 + 1, 2a - 1)$, where a is an arbitrary positive integer.

Solution: Using the property that (a, b) is equal to $(a + nb, b)$, for any integer n , we get

$$(4a^2 + 1, 2a - 1) = (4a^2 + 1 - (2a + 1)(2a - 1), 2a - 1) = (2, 2a - 1) = 1.$$

- (ii) The remainder of 2009^{2008} upon division by 9.

Solution: We need to find the least nonnegative residue of 2009^{2008} modulo 9. Now, $2009 \equiv 2 \pmod 9$, $2^3 = 8 \equiv -1 \pmod 9$, and $2008 = 3 \cdot 669 + 1$, so

$$2009^{2008} \equiv 2^{2008} \equiv 2^{3 \cdot 669 + 1} \equiv (2^3)^{669} \cdot 2 \equiv (-1)^{669} \cdot 2 \equiv -2 \pmod 9.$$

so $\boxed{7}$ is the least nonnegative remainder.

- (iii) The last two decimal digits of 453^{561} .

Solution: The two decimal digits of a positive integer n (interpreted as a single 1- or 2-digit integer) are given by the least nonnegative residue of n modulo 100. Since $\varphi(100) = \varphi(2^2 \cdot 5^2) = 1 \cdot 2 \cdot 4 \cdot 5 = 40$ and $(453, 100) = 1$, Euler's theorem gives $453^{40} = 453^{\varphi(100)} \equiv 1 \pmod{100}$. Now $561 = 40 \cdot 16 + 1$, so

$$453^{561} = 453^{40 \cdot 16 + 1} = (453^{40})^{16} \cdot 453^1 \equiv 453^1 \equiv 53 \pmod{100},$$

so $\boxed{53}$ are the last digits of 453^{561} .

Problem 4 (15 points)

(Short proofs)

- (i) Prove that if p is a prime greater than 10, then at least one of the numbers $p + 2$ and $5p + 2$ is composite.

Solution: We consider congruences modulo 3. Since p is greater than 3, we have either $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$. In the first case, $p + 2 \equiv 0 \pmod 3$, while in the second $5p + 2 \equiv 5 \cdot 2 + 2 = 12 \equiv 0 \pmod 3$. Thus, in either case, one of the two numbers $p + 2$ and $5p + 2$ is divisible by 3 and hence must be composite.

- (ii) Prove that if n is composite, then $2^n - 1$ is also composite.

Solution: Suppose n is composite. Then $n = ab$ for some integers $a, b \geq 2$. Since $2^a \equiv 1 \pmod{(2^a - 1)}$, we have $2^n = (2^a)^b \equiv 1^b = 1 \pmod{(2^a - 1)}$. Thus, $2^n - 1$ is divisible by $2^a - 1$, and since $1 < a < n$, the integer $2^a - 1$ is a proper divisor of $2^n - 1$ (i.e., strictly greater than 1 and less than n). Hence $2^n - 1$ is composite.

- (iii) Let p and q be distinct primes. Prove that, for any $a \in \mathbf{Z}$, $a^{pq} + a \equiv a^p + a^q \pmod{pq}$.

Solution: We apply Fermat's Little Theorem in the version

$$(1) \quad a^p \equiv a \pmod{p},$$

which holds for any prime p and any integer a (regardless of whether or not a is relatively prime to p). Applying this with a^q in place of a , we get

$$(2) \quad a^{qp} = (a^q)^p \equiv a^q \pmod{p}.$$

Adding (1) and (2) gives

$$(3) \quad a^{qp} + a \equiv a^q + a^p \pmod{p}.$$

Interchanging the roles of p and q shows that the congruence (3) also holds modulo q , and since p and q are distinct primes, it follows that (3) holds modulo pq , as desired.

Problem 5 (10 points)

- (i) Use the Euclidean algorithm to determine the gcd of 453 and 408, and express this gcd as a linear combination of 453 and 408 with integer coefficients.

Solution: We apply the Euclidean algorithm to the pair (453, 408):

$$453 = 408 \cdot 1 + 45, \quad 408 = 45 \cdot 9 + 3, \quad 45 = 3 \cdot 15.$$

This shows that $\boxed{(453, 408) = 3}$. Working backwards, we get the desired linear combination:

$$\begin{aligned} 3 &= 408 - 45 \cdot 9 \\ &= 408 - (453 - 408 \cdot 1) \cdot 9 \\ &= \boxed{408 \cdot 10 + 453 \cdot (-9)}. \end{aligned}$$

- (ii) Determine, with explanation, which (if any) of the numbers 2007, 2008, 2009 can be expressed in the form $408x + 453y$, with $x, y \in \mathbf{Z}$. (This problem concerns only the *existence* of such a representation; you do not need to *find* such a representation.)

Solution: The set of numbers expressible in the above form consists exactly of the integer multiples of $(408, 453) = 3$. Of the three given numbers, only the first, 2007, is a multiple of 3, so 2007 can be expressed in the given form, while 2008 and 2009 cannot.

