Number Theory

Exercises

1 The Euclidean Algorithm

1. Prove that, if a is an odd integer, then $32|(a^2-5)(a^2+15)$.

2. Prove that, for every solution of the diophantine equation $a^2+b^2=c^2$, either a or b must be even.

3. Prove that for every integer a there exist integers b and c such that $b(4a+3)+c(11a+8)=1$.

4. Prove, without using combinatorial considerations, that, for any integers a and k with $2 \leq k \leq 6$, the number

$$\frac{a(a+1)\ldots(a+k-1)}{k!}$$

is an integer.

5. Prove that, if $a|b$ and $c|d$, then $\gcd(a,c)|\gcd(b,d)$.

6. Prove that, if a is relatively prime to both b and c, then a is relatively prime to bc.

7. Employ the Euclidean algorithm to calculate the greatest common divisor of 38076 and 5256.

8.

(a) Explain how, given integers a, b with $\gcd(a,b)=d$, we can apply the Euclidean algorithm to find integers s, t such that $sa+tb=d$.

(b) Find integers s, t such that $s \cdot 1001 + t \cdot 1643 = 1$.

9. Let a and b be relatively prime positive integers.

(a) Prove that there exists an integer $N = N(a, b)$, such that every integer $n \geq N$ can be expressed in the form $n = sa + tb$ for appropriate integers $s, t \geq 0$.

(b) Find an upper bound on N in terms of a and b only.

10. Prove that, if a, b, c are integers, at least two of which are nonzero, then $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$.

2 The Fundamental Theorem of Arithmetic

11. Let n be a positive integer with known prime power factorization $n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$.

(a) Find the number of divisors of n.

(b) Find the sum of these divisors.

12. Let a, b be integers such that $\gcd(a, b) = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$.

(a) What are the possible values of $\gcd(a^2, b^2)$?

(b) Same for $\gcd(a^2, b)$ and $\gcd(a^2, b^3)$.

13. Write down the prime power factorization of $n!$ as explicitly as possible.

14. Let $n \geq 2$.

(a) Show that, unless n is a power of 2, the number $2^{2^n} + 1$ is composite.

(b) Show that, unless n is a prime, the number $2^n - 1$ is composite.

15. A number is an *almost prime* if it is either a prime or a product of two primes. Suggest an algorithm with running time $O(n^\theta)$, where $\theta < 1/2$, for deciding whether an integer n is an almost prime.

16. Which positive integers n have the property that $n, n+2, n+4$ are all prime?

17.

(a) Prove that there exist infinitely many primes of the form $6n+5$.

(b) Explain why your proof does not work to show that there exist infinitely many primes of the form $6n+1$.

18. Prove that, if $p_1, p_2, \ldots, p_n$ are distinct primes, then the sum $1/p_1 + 1/p_2 + \ldots + 1/p_n$ cannot be an integer.

3 Congruences

19. Calculate:

(a) $88^{88} \bmod 15$.

(b) $213^{1024} \bmod 7$.

20. For any $b \geq 2$, find two integers d_1, d_2, relatively prime to b, such that it is easy to test the divisibility of a number n by d_1 and d_2 in terms of the base b expansion of n. Formulate and prove the divisibility criteria.

21. Let $b \geq 2$. Characterize the integers d possessing the following property: There exists a constant $C = C(b, d)$ such that the divisibility of an integer n by d can be decided if we know only the C least significant digits in the base b expansion of n.

22.

(a) Show that, given the last digit in the base 10 expansion of n^3, you can determine the last digit in the expansion of n.

(b) Conclude that, by memorizing the cubes of the integers in the range 0-9, you can easily find n if n^3 is given and is a number with at most 6 digits.

23. Find all solutions of the following congruences:

(a) $x^3 - 6x^2 + 2x + 3 \equiv 0 \pmod{7}$.

(b) $2x^4 + 3x^3 + x + 2 \equiv 0 \pmod{5}$.

(c) $x^5 - 1 \equiv 0 \pmod{9}$.

24. Solve the following congruences:

(a) $49x \equiv 287 \pmod{1001}$.

(b) $63x \equiv 999 \pmod{2142}$.

(c) $15x \equiv 40 \pmod{196}$.

25. Let $p_1, p_2, \ldots, p_k$ be distinct primes. Prove that there exist infinitely many integers n which are congruent to 1 modulo p_1, to 2 modulo p_2^2, to 3 modulo p_3^3, and so forth.

26.

