MATH 312
AN INTRODUCTION TO NUMBER THEORY: PROBLEM SETS

By

NUNO FREITAS and ADELA GHERGA

The University of British Columbia

Problem Set 1

Section 1.3.

Exercise 4. Conjecture a formula for $\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)}$ from the value of this sum for small integers n. Prove that your conjecture is correct using mathematical induction.

Exercise 14. Show that any amount of postage that is an integer number of cents greater than 53 cents can be formed using just 7-cent and 10-cent stamps.

Exercise 22. Show by mathematical induction that if $h \geq -1$, then $1 + nh \leq (1+h)^n$ for all nonnegative integers n.

Exercise 24. Explain what is wrong with the following proof by mathematical induction that all horses are the same colour: Clearly all horses in any set of 1 horse are all the same colour. This completes the basic step. Now assume that all horses in any set of n horses are the same colour. Consider the set of $n+1$ horses, labeled with the integers $1, 2, \ldots, n+1$. By the inductive hypothesis, horses $1, 2, \ldots, n$ are all the same colour, as are horses $2, 3, \ldots, n+1$. Because these two sets of horses have common members, namely, horses $2, 3, 4, \ldots, n$, all $n+1$ horses must be the same colour. This completes the inductive argument.

Section 1.5.

Exercise 26. Show that if a and b are positive integers, then there are unique integers q and r such that $a = bq + r$, where $-b/2 < r \leq b/2$. This result is called the *modified division algorithm.*

Exercise 36. Show that if a is an integer, then 3 divides $a^3 - a$.

Section 2.1.

Exercise 12. Show that every nonzero integer can be uniquely represented in the form

$$e_k 3^k + e_{k-1} 3^{k-1} + \cdots + e_1 3 + e_0,$$

where $e_j = -1, 0$ or 1 for $j = 0, 1, 2, \ldots, k$ and $e_k \neq 0$. This expansion is called a *balanced ternary expansion.* (Hint: use the modified division algorithm of Exercise 26.)

Exercise 13. Consider a balance scale with 2 pans, A and B. Use Exercise 12 to show that any weight not exceeding $(3^k - 1)/2$ that is placed in pan A may be measured, by placing in either pan A or B, a subset of weights of $\{1, 3, 3^2, \ldots, 3^{k-1}\}$.

Exercise 17. If the base b expansion of n is $n = (a_k a_{k-1} \ldots a_1 a_0)_b$, what is the base b expansion of $b^m n$?

Section 3.1.

Exercise 6. Show that no integer of the form $n^3 + 1$ is a prime, other than $2 = 1^3 + 1$.

Exercise 8. This exercise constructs another proof of the infinitude of primes. Show that the integer $Q_n = n! + 1$, where n is a positive integer, has a prime divisor greater than n. Conclude that there are infinitely many primes.

Exercise 9. Can you show that there are infinitely many primes by looking at the integers $S_n = n! - 1$, where n is a positive integer?

Section 3.3.

Exercise 6. Let a be a positive integer. What is the greatest common divisor of a and $a+2$?

Exercise 10. Show that if a and b are integers with $(a,b) = 1$, then $(a+b, a-b) = 1$ or 2.

Exercise 12. Show that if a and b are both even integers that are not both 0, then $(a,b) = 2(a/2, b/2)$.

Exercise 24. Show that if k is a positive integer, then $3k+2$ and $5k+3$ are relatively prime.

Section 3.4.

Exercise 2. Use the Euclidean algorithm to find each of the following greatest common divisors.

(a) $(51, 87)$
(b) $(105, 300)$
(c) $(981, 1234)$

Exercise 6. Find the greatest common divisor of each of the following sets of integers.

(a) $15,\ 35,\ 90$
(b) $300,\ 2160,\ 5040$

Section 3.5.

Exercise 10. Show that if a and b are positive integers and $a^3 \mid b^2$, then $a \mid b$.

Exercise 30. Find the greatest common divisor and least common multiple of the following pairs of integers.

(a) $2 \cdot 3^2 \cdot 5^3,\ 2^2 \cdot 3^3 \cdot 7^2$
(b) $2 \cdot 3 \cdot 5 \cdot 7,\ 7 \cdot 11 \cdot 13$
(c) $2^8 \cdot 3^6 \cdot 5^4 \cdot 11^{13},\ 2 \cdot 3 \cdot 5 \cdot 11 \cdot 13$
(d) $41^{101} \cdot 47^{43} \cdot 103^{1001},\ 41^{11} \cdot 43^{47} \cdot 83^{111}$

Exercise 34. Which pairs of integers a and b have greatest common divisor 18 and least common multiple 540?