Problem 6 (10 points)

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

Solution: By the multiplicativity of the Legendre symbol, the product of two nonresidues is a residue, while the product of three nonresidues is a nonresidue. Of the above integers, the first three, $\boxed{15, 21, 35}$ are products of two of the given primes, and hence **quadratic residues**, while the last one, $\boxed{105}$, is a product of three of the primes, and hence a **quadratic nonresidue**.

- (ii) Determine, with explanation, whether there exists an integer n such that $n^{10} + 1$ is divisible by 151. (Note that 151 is prime.)

Solution: We show by contradiction that no such integer exists. Suppose n is an integer such that $n^{10} + 1$ is divisible by 151. Then (*) $n^{10} \equiv -1 \pmod{151}$. Hence (**) $n^{150} = (n^{10})^{15} \equiv (-1)^{15} = -1 \equiv -1 \pmod{151}$. On the other hand, by Fermat's Theorem, $n^{150} \equiv 1 \pmod{151}$ if $151 \nmid n$, while for $151 \mid n$, $n^{150} \equiv 0 \pmod{151}$. Thus, in either case we have obtained a contradiction to (**).

Alternative proof: One can also argue via quadratic residues: Writing the congruence (*) as $(n^5)^2 \equiv -1 \pmod{151}$, we see that if (*) holds, then $x^2 \equiv -1 \pmod{151}$ has an integer solution (namely $x = n^5$), so -1 must be a quadratic residue modulo 151. However, since $151 \equiv 3 \pmod{4}$, -1 is a quadratic nonresidue modulo 151, so we again arrive at a contradiction.

Problem 7 (20 points)

Given that 151 is a prime, determine:

- (i) The number of incongruent quadratic nonresidues modulo 151 that are **not** primitive roots modulo 151.

Solution: The number of incongruent quadratic nonresidues modulo 151 is $(151 - 1)/2 = 75$. The number of incongruent primitive roots modulo 151 is $\varphi(\varphi(151)) = \varphi(150) = \varphi(2 \cdot 3 \cdot 5^2) = 40$. Since a primitive root is necessarily a quadratic nonresidue, the number of incongruent nonresidues that are **not** primitive roots is $75 - 40 = \boxed{35}$.

- (ii) The number of incongruent integers a with $a^3 \equiv 1 \pmod{151}$.

Solution: We have $a^3 \equiv 1 \pmod{151}$ if and only if $\text{ord}_{151} a \mid 3$, i.e., if and only if the order of a modulo 151 is 1 or 3. Since 3 and 1 divide $\varphi(151) = 150$, there are $\varphi(3) = 2$ incongruent integers of order 3, and there is $\varphi(1) = 1$ incongruent integer (namely $a = 1$) of order 1. Thus, there are a total of $\boxed{3}$ incongruent integers a with $a^3 \equiv 1 \pmod{151}$.

- (iii) The exact set of integers that are orders modulo 151 of some integer coprime to 151 (i.e., the set $\{\text{ord}_{151} a : a \in \mathbf{Z}, (a, 151) = 1\}$.)

Solution: The possible orders modulo a prime p are the positive divisors of $\varphi(p) = p - 1$. Since $p - 1 = 150 = 2 \cdot 3 \cdot 5^2$, these are the numbers $\boxed{1, 2, 3, 5, 6, 10, 15, 25, 30, 50, 75, 150}$. (Note that there are $\nu(150) = \nu(2^1 \cdot 3^1 \cdot 5^2) = (1 + 1)(1 + 1)(2 + 1) = 12$ such divisors.)

- (iv) An inverse of 2^{145} modulo 151. (Express the answer as an integer a in the range $1 \leq a \leq 151$.)

Solution: Since 151 is prime, and $(2, 151) = 1$, we have, by Fermat's Little Theorem, $2^{150} \equiv 1 \pmod{151}$. Writing $2^{150} = 2^{145} \cdot 2^5$, we see that $2^{145} \cdot 2^5 \equiv 1 \pmod{151}$, so $2^5 = \boxed{32}$ is an inverse of 2^{145} modulo 151.

Problem 8 (10 points)

- (i) Evaluate $\sum_{d|10^{10}} d\mu(10^{10}/d)$.

Solution: The given divisor sum can be written as $f(10^{10})$, where $f = \mathbf{i} \star \mu$, with \mathbf{i} being the identity function. Using Gauss' identity $\mathbf{i} = \varphi \star \mathbf{1}$ and the fact that the Moebius function is the Dirichlet inverse of the function $\mathbf{1}$, we get $f = \mathbf{i} \star \mu = (\varphi \star \mathbf{1}) \star \mu = \varphi \star (\mathbf{1} \star \mu) = \varphi$, so $f(10^{10}) = \varphi(10^{10}) = \varphi(2^{10} \cdot 5^{10}) = 2^9 \cdot (5 - 1) \cdot 5^9 = \boxed{2^{11} 5^9}$.

- (ii) Find all positive integers n for which $\varphi(n)$ is 2 times an odd number.

Solution: We seek to characterize those integers n for which $\varphi(n)$ contains the prime 2 to exactly the first power.

Note that a factor p^α in the standard prime factorization of n contributes a factor $p^{\alpha-1}(p-1)$ to $\varphi(n)$.