(a) Prove that the system of congruences $x \equiv a \pmod{m}$
$x \equiv b \pmod{n}$ has a solution if and only if $\gcd(m,n)|b-a$. Show that the solution, if it exists, is unique modulo $\operatorname{lcm}(m,n)$.

(b) Conclude that, given a system of congruences as in the Chinese Remainder Theorem, but without the provision that the moduli are pairwise prime, you can effectively solve it.

27. Find all solutions of the following systems of congruences:

(a) $x \equiv 1 \pmod{3}$
$x \equiv 2 \pmod{4}$
$x \equiv 4 \pmod{5}$
$x \equiv 17 \pmod{49}$.

(b) $x \equiv 0 \pmod{12}$
$x \equiv 2 \pmod{31}$
$x \equiv 3 \pmod{35}$
$x \equiv 100 \pmod{121}$.

(c) $x \equiv 6 \pmod{10}$
$x \equiv 60 \pmod{63}$
$x \equiv 600 \pmod{1331}$.

28.

(a) Let a be a positive integer, c a divisor of a and $X \sim \mathrm{U}[0, a-1]$. Let Y be the least non-negative residue of X modulo c. Determine the distribution of Y.

(b) Let a, b be relatively prime positive integers, $X \sim \mathrm{U}[0, a-1]$ and $Y \sim \mathrm{U}[0, b-1]$. Let Z be the least non-negative integer which is congruent to X modulo a and to Y modulo b. Determine the distribution of Z.

29. A certain top secret is held in the form a very large integer N. The secret is known to the Airforce commander only. The commander wants that, in case he is incapacitated, any three of his r assistants will be able to recover N, but no two of them will be able to do so by themselves.

(a) Let $p_1, p_2, \ldots, p_r$ be distinct primes, all of which are much smaller than $\sqrt{N}$ but much larger than $\sqrt[3]{N}$. Suggest a way of using the p_i's to give the assistants partial information as required.

(b) More generally, suggest a way of solving the problem if any k of the assistants should be able to recover N, but no $k-1$ should.

4 Fermat's Little Theorem

30. Prove in a combinatorial way that, if p is a prime and $1 \le k \le p-1$, then $p|\binom{p}{k}$.

31. Prove that $\log_2 n!$ is irrational for $n \ge 3$. (Consequently, the average number of comparisons required for sorting an n-element list, by any algorithm based on the comparison of keys, is strictly larger than $\log_2 n!$.)

32. Employ Fermat's Theorem to show that:

(a) If $\gcd(a, 1001) = 1$, then $a^{60} \equiv 1 \pmod{1001}$.

(b) If $\gcd(a, 78) = \gcd(b, 78) = 1$, then $1872|a^{12} - b^{12}$.

33. Let p be a prime, and a, b integers not divisible by p, such that $p|a^p - b^p$. Show that $p|a - b$, and use it to show that $p^2|a^p - b^p$.

34. Show that, if p is an odd prime, then $\binom{p-1}{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod{p}$.

35.

(a) Show that, if $k|l$, then $a^k - 1|a^l - 1$ for every integer a.

(b) Use part (a) to show that, if p is a prime, then $2^p - 1$ is either a prime or a pseudoprime in base 2.

(c) Use part (a) to show that, for any positive integer n, the number $2^{2^n} + 1$ is either a prime or a pseudoprime in base 2.

36.

(a) Find all bases b such that 15 is a pseudoprime in base b.

(b) Find all bases b such that 21 is a pseudoprime in base b.

37. Show that $6601 = 7 \cdot 23 \cdot 41$ is a Carmichael number.

38. Prove that the set $\{k! \bmod p : 1 \leq k \leq p-1\}$ is of cardinality $\lceil \sqrt{2(p-2)} \rceil$ at least.

39. Show that $18! \equiv -1 \pmod{437}$.

40. Prove that a number $n > 1$ is prime if and only if $(n-2)! \equiv -1 \pmod{n}$.

41. Let $n = p_1 p_2 \ldots p_r$ be a product of distinct primes. How many solutions does the congruence $x^2 \equiv -1 \pmod{n}$ have? (Hint: your answer should depend on whether all p_i's are 1 modulo 4 or not all of them are.)

42. Prove that, if $p, p+2$ are twin primes, then $4(p-1)! + p + 4 \equiv 0 \pmod{p(p+2)}$.

5 Euler's Totient Function and Euler's Theorem

43. Let a, b be divisors of n and $X \sim \mathrm{U}[0, n-1]$. Under what conditions are the events $\{\gcd(X, a) = 1\}$ and $\{\gcd(X, b) = 1\}$ independent?