Exercise 56. Prove that there are infinitely many primes of the form $6k+5$, where k is a positive integer.

Section 3.7.

Exercise 2. For each of the following linear diophantine equations, either find all solutions or show that there are no integral solutions.

(a) $3x + 4y = 7$
(b) $12x + 18y = 50$
(c) $30x + 47y = -11$
(d) $25x + 95y = 970$
(e) $102x + 1001y = 1$

Exercise 6. The Indian astronomer and mathematician Mahavira, who lived in the ninth century, posed this puzzle: A band of 23 weary travellers entered a lush forest where they found 63 piles each containing the same number of plantains and a remaining pile containing 7 plantains. They divided the plantains equally. How many plantains were in each of the 63 piles? Solve this puzzle.

Problem Set 2

Exercise 7. Show that if a is an even integer, then $a^2 \equiv 0 \pmod 4$, and if a is an odd integer, then $a^2 \equiv 1 \pmod 4$.

Exercise 8. Show by mathematical induction that if n is a positive integer, then $4^n \equiv 1 + 3n \pmod 9$

Exercise 9. Find the least positive residues modulo 47 of each of the following integers.

(a) 2^{32}
(b) 2^{47}
(c) 2^{200}

Exercise 10. Find all solutions of each of the following linear congruences.

(a) $3x \equiv 2 \pmod 7$
(b) $6x \equiv 3 \pmod 9$
(c) $17x \equiv 14 \pmod{21}$
(d) $15x \equiv 9 \pmod{25}$

Exercise 11. For which integers c, $0 \leq c < 30$, does the congruence $12x \equiv c \pmod{30}$ have solutions? When there are solutions, how many incongruent solutions are there?

Exercise 12. Find an inverse modulo 13 of each of the following integers.

(a) 2
(b) 3
(c) 5
(d) 11

Exercise 13.

(a) Determine which integers a, where $1 \leq a \leq 14$, have an inverse modulo 14.
(b) Find the inverse of each of the following integers from part (a) that have an inverse modulo 14.

Exercise 14. Find an integers that leaves a remainder of 1 when divided by either 2 or 5, but that is divisible by 3.

Exercise 15. Find all the solutions of each of the following systems of linear congruences.

(a)
$$\begin{aligned} x &\equiv 4 \pmod{11} \\ x &\equiv 3 \pmod{17} \end{aligned}$$

(b)
$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

(c)
$$\begin{aligned} x &\equiv 0 \pmod 2 \\ x &\equiv 0 \pmod 3 \\ x &\equiv 1 \pmod 5 \\ x &\equiv 6 \pmod 7 \end{aligned}$$

Exercise 16. An ancient Chinese problem asks for the least number of gold coins a band of 17 pirates could have stolen. The problem states that when the pirates divided the coins into equal piles, 3 were left over. When they fought over who should get the extra coins, one of the pirates was slain. When the remaining pirates divided the coins into equal piles, 10 coins were left over. When the pirates fought again over who should get the extra coins, another pirate was slain. When they divided the coins into equal piles again, no coins were left over. What is the answer to this problem?

Exercise 17. Determine the highest power of 5 that divides each of the following positive integers.

(a) $112,250$
(b) $4,860,625$
(c) $235,555,790$
(d) $48,126,953,125$

Exercise 18. Which of the following integers is divisible by 11?

(a) $10,763,732$
(b) $1,086,320,015$
(c) $674,310,976,375$
(d) $8,924,310,064,537$

Exercise 19. An old receipt has faded. It reads 88 chickens at a total of $\$x4.2y$, where x and y are unreadable digits. How much did each chicken cost?

Exercise 20. Suppose that one digit, indicated with a question mark, in each of the following ISBN-10 codes has been smudged and cannot be read. What should this missing digit be?

(a) $0-19-8?3804-9$
(b) $91-554-212?-6$
(c) $?-261-05073-X$

Exercise 21. While copying the ISBN-10 for a book, the clerk accidentally transposed two digits. If the clerk copied the ISBN-10 as $0-07-289095-0$ and did not make any other mistakes, what is the correct ISBN-10 for this book?

Problem Set 3

Exercise 22. What is the remainder when $5!25!$ is divided by 31?

Exercise 23. What is the remainder when 6^{2000} is divided by 11?

Exercise 24. Using Fermat's little theorem, find the least positive residue of $2^{1,000,000}$ modulo 17.

Exercise 25. Show that $1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$ when p is an odd prime.

Exercise 26. Show that 45 is a pseudoprime to the bases 17 and 19

Exercise 27. Show that if p is a prime and $2^p - 1$ is composite, then $2^p - 1$ is a pseudoprime to the base 2.

Exercise 28. Show that 25 is a strong pseudoprime to the base 7.

