

## 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.**

A justification typically consists of citing and applying an appropriate theorem (e.g., “by Chamberlain’s Theorem”), and if necessary stating why the cited theorem can be applied. Be specific; e.g., say “Since  $(453, 347) = 1$ , ’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”.

- (i) An integer  $n > 2$  is composite if and only if  $n$  does not divide  $(n - 1)! + 1$ .

**Solution:** TRUE **Wilson’s theorem** states that an integer  $n > 2$  is prime if and only if  $(*) (n - 1)! \equiv -1 \pmod{n}$ . The given condition, “ $n$  does not divide  $(n - 1)! + 1$ ”, is the negation of  $(*)$ , so it holds if and only if  $n$  is composite.

- (ii) There exists an integer  $x$  such that  $3x \equiv 347 \pmod{453}$ . (Note that 3 and 347 are prime, and 453 has prime factorization  $453 = 3 \cdot 151$ .)

**Solution:** FALSE A congruence  $ax \equiv b \pmod{m}$  has a solution if and only if  $(a, m) \mid b$ . In the given case  $(a, m) = (3, 453) = 3$ , and since  $3 \nmid 347$ , no solution exists.

- (iii) If  $n$  is an integer  $\geq 2$  satisfying  $n \mid a^{n-1} - 1$  for **all** positive integers  $a$  with  $(a, n) = 1$ , then  $n$  is prime.

**Solution:** FALSE Composite integers  $n$  that satisfy the given condition, i.e.,  $a^{n-1} \equiv 1 \pmod{n}$  for **all**  $a$  with  $(a, n) = 1$ , are **Carmichael numbers**, and these are known to exist (e.g.,  $n = 561$ ).

**Remark:** Note that the existence of pseudoprimes, i.e., composite numbers satisfying  $a^{n-1} \equiv 1 \pmod{n}$  for a given base  $a$ , is **not** enough to disprove the statement, since pseudoprimes are defined with respect to a **fixed** base  $a$ . A Carmichael number must satisfy the above congruence for **all** bases  $a$  coprime with  $n$ , which is a much more restrictive condition on  $n$ .

## 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) Give a **precise** statement of the “Best Approximation Property” of the convergents  $\frac{p_i}{q_i}$  of the continued fraction expansion of a real number  $\alpha$ .

**Solution:** For any rational number  $a/b$ , with  $a \in \mathbf{Z}$ ,  $b \in \mathbf{N}$ , and  $b \leq q_i$ , we have  $|\alpha - p_i/q_i| \leq |\alpha - a/b|$ .

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

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

- (iii) State Dirichlet’s Theorem for primes in arithmetic progressions.

**Solution:** Let  $a, b \in \mathbf{N}$  such that  $(a, b) = 1$ . Then there exist infinitely many primes of the form  $an + b$ , where  $n \in \mathbf{N}$ .

### 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  $7^{2012}$  upon division by 2011.

**Solution:** Since 2011 is prime, Fermat's Theorem gives  $7^{2010} \equiv 1 \pmod{2011}$ , so  $7^{2012} \equiv 7^2 = \boxed{49} \pmod{2011}$

- (ii) Find the last **two** decimal digits of  $413^{402}$ . (Don't try this with brute force. With the right approach, this requires only minimal computations.)

**Solution:** The last two decimal digits of a positive integer  $n$  are given by the least nonnegative residue of  $n$  modulo 100. Since  $413 \equiv 13 \pmod{100}$ , it suffices to compute  $13^{402} \pmod{100}$ . Euler's theorem gives  $13^{\varphi(100)} = 13^{40} \equiv 1 \pmod{100}$  (note  $\varphi(100) = \varphi(2^2 \cdot 5^2) = (2-1) \cdot 2^1 \cdot (5-1) \cdot 5^1 = 40$ ). Then

$$13^{402} = 13^{40 \cdot 10 + 2} = (13^{40})^{10} \cdot 13^2 \equiv 1^{10} \cdot 13^2 \equiv 169 \equiv \boxed{69} \pmod{100}.$$

- (iii) Find **all** integer solutions  $(x, y)$  of the equation  $13x + 11y = 7$ .

**Solution:** We first apply the Euclidean algorithm to 13 and 11 to obtain a single solution  $(x_0, y_0)$  to the equation  $13x + 11y = 1$ :

$$13 = 1 \cdot 11 + 2, \quad 11 = 5 \cdot 2 + 1, \quad 5 = 5 \cdot 1.$$

Reversing the steps gives

$$1 = 1 \cdot 11 - 5 \cdot 2 = 1 \cdot 11 - 5 \cdot (13 - 11) = 6 \cdot 11 - 5 \cdot 13,$$

This shows that  $(x_0, y_0) = (-5, 6)$  is a solution to the equation  $13x + 11y = 1$ .

Multiplying through by 7 gives a **particular** solution to  $13x + 11y = 7$ :  $(x_1, y_1) = 7(x_0, y_0) = (-35, 42)$ .