44. Let $n \geq 2$. Let the random variable X be the result of choosing one of the $\phi(n)$ numbers between 1 and $n-1$ which are relatively prime to n, with the same probability $1/\phi(n)$ for each. Find $E(X)$.

45. Prove the explicit formula for $\phi(n)$ directly from the inclusion-exclusion principle.

46. A *lattice point in the plane* is a point (m, n) with integer coordinates. A lattice point is *visible from the origin* if the line segment connecting it to the origin contains no lattice points strictly between the point and the origin. Prove that the number of lattice points visible from the origin in the square $[1, N] \times [1, N]$ is $1 + 2\sum_{k=2}^{n} \phi(k)$.

47. Show that $\phi(n) = (1 - 1/p)n$ for a prime p and integer n if and only if n is a non-trivial power of p.

48. Show that the diophantine equation $\phi(n) = m^k$ has infinitely many solutions (m, n) for any fixed k.

49. Prove that, if $\delta > 0$ is any fixed real number, then $\phi(n) > n^{1-\delta}$ for all sufficiently large n.

50. Characterize the pairs (m, n) for which $\phi(mn) = m\phi(n)$.

51. Prove that, if $\phi(n)|n - 1$, then n is square-free.

52. Find all solutions (if any) of the equations:

(a) $\phi(n) = 10$.

(b) $\phi(n) = 14$.

(c) $\phi(n) = 100$.

53. Show that:

(a) $a^{13} \equiv a \pmod{2 \cdot 3 \cdot 5 \cdot 7 \cdot 13}$ for every integer a.

(b) $a^{17} \equiv a \pmod{2^6 \cdot 3 \cdot 5 \cdot 17}$ for every odd integer a.

54. Show that, if m, n are relatively prime, then $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$.

55. Calculate:

(a) The last two digits in the decimal expansion of 3^{100}.

(b) $3^{1000000} \bmod 35$.

6 The Group of Units Modulo an Integer

56. Prove that, if there exists an element of order $n - 1$ modulo n, then n is a prime.

57. Denote by $\mathrm{ord}_n(a)$ the order of a (with $\gcd(a, n) = 1$) modulo n. Prove that $\max_{a:\gcd(a,n)=1} \mathrm{ord}_n(a) \xrightarrow[n\to\infty]{} \infty$.

58. Prove that, if the order of a modulo an odd prime p is $2k$, then $a^k \equiv -1 \pmod{p}$.

59. Suppose $a^{128} \equiv -1 \pmod{257}$ for a certain a. Show that a is a primitive root modulo 257.

60. Let a be a primitive root modulo some odd prime p. Provide a simple necessary and sufficient condition on p for $-a$ to be also a primitive root modulo p.

61. Let p be an odd prime, and a an element of order 3 modulo p. Prove that $a+1$ is of order 6 modulo p. (Hint: Show that $a^2+a+1 \equiv 0 \pmod{p}$.)

62.

(a) Show that all the odd primes appearing in the prime power factorization of a number of the form $n^2 + 1$ are of the form $4k+1$. (Hint: Find the order of n modulo an odd prime divisor of $n^2 + 1$.)

(b) Conclude from the preceding part that there exist infinitely many primes of the form $4k+1$. (Hint: Suppose there exist only finitely many primes $p_1, p_2, \ldots, p_l$ of this form, and consider the number $(2p_1p_2 \ldots p_l)^2 + 1$.)

63. Let p be an odd prime, and a a primitive root modulo p.

(a) Show that $a^{(p-1)/2} \equiv -1 (\operatorname{mod} p)$.

(b) Conclude from the preceding part that the product of two primitive roots modulo p cannot possibly be a primitive root modulo p.

64. Let p be an odd prime. Find the value modulo p of the product of all primitive roots modulo p.

65. Prove that, if a is a primitive root modulo n and $m|n$, then a is a primitive root modulo m.

66. Find a primitive root modulo 29^{29}.

67. Given a positive integer n, denote by $e(n)$ the smallest positive integer e for which $a^e \equiv 1 \pmod{n}$ for every a with $\gcd(a, n) = 1$.

(a) Express $e(n)$i terms of the prime power factoriztion of n.

(b) Does there necessarily exist an integer a whose order modulo n is $e(n)$?