Exercise 29.

(a) Show that every integer of the form $(6m+1)(12m+1)(18m+1)$, where m is a positive integer such that $6m+1, 12m+1$, and $18m+1$ are all primes, is a Carmichael number.
(b) Conclude from part (a) that $1729 = 7 \cdot 13 \cdot 19$; $294,409 = 37 \cdot 73 \cdot 109$; $56,052,361 = 211 \cdot 421 \cdot 631$; $118,901,521 = 271 \cdot 541 \cdot 811$; and $172,947,529 = 307 \cdot 613 \cdot 919$ are Carmichael numbers.

Exercise 30. Find the last digit of the decimal expansion of $7^{999,999}$.

Exercise 31. Show that if a is an integer such that a is not divisible by 3 or such that a is divisible by 9, then $a^7 \equiv a \pmod{63}$.

Exercise 32. Show that $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$, if a and b are relatively prime positive integers.

Exercise 33. Show that the solutions to the simultaneous system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}, \end{aligned}$$

where the m_j are pairwise relatively prime, are given by

$$x \equiv a_1 M_1^{\phi(m_1)} + a_2 M_2^{\phi(m_2)} + \cdots + a_r M_r^{\phi(m_r)} \pmod{M},$$

where $M = m_1 m_2 \cdots m_r$ and $M_j = M/m_j$ for $j = 1, 2, \ldots, r$.

Exercise 34. Find all positive integers n such that $\phi(n)$ has each of these values. Be sure to prove that you have found all solutions.

(a) 1
(b) 2
(c) 3
(d) 4

Exercise 35. Show that there is no positive integer n such that $\phi(n) = 14$.

Exercise 36. Show that if n is an odd integer, then $\phi(4n) = 2\phi(n)$.

Problem Set 4

Exercise 37. For which positive integers n is the sum of divisors of n odd?

Exercise 38. Show that if $k > 1$ is an integer, then the equation $\tau(n) = k$ has infinitely many solutions.

Exercise 39. Which positive integers have exactly four positive divisors?

Exercise 40. Show that the equation $\sigma(n) = k$ has at most a finite number of solutions when k is a positive integer.

Exercise 41. Show that a positive integer n is composite if and only if $\sigma(n) > n + \sqrt{n}$.

Exercise 42. Find the six smallest even perfect numbers.

If n is a positive integer, we say that n is *deficient* if $\sigma(n) < 2n$, and we say that n is *abundant* if $\sigma(n) > 2n$. Every integer is either deficient, perfect, or abundant.

Exercise 43. Show that any proper divisor of a deficient or perfect number is deficient.

Exercise 44. Show that if $n = p^a q^b$, where p and q are distinct odd primes and a and b are positive integers, then n is deficient.

Problem Set 5

Exercise 45. Determine the following orders

(a) $\operatorname{ord}_{11} 3$
(b) $\operatorname{ord}_{17} 2$
(c) $\operatorname{ord}_{21} 10$
(d) $\operatorname{ord}_{25} 9$

Exercise 46. Find a primitive root modulo each of the following integers.

(a) 4
(b) 5
(c) 10
(d) 13
(e) 14
(f) 18

Exercise 47. Show that the integer 20 has no primitive roots.

Exercise 48. Show that if n is a positive integer and a and b are integers relatively prime to n such that $(\operatorname{ord}_n a, \operatorname{ord}_n b) = 1$, then $\operatorname{ord}_n(ab) = \operatorname{ord}_n a \cdot \operatorname{ord}_n b$.

Exercise 49. Show that if m is a positive integer and a is an integer relatively prime to m such that $\operatorname{ord}_m a = m - 1$, then m is prime.

Exercise 50. Find a complete set of incongruent primitive roots of 13.

Exercise 51. Let r be a primitive root of the prime p with $p \equiv 1 \pmod 4$. Show that $-r$ is also a primitive root.

Exercise 52.

(a) Find the number of incongruent roots modulo 6 of the polynomial $x^2 - x$.
(b) Explain why the answer to part (a) does not contradict Lagrange's Theorem.

Exercise 53. Show that if p is a prime and $p = 2q + 1$, where q is an odd prime and a is a positive integer with $1 < a < p - 1$, then $p - a^2$ is a primitive root modulo p.

Exercise 54. Find all the solutions of the following congruences.

(a) $3x^5 \equiv 1 \pmod{23}$
(b) $3x^{14} \equiv 2 \pmod{23}$

Exercise 55. Find all the solutions of the following congruences.

(a) $3^x \equiv 2 \pmod{23}$
(b) $13^x \equiv 5 \pmod{23}$

Exercise 56. For which positive integers a is the congruence $ax^4 \equiv 2 \pmod{13}$ solvable?