To get **all** solutions, we add an integer multiple of 11 to  $x_0$  and subtract the same multiple of 13 from  $y_0$ :  $(x, y) = (-35 + 11k, 42 - 13k), \quad k \in \mathbf{Z}$

### Problem 4

**Short proofs.**

- (i) Prove that if  $2^n - 1$  is a prime number, then  $n$  is also a prime number.

**Solution:** We show the equivalent statement that if  $n$  is composite, then  $2^n - 1$  is also composite. 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.

- (ii) 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:** This is similar to Problem 59 from HW 4. First observe that, since  $p$  and  $q$  are distinct primes, a congruence modulo  $pq$  is equivalent to a system of two congruences modulo  $p$  and modulo  $q$ . Thus, it suffices to prove that the desired congruence holds modulo each of the primes  $p$  and  $q$ , i.e., that

$$(1) \quad a^{qp} + a \equiv a^q + a^p \pmod{p}, \quad a^{qp} + a \equiv a^q + a^p \pmod{q}.$$

By Fermat's Little Theorem we have, for any integer  $a$ ,

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

Applying this with  $a^q$  in place of  $a$ , we get

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

Substituting (2) and (3) on the left side of (1) gives the first congruence in (1); the second follows in the same way by interchanging the roles of  $p$  and  $q$ .

- (iii) In the RSA encryption system, a message  $M$  is encrypted by computing  $E \equiv M^e \pmod{m}$ , where  $e$  is the public encryption exponent and  $m$  the public modulus. The encrypted message  $E$  is decrypted by computing  $E^d \pmod{m}$ , where  $d$  is the decryption exponent. State precisely how  $d$  is defined, and prove that with this choice of  $d$  decryption returns the original message  $M$ , i.e., that  $E^d \equiv M \pmod{m}$ .

**Solution:** The decryption exponent is defined as a (positive) solution to the congruence

$$de \equiv 1 \pmod{\varphi(m)}.$$

With this definition,  $de = 1 + k\varphi(m)$  for some positive integer  $k$ . Since by Euler's Theorem  $M^{\varphi(m)} \equiv 1 \pmod{m}$ , we get

$$E^d \equiv (M^e)^d = M^{ed} = M^{\varphi(m)k+1} = (M^{\varphi(m)})^k M \equiv 1^k M \equiv M \pmod{m}.$$

## Problem 5

State **three** primality tests covered in class. In each case, state the name of the test, the *precise* conditions that need to be tested, and the conclusion (e.g., “ $n$  is prime”, “ $n$  is composite”, “test is inconclusive”), for each of the possible outcomes.

(i) **Test 1:**

(ii) **Test 2:**

(iii) **Test 3:**

**Solution:** Possible choices are Trial Division, Fermat Test, Lucas Test, Wilson's Test, and Pepin's Test. See the class notes for the precise formulation.

## Problem 6

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

**Solution:** We have

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

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  $\alpha$  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

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

## Problem 7

- (i) Evaluate  $f(10^{99})$ , where  $f(n) = \sum_{d|n} \mu(d)\sigma(n/d)$ . (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:** Using Dirichlet product notation, the given identity for  $f$  can be written as  $f = \mu \star \sigma$ . We have  $\sigma = \mathbf{1} \star \mathbf{id}$ , so  $f = \mu \star (\mathbf{1} \star \mathbf{id}) = (\mu \star \mathbf{1}) \star \mathbf{id} = \delta \star \mathbf{id} = \mathbf{id}$ , by the properties of the Dirichlet product. Hence  $f(n) = \mathbf{id}(n) = n$  for all  $n \in \mathbb{N}$ , so  $f(10^{99}) = \boxed{10^{99}}$ .

- (ii) Let  $\mathbf{1}$  and  $\mathbf{id}$  denote the arithmetic functions defined by  $\mathbf{1}(n) = 1$  and  $\mathbf{id}(n) = n$  for all  $n \in \mathbb{N}$ , and let  $\mathbf{1}^{-1}$  and  $\mathbf{id}^{-1}$  denote the Dirichlet product inverses of these functions. Express each of the following functions as a Dirichlet product of two of these functions, i.e., in the form  $f \star g$ , where  $f, g \in \{\mathbf{1}, \mathbf{1}^{-1}, \mathbf{id}, \mathbf{id}^{-1}\}$ .

- (a) (Sum-of-divisors function)  $\sigma =$   
 (b) (Euler phi function)  $\varphi =$   
 (c) (Divisor function)  $\nu =$

**Solution:** (a)  $\sigma = \mathbf{1} \star \mathbf{id}$ ; (b)  $\varphi = \mathbf{id} \star \mathbf{1}^{-1}$  (since  $\mathbf{id} = \varphi \star \mathbf{1}$  by Gauss' Identity); (c)  $\nu = \mathbf{1} \star \mathbf{1}$ .

- (iii) Determine, with proof, all positive integers  $n$  for which  $\varphi(3n) = 2\varphi(n)$ .

