

## Problem 1

**True/false questions.** For each of the following statements, determine 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, a *specific* counterexample may be enough as justification.

- (i) There exist infinitely many integers  $x, y$  satisfying  $9x = 15y + 453$ .

**Solution:** TRUE The given equation is of the form  $ax + by = c$  with  $a = 9$ ,  $b = -15$ ,  $c = 453$ . Since  $(9, -15) = 3$  and 3 divides 453, by the general theory for equations of the form  $ax + by = c$ , there are infinitely many integer solutions. (Given one solution  $(x_0, y_0)$  of  $9x = 15y + 453$ , one can get infinitely many solutions by setting  $x = x_0 + 5k$ ,  $y = y_0 + 3k$ , where  $k$  is an arbitrary integer; see Problem 36 from HW 1 for a similar situation.)

- (ii) The numbers  $0, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2$  form a complete system of residues modulo 7.

**Solution:** FALSE This can be seen by reducing the given numbers modulo 7:  $0 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 2, 4^2 \equiv 2, 5^2 \equiv 4, 6^2 \equiv 1$ . Since only 4 of the 7 possible residue classes modulo 7 (namely,  $0, 1, 2, 4$ ) are represented, the given numbers do not form a complete system of residues modulo 7.

- (iii) If  $a, b, c$  are positive integers such that  $(a, c) = 1$  and  $(b, c) = 1$ , then for any positive integers  $m$  and  $n$ ,  $(am + bn, c) = 1$ .

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

## Problem 2

**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 Prime Number Theorem (be sure to define/explain any notation involved).

**Solution:** The Prime Number Theorem asserts that  $\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} = 1$ , where  $\pi(x)$  denotes the number of primes  $\leq x$ .

- (ii) (a) What is a pseudo-prime to base 7? (b) What is a Carmichael number?

**Solution:** A base 7 pseudo-prime is a composite number  $n$  satisfying  $7^{n-1} \equiv 1 \pmod{n}$ . A Carmichael number is an integer  $n$  that is a pseudoprime to all bases  $a$  with  $(a, n) = 1$ .

- (iii) State **two** famous conjectures about primes that came up in the book or in class. In each case, give the name of the conjecture (e.g., “Silvercreek Conjecture”, “Carmichael’s Conjecture”), and the *precise* statement of the conjecture.

**Solution:** Examples include the Goldbach Conjecture, the Twin Prime Conjecture, the infinitude of Mersenne primes, the infinitude of primes of the form  $n^2 + 1$ . See the class notes and Chapter 1 of the text for precise statements.

## Problem 3

**Short computations.** Each of the following questions can be answered using only a minimal amount of pencil/paper calculations *if approached with the right method*. If you get entangled in a messy hand computation (e.g., multiplying or dividing multidigit numbers), you are on the wrong track. Answers arrived at by brute force methods, trial and error, or guessing won't earn credit.

Make sure to show your work, cite any theorems you use (e.g., by “Dirichlet’s Theorem”), and circle/box your final answer.

- (i) Find the remainder of  $2011^{23}$  upon division by 9.

**Solution:** We have  $2011 \equiv 2 + 1 + 1 = 4 \pmod{9}$ , and  $4^3 = 64 \equiv 1 \pmod{9}$ , so  $2011^{23} \equiv 4^{23} \equiv (4^3)^7 4^2 \equiv 4^2 \equiv \boxed{7} \pmod{9}$ .

**Remark:** Fermat's Theorem doesn't apply here since 9 is not a prime. In fact, a blind application of Fermat would give (\*)  $4^8 \equiv 1 \pmod{9}$ , which, however, is false: Since  $4^3 = 64 \equiv 1 \pmod{9}$ , so  $4^8 \equiv (4^3)^2 4^2 \equiv 16 \equiv 7 \pmod{9}$  contradicting (\*).