If p is congruent to 1 mod 4, then $p-1$ is divisible by 4, so $\varphi(n)$ is divisible by 4 as well and so is not of the desired form. Thus, n cannot contain a prime factor congruent to 1 modulo 4.

On the other hand, if p is congruent to 3 mod 4, then $p-1$ is divisible by 2. Thus, in order for $\varphi(n)$ to be exactly divisible by 2, n can contain at most one prime factor congruent to 3 modulo 4.

Thus n necessarily has to be one of the following forms: (1) $n = 2^\alpha$, (2) $n = p^\alpha$, or (3) $n = p^\alpha 2^\beta$, with $\alpha, \beta \in \mathbf{N}$ and $p \equiv 3 \pmod{4}$. The φ -values for these three types of numbers are (1) $2^{\alpha-1}$, (2) $p^{\alpha-1}(p-1)$, (3) $p^{\alpha-1}(p-1)2^{\beta-1}$. These are divisible by exactly the first power of 2 if (1) $\alpha = 2$, (2) α is arbitrary, and (3) $\beta = 1$, with α arbitrary. Summarizing, the integers n for which $\varphi(n)$ is 2 times an odd number are exactly those of the forms

$$\boxed{(1) n = 4, \quad (2) n = p^\alpha, \alpha \in \mathbf{N}, p \equiv 3 \pmod{4}, \quad (3) n = 2p^\alpha, \alpha \in \mathbf{N}, p \equiv 3 \pmod{4}}$$

Problem 9 (10 points)

In the following statements fill in the blanks with appropriate values (such as $1/453$ or 0.001) that make the statements true and best-possible (to the best of your knowledge).

- (i) If α is an irrational number satisfying

$$\left| \alpha - \frac{453}{100} \right| \leq \dots$$

then $453/100$ is a convergent to the continued fraction expansion of α .

Solution: By Theorem 6.8(ii) in the Notes, the correct bound needed to *guarantee* that a reduced fraction a/b is a convergent, is $1/(2b^2)$, which in this case is $\boxed{1/(2 \cdot 100^2)}$.

- (ii) If α is an irrational number satisfying

$$\left| \alpha - \frac{453}{100} \right| > \dots$$

then $453/100$ is **not** a convergent to the continued fraction expansion of α .

Solution: By Theorem 6.8(i) in the Notes, in contrapositive form, the correct bound here is $1/b^2$, i.e., $\boxed{1/100^2}$.

Problem 10 (10 points)

- (i) Expand $5/18$ into a simple continued fraction, and find all of its convergents.

Solution: We have

$$\begin{aligned} \frac{5}{18} &= 0 + \frac{1}{\frac{18}{5}} = 0 + \frac{1}{3 + \frac{3}{5}} = 0 + \frac{1}{3 + \frac{1}{\frac{5}{3}}} \\ &= 0 + \frac{1}{3 + \frac{1}{1 + \frac{2}{3}}} = 0 + \frac{1}{3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}} \\ &= [0, 3, 1, 1, 2]. \end{aligned}$$

The convergents are

$$\begin{aligned} C_0 &= [0] = \boxed{\frac{0}{1}}, \\ C_1 &= [0, 3] = 0 + \frac{1}{3} = \boxed{\frac{1}{3}}, \\ C_2 &= [0, 3, 1] = 0 + \frac{1}{3 + \frac{1}{1}} = \boxed{\frac{1}{4}}, \\ C_3 &= [0, 3, 1, 1] = 0 + \frac{1}{3 + \frac{1}{1 + \frac{1}{1}}} = \boxed{\frac{2}{7}}, \\ C_4 &= [0, 3, 1, 1, 2] = \boxed{\frac{5}{18}}. \end{aligned}$$

(ii) Find the number α whose simple continued fraction expansion is $\alpha = [1, 2, 3, 2, 3, \dots] = [1, \overline{2, 3}]$.

Solution: We have $\alpha = 1 + \frac{1}{\beta}$, where $\beta = [\overline{2, 3}]$. Now,

$$\begin{aligned} \beta &= [2, 3, \overline{2, 3}] = [2, 3, \beta] \\ &= 2 + \frac{1}{3 + \frac{1}{\beta}} = 2 + \frac{\beta}{3\beta + 1} \\ &= \frac{7\beta + 2}{3\beta + 1}, \end{aligned}$$

so

$$3\beta^2 - 6\beta - 2 = 0.$$

Solving this quadratic equation (ignoring the negative root, since $\beta = [\overline{2, 3}]$ must be a positive number),

we get

$$\begin{aligned}\beta &= \frac{6 + \sqrt{60}}{6} = \frac{3 + \sqrt{15}}{3}, \\ \alpha &= 1 + \frac{1}{\beta} = 1 + \frac{3}{3 + \sqrt{15}} \\ &= \frac{\sqrt{15} + 6}{\sqrt{15} + 3} = \frac{(\sqrt{15} + 6)(\sqrt{15} - 6)}{15 - 3^2} \\ &= \boxed{\frac{-1 + \sqrt{15}}{2}}.\end{aligned}$$