**Solution:** Writing  $n = 3^\alpha m$ , where  $(3, m) = 1$  and  $\alpha$  is a nonnegative integer, we have, by the multiplicativity of  $\varphi$ ,  $\varphi(3n) = \varphi(3^{\alpha+1}m) = \varphi(3^{\alpha+1})\varphi(m)$  and  $\varphi(n) = \varphi(3^\alpha m) = \varphi(3^\alpha)\varphi(m)$ . Hence  $\varphi(3n) = 2\varphi(n)$  holds if and only if (\*)  $\varphi(3^{\alpha+1}) = 2\varphi(3^\alpha)$ . The left side of (\*) equals  $\varphi(3^{\alpha+1}) = 2 \cdot 3^\alpha$  for any  $\alpha \geq 0$ . On the other hand, the right side equals 2 if  $\alpha = 0$ , and  $2 \cdot 3^{\alpha-1}$  if  $\alpha \geq 1$ . Hence (\*) holds if and only if  $\alpha = 0$ . Therefore the positive integers  $n$  with  $\varphi(3n) = 2\varphi(n)$  are exactly those that are not divisible by 3.

- (iv) Let  $f(n) = \sum_{d|n} \nu(d)$  (where  $\nu(d)$  is the number-of-divisors function). Find a formula for  $f(n)$  in terms of the standard prime factorization  $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$  (where, as usual, the  $p_i$  are distinct primes and the  $\alpha_i$  are positive integers). Use back of page for work if needed.

**Solution:** Since  $\nu$  is multiplicative, so is  $f$ . At prime powers  $p^\alpha$ , we can compute  $f$  directly from the definition:

$$f(p^\alpha) = \sum_{d|p^\alpha} \nu(d) = \sum_{\beta=0}^{\alpha} \nu(p^\beta) = \sum_{\beta=0}^{\alpha} (\beta + 1) = \frac{(\alpha + 1)(\alpha + 2)}{2}.$$

By the multiplicativity of  $f$  it follows that for  $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ ,

$$f(n) = f(p_1^{\alpha_1} \dots p_r^{\alpha_r}) = f(p_1^{\alpha_1}) \dots f(p_r^{\alpha_r}) = \prod_{i=1}^r \frac{(\alpha_i + 2)(\alpha_i + 1)}{2}$$

## Problem 8

- (i) Determine, with explanation, 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.)

- (ii) Determine, with explanation, whether there exists an integer  $n$  such that  $n^4 + 1$  is divisible by 2011. (Note that 2011 is prime.)

**Solution:** No such integer exists. Proof (by contradiction): Suppose such an  $n$  exists. Then  $(n^2)^2 = n^4 \equiv -1 \pmod{2011}$ . Therefore  $(*) x^2 \equiv -1 \pmod{2011}$  has a solution (namely  $x = n^2$ ), which means that  $-1$  is a quadratic residue modulo 2011. However, since  $2011 \equiv 3 \pmod{4}$ ,  $-1$  is a quadratic nonresidue modulo 2011 (by the formula for  $\left(\frac{-1}{p}\right)$ ). Thus we have a contradiction.

- (iii) Determine, with explanation, whether there exists an integer  $a$  in the range  $1 < a < 2011$  such that  $a^{11} - 1$  is divisible by 2011. (Note that 2011 is prime.)

**Solution:** We claim that no such integer exists. The divisibility condition on  $a$  implies that the congruence  $(*) a^k \equiv 1 \pmod{2011}$  holds for  $k = 11$ . Thus the order of  $a$  modulo 2011 must be a (positive) divisor of 11, and hence equal to 1 or 11. Since  $1 < a < 2011$ , we have  $a^1 \not\equiv 1 \pmod{11}$ , so the order of  $a$  cannot be 1 and therefore must be 11. On the other hand, the order must be a divisor of  $\varphi(2011) = 2010$ . Since 11 does not divide 2010 (this can easily be seen by the divisibility test modulo 11), this is impossible.

## Problem 9

**Extra Credit:** Let  $p$  be an odd prime, and let  $r$  be a primitive root modulo  $p$ . Using the known properties of primitive roots, give a *careful* proof of Wilson's Theorem. (You may use other named theorems in your proof.)

**Solution:** Wilson's Theorem states that, when  $p$  is prime, then  $(*) (p - 1)! \equiv -1 \pmod{p}$ . The key property of primitive roots needed for the proof is that the numbers  $r^1, r^2, \dots, r^{p-1}$  form a *reduced system of residues modulo  $p$* , and thus are congruent modulo  $p$  to the numbers  $1, 2, \dots, p - 1$ , in some permutation. Therefore

$$\begin{aligned} (p - 1)! &\equiv \prod_{i=1}^{p-1} r^i = r^{1+2+\dots+(p-1)} = r^{(p-1)p/2} \pmod{p} \\ &= \left(r^{(p-1)/2}\right)^p \equiv \left(\frac{r}{p}\right)^p \quad (\text{by Euler's Criterion}) \\ &= (-1)^p \quad (\text{since a primitive root is a quadratic nonresidue}) \\ &= -1 \quad (\text{since } p \text{ is odd}), \end{aligned}$$

which proves  $(*)$ .