- (ii) Determine, with explanation, which (if any) of the 6 numbers (in decimal) 1, 11, 111, 1111, 11111, 111111, 1111111 can be expressed in the form  $15x + 51y$ , with  $x, y \in \mathbf{Z}$ . (This question 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 the gcd  $(15, 51)$ . Since  $(15, 51) = 3$ , those are exactly the integers divisible by 3. By the divisibility test for 3, of the given numbers exactly 2, namely  $\boxed{111}$  and  $\boxed{111111}$ , are divisible by 3. Hence these two numbers can be represented in the above form, and all others cannot be represented in this form.

- (iii) Find the number of positive divisors of  $2^{23}3^{150}$ .

**Solution:** The positive divisors of  $2^{23}3^{150}$  are the numbers of the form  $2^a 3^b$  with  $a, b$  nonnegative integers satisfying  $a \leq 23$  and  $b \leq 150$ . (This is a consequence of the Fundamental Theorem of Arithmetic; see Prop. 1.21 of the class notes.) There are 24 choices for  $a$  and 151 choices for  $b$  (note that  $a = 0$  and  $b = 0$  need to be included in these counts), so a total of  $24 \cdot 151 = 3624$  pairs  $(a, b)$ . Since distinct pairs  $(a, b)$  of exponents yield distinct divisors (by the FTA), the total number of divisors is equal to the number of such exponent pairs, i.e.,  $\boxed{3624}$ .

## Problem 4

### Short proofs.

- (i) Prove that if  $p$  is a prime greater than 3, then at least one of the numbers  $p + 2$  and  $5p + 2$  is composite.

**Solution:** This is similar to a homework problem asking to prove that at least one of the numbers  $p, p + 2, p + 4$  is composite. We consider congruences modulo 3. Since  $p$  is a prime greater than 3,  $p$  cannot be divisible by 3, so 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, for any positive integer  $n$ , the number  $n^{13} - n$  is divisible by 35.

**Solution:** Divisibility by 35 is equivalent to divisibility by 5 and by 7, so it suffices to show that (1)  $n^{13} \equiv n \pmod{5}$  and (2)  $n^{13} \equiv n \pmod{7}$  for all  $n$ . If  $5 \nmid n$ , then Fermat's Little Theorem gives  $n^4 \equiv 1 \pmod{5}$  and so  $n^{13} = (n^4)^3 n \equiv n \pmod{5}$ , which proves (1) in this case. If, on the other hand,  $5 \mid n$ , then both  $n^{13} \equiv 0 \pmod{5}$  and  $n \equiv 0 \pmod{5}$ , so (1) holds in this case as well. Similarly, if  $7 \nmid n$ , then  $n^6 \equiv 1 \pmod{7}$ , so  $n^{13} = (n^6)^2 n \equiv n \pmod{7}$ , and if  $7 \mid n$ , then  $n^{13} \equiv 0 \equiv n \pmod{7}$ , proving (2).

- (iii) Prove that, for all integers  $n \geq 2$ , the number  $n^{40} + 1$  is composite, and find a nontrivial divisor of this number.

**Solution:** We use the same argument as that in class to prove the compositeness numbers of the form  $2^n + 1$  when  $n$  is *not* a power of 2: We split off the "odd" part of the exponent, writing 40 as  $40 = 8 \cdot 5$ , and  $n^{40} + 1$  as  $(n^8)^5 + 1$ . The latter form suggests trying congruences modulo  $n^8 + 1$ , and this does indeed the trick:  $n^8 \equiv -1 \pmod{n^8 + 1}$ ,  $(n^8)^5 \equiv (-1)^5 = -1 \pmod{n^8 + 1}$ , so  $n^8 + 1$  divides  $n^{40} + 1$ . Since  $1 < n^8 + 1 < n^{40} + 1$  for  $n \geq 2$ , this proves that  $n^{40} + 1$  is composite.

**Remark:** Fermat's Little Theorem is of no use here since it gives a congruence of the form  $n^{40} \equiv 1$ , whereas divisibility of  $n^{40} + 1$  requires a congruence of the form  $n^{40} \equiv -1$ .