

Problem 1

(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 prime numbers whose decimal representation ends in the digits 453.

Solution: TRUE A positive integer n ends in the digits 453 if and only if n is of the form (*) $n = 1000q + 453, q = 0, 1, 2, \dots$. Since $(453, 1000) = 1$, Dirichlet’s Theorem for primes in arithmetic progressions guarantees that there are infinitely many primes of the form (*).

[This is a variation on a hw problem (Chapter 1, Problem 84), which asked to show that there are infinitely many primes ending in k 1’s, for any k .]

- (ii) There exist infinitely many solutions $x, y \in \mathbf{Z}$ to the equation $x^2 = 4y - 453$.

Solution: FALSE The given equation implies $x^2 \equiv -453 \equiv 3 \pmod{4}$. However, this is impossible, since for $x \equiv 0, 1, 2, 3 \pmod{4}$, we have, respectively, $x^2 \equiv 0^2, 1^2, 2^2, 3^2 \equiv 0, 1, 0, 1 \pmod{4}$, so x^2 can only occupy the residue classes 0 or 1 modulo 4.

- (iii) If n is an integer ≥ 2 satisfying $(n - 1)! \equiv -1 \pmod{n}$, then n is prime.

Solution: TRUE This is the converse to Wilson’s theorem.

- (iv) If a, b, c are positive integers satisfying $(a, b) > 1$, $(a, c) > 1$, and $(b, c) > 1$, then $(a, b, c) > 1$.

Solution: FALSE A counterexample is given by $a = 2 \cdot 3$, $b = 3 \cdot 5$, and $c = 2 \cdot 5$: With this choice $(a, b) = 3$, $(a, c) = 2$, $(b, c) = 5$, but $(a, b, c) = 1$.

[This is a simplified version of a homework problem (Chapter 1, Problem 35), which asked to construct 4 integers with the same property.]

Problem 2

(Short computations) Evaluate each of the following quantities. Show work!

- (i) The last decimal digit of 7^{453} .

Solution: The last decimal digit of a positive integer n is the least nonnegative residue of n modulo 10. Since $(7, 10) = 1$ and $\varphi(10) = 4$, we have, by Euler’s theorem, $7^4 = 7^{\varphi(10)} \equiv 1 \pmod{10}$. Thus,

$$7^{453} = 7^{4 \cdot 113 + 1} = (7^4)^{113} \cdot 7^1 \equiv 7 \pmod{10},$$

so 7 is the last digit of 7^{453} .

- (ii) The greatest common divisor of $3^{453} - 1$ and $3^{151} - 1$.

Solution: Note that

$$\begin{aligned} 3^{151} &\equiv 1 \pmod{3^{151} - 1}, \\ 3^{453} &= (3^{151})^3 \equiv 1^3 = 1 \pmod{3^{151} - 1}. \end{aligned}$$

Thus $3^{151} - 1 \mid 3^{453} - 1$, and so $(3^{453} - 1, 3^{151} - 1) = 3^{151} - 1$.

[The same argument came up in a recent homework problem which asked to show that $2^m - 1 \mid 2^n - 1$ if $m \mid n$.]

- (iii) The number of positive integers $\leq 18,000 (= 2^4 3^2 5^3)$ that are divisible by **each** of the numbers 8, 9, 10, 12.

Solution: We use the fact that divisibility by each of a set of given numbers is equivalent to divisibility by the least common multiple of these numbers. Now,

$$[8, 9, 10, 12] = [2^3, 3^2, 2 \cdot 5, 2^2 \cdot 3] = 2^3 \cdot 3^2 \cdot 5 = 360,$$

and the number of positive integers $\leq 18,000$ divisible by 360 is $18,000/360 = \boxed{50}$.

[Note: The above solution was the intended interpretation of the problem. Some students interpreted the problem as being four questions, one for each of the divisors 8, 9, 10, 12; full credit was given for a correct solution under this interpretation.]

- (iv) The least nonnegative residue of $50 \cdot 50!$ modulo 53. (Hint: What is $2 \cdot 50!$ modulo 53?)

Solution: Since 53 is prime, we have by Wilson's theorem

$$-1 \equiv 52! = 50!(51)(52) \equiv 50!(-2)(-1) = 2 \cdot 50! \pmod{53}.$$

Multiplying by 25, we get $50 \cdot 50! \equiv 25(-1) = -25 \equiv 28 \pmod{53}$, so $\boxed{28}$ is the least nonnegative residue of $50 \cdot 50! \pmod{53}$.

[The underlying argument here is the same as in a homework problem (Chapter 2, Problem 43), which asked to compute $2 \cdot (p-3)! \pmod{p}$ when p is prime. (Hence the hint to consider first $2 \cdot 50! \pmod{53}$.)]

Problem 3

(Short proofs)

- (i) Prove that $453 \cdot 347^n + 408^{n+1}$ is divisible by 5 for all **odd** positive integers n .

Solution: The assertion is equivalent to $453 \cdot 347^n + 408^{n+1} \equiv 0 \pmod{5}$, for all odd $n \in \mathbf{N}$. Reducing everything modulo 5, we get

$$453 \cdot 347^n + 408^{n+1} \equiv 3 \cdot 2^n + 3^{n+1} \equiv 3 \cdot 2^n + (-2)^{n+1} \pmod{5}$$

For n odd, we have $(-2)^{n+1} = 2^{n+1}$, so the above becomes $3 \cdot 2^n + 2^{n+1} = 5 \cdot 2^n \equiv 0 \pmod{5}$, which proves the claim.

- (ii) Using only the definition of divisibility (i.e., without appealing to any of the theorems, propositions, properties, etc., about divisibility that you might know), prove the following statement:

Let $a, b, c, d \in \mathbf{Z}$. If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

Solution: Let $a, b, c, d \in \mathbf{Z}$, and suppose $a \mid b$ and $c \mid d$. By the definition of divisibility, this means that there exist $x, y \in \mathbf{Z}$ such that $b = ax$ and $d = cy$. Hence $(*)$ $bd = (ax)(cy) = (ac)(xy)$. Since x and y are integers, so is xy , and $(*)$ therefore implies that $ac \mid bd$, with xy as the "multiplier".

Problem 4

Determine all incongruent solutions of the congruence $408x \equiv 6 \pmod{453}$, or show that no solutions exist.

Solution: Using the factorizations $453 = 3 \cdot 151$, $408 = 2^3 \cdot 3 \cdot 17$, we get $(408, 453) = 3$, and since $3 \mid 6$, the congruence has a solution. Moreover, there are exactly 3 incongruent solutions modulo 453.

To find a particular solution, we apply the Euclidean algorithm to the pair $(453, 408)$:

$$453 = 408 \cdot 1 + 45$$

$$408 = 45 \cdot 9 + 3$$

$$45 = 3 \cdot 15.$$

Working backwards, we get

$$\begin{aligned} 3 &= 408 - 45 \cdot 9 \\ &= 408 - (453 - 408 \cdot 1) \cdot 9 \\ &= 408 \cdot 10 + 453 \cdot (-8). \end{aligned}$$

Thus, $408 \cdot 10 \equiv 3 \pmod{453}$. Multiplying by 2, we get $408 \cdot 20 \equiv 6 \pmod{453}$. Thus $x_0 = 20$ is one solution to the given congruence. Adding to this solution $k(453/3) = 151k$, for $k = 0, 1, 2$ gives all incongruent solutions modulo 453: $\boxed{20, 171, 322}$.