Exercise 57. For which positive integers b is the congruence $8x^7 \equiv b \pmod{29}$ solvable?

Exercise 58. Show that if p is an odd prime and r is a primitive root of p, then $\operatorname{ind}_r(p-1) = (p-1)/2$.

Exercise 59. Let p be an odd prime. Show that the congruence $x^4 \equiv -1 \pmod{p}$ has a solution if and only if p is of the form $8k + 1$.

Exercise 60. Let p be a prime, $p > 3$. Show that if $p \equiv 2 \pmod{3}$, then every integer not divisible by 3 is a third-power, or *cubic*, residue of p, whereas if $p \equiv 1 \pmod{3}$, an integer a is a cubic residue of p if and only if $a^{(p-1)/3} \equiv 1 \pmod{p}$.

Problem Set 6

Exercise 61. Show that if (x, y, z) is a primitive Pythagorean triple, then either x or y is divisible by 3.

Exercise 62. Show that if (x, y, z) is a primitive Pythagorean triple, then exactly one of x,y, and z is divisible by 5.

Exercise 63. Show that if (x, y, z) is a primitive Pythagorean triple, then at least one of x, y, and z is divisible by 4.

Exercise 64. Let $x_1 = 3$, $y_1 = 4$, $z_1 = 5$, and let x_n, y_n, z_n, for $n = 2, 3, 4, \ldots$, be defined recursively by

$$\begin{aligned} x_{n+1} &= 3x_n + 2z_n + 1, \\ y_{n+1} &= 3x_n + 2z_n + 2, \\ z_{n+1} &= 4x_n + 3z_n + 2. \end{aligned}$$

Show that (x_n, y_n, z_n) is a Pythagorean triple.

Exercise 65. Find formulas for the integers of all Pythagorean triples (x, y, z) with $z = y+2$.

Exercise 66. Using Fermat's little theorem, show that if p is prime, and

(a) if $x^{p-1} + y^{p-1} = z^{p-1}$, then $p \mid xyz$.
(b) if $x^p + y^p = z^p$, then $p \mid (x + y - z)$.

Exercise 67. The Diophantine equation $x^4 - y^4 = z^2$ has no solutions in nonzero integers. Using this fact, show that the area of a right triangle with integer sides is never a perfect square.

Problem Set 7

Exercise 68. Using the Fermat factorization method, factor each of the following positive integers.

(a) 73
(b) 46,009
(c) 11,021

Exercise 69. Use the Pollard $p-1$ method to find a divisor of 7,331,117. (For this exercise, you will need to use either a calculator or computational software.)

Exercise 70. Decrypt the ciphertext message $LFDPHLVDZLFRQTXHUHG$, which has been encrypted using the Caesar cipher

Exercise 71. Decrypt the message $RTOLKTOIK$, which has been encrypted using the affine transformation $C \equiv 3P + 24 \pmod{26}$

Exercise 72. The message

$$KYVMRCLVFWKYVBVPZJJVMVEKVVE$$

was encrypted using a shift transformation $C \equiv P + k \pmod{26}$. Use frequencies of letters to determine the value of k. What is the plaintext message?

Exercise 73. If the two most common letters in a long ciphertext, encrypted by an affine transformation $C \equiv aP + b \pmod{26}$, are X and Q, respectively, then what are the most likely vales for a and b?

Exercise 74. The message

$$MJMZKCXUNMGWIRYVCPUWMPRRWGMIOPMSNYSRYRAZPXMCDWPRYEYXD$$

was encrypted using an affine transformation $C \equiv aP+b \pmod{26}$. Use frequencies of letters to determine the values of a and b. What is the plaintext message?

Exercise 75. With modulus $p = 29$ and unknown encryption key e, modular exponentiation produces the ciphertext 04 19 19 11 04 24 09 15 15. Cryptanalyze the above cipher, if it is also known that the ciphertext block 24 corresponds to the plaintext letter U (with numerical equivalent 20). (Hint: First find the logarithm of 24 to the base 20 modulo 29, using some guesswork.)

Exercise 76. Find the primes p and q if $n = pq = 4,386,607$ and $\phi(n) = 4,382,136$.

Exercise 77. If the ciphertext message produced by RSA encryption with the key $(e, n) = (5, 2881)$ is

$$0504\ 1874\ 0347\ 0515\ 2088\ 2356\ 0736\ 0468,$$

what is the plaintext message?

Exercise 78.

Exercise 79. Suppose that two people have RSA encryption keys with encryption moduli n_1 and n_2, respectively, where $n_1 \neq n_2$. Show how you could break the system if $(n_1, n_2) > 1$.