7 Diophantine Equations

68. Show that every integer $n \geq 3$ belongs to some Pythagorean triple.

69. Find all Pythagorean triples whose terms form

(a) an arithmetic progression;

(b) a geometric progression.

70. Prove that the Diophantine equation

$$x^2 + y^2 = z^4$$

has infinitely many solutions with $\gcd(x, y, z) = 1$.

71. Find all solutions of the Diophantine equation

$$x^2 + y^2 = 2z^2.$$

(Hint: Multiply both sides by 2 and write the left-hand side as a sum of two squares.)

72. Let C denote the unit circle in the plane:

$$C = \{(x, y) : x^2 + y^2 = 1\}.$$

Prove that the set of all points on C, both of whose coordinates are rational, is dense in C.

73. For which integers z does the Diophantine equation

$$x^2 - y^2 = z$$

have a solution?

74. Show that the following Diophantine equations have no solutions:

(a) $x^2 + y^2 = 4z + 3$.

(b) $x^2 + y^2 = 9z + 3$.

(c) $x^2 + 2y^2 = 8z - 3$.

75. Show that the Diophantine equation

$$x^2 + y^2 = 3(s^2 + t^2)$$

has no non-trivial solutions.

76. Show that the Diophantine equation

$$x^3 + 2y^3 + 4z^3 = 6xyz$$

has no non-trivial solutions. (Hint: First study the possible solutions modulo 7.)

77. Show that the Diophantine equation

$$x^3 + 2y^3 = 7(s^3 + 2t^3)$$

has no non-trivial solutions.

8 Perfect Numbers

78.

(a) Show that an even perfect number ends with either 6 or 8.

(b) Show that, moreover, it ends with either 6 or 28.

79. Find infinitely many positive integers n satisfying $\sigma(n) = 2n - 1$.

80.

(a) Prove that for any real number $\beta \geq 1$ (or $\beta = \infty$) there exists a sequence of integers $(n_k)_{k=1}^{\infty}$ such that $\sigma(n_k)/n_k \underset{k\to\infty}{\longrightarrow} \beta$. (Hint: You may use the fact that the sum of reciprocals of all primes is infinite.)

(b) Prove that for any real number $\gamma \leq 1$ (or $\gamma = 0$) there exists a sequence of integers $(n_k)_{k=1}^{\infty}$ such that $\phi(n_k)/n_k \underset{k\to\infty}{\longrightarrow} \gamma$.

81.

(a) Show that an odd perfect number must have at least three distinct prime factors.

(b) Show that an odd perfect square-free number must have at least five prime factors.

82.

(a) Prove that, if there exist infinitely many odd perfect numbers, then there exist infinitely many integers n satisfying $\sigma(n) = 3n$.

(b) Verify that each of the three numbers $120, 672$ and 523776 solves the equation $\sigma(n) = 3n$.

(c) A number n is *multi-perfect* if $n|\sigma(n)$. Verify that the numbers 30240 and 32760 are multi-perfect.

83. Two positive integers are *amicable* if the sum of proper divisors of each is equal to the other. Verify that 220 and 284 are amicable, as are 1184 and 1210.

9 Quadratic Residues and Quadratic Reciprocity

84. Find the number of solutions of each of the following congruences:

(a) $x^2 \equiv 2 \pmod{107}$.

(b) $x^2 \equiv -2 \pmod{107}$.

(c) $x^2 \equiv 2 \pmod{109}$.

(d) $x^2 \equiv -2 \pmod{109}$.

85. Find the number of solutions of each of the following congruences:

(a) $x^2 \equiv -1 \pmod{899}$.

(b) $x^2 \equiv -1 \pmod{578}$.

(c) $x^2 \equiv -1 \pmod{1105}$.

86. Let r be a primitive root modulo $n > 2$. Show that $r^{\phi(n)/2} \equiv 1 \pmod{n}$.

87.

(a) Show that, if p is a prime of the form $4k + 1$, then the sum of all quadratic residues modulo p in the interval $[1, p - 1]$ is $p(p - 1)/4$, and in particular is divisible by p.

(b) Show that, if p is a prime of the form $4k + 3$, then the sum of all quadratic residues modulo p in the interval $[1, p - 1]$ is divisible by p (although it cannot be $p(p - 1)/4$ any more).

88. Let p be a prime. An integer a, which is relatively prime to p, is a *cubic residue modulo* p if the congruence $x^3 \equiv a \pmod{p}$ has a solution.

(a) Prove that, if p is of the form $3k+2$, then all integers in the range $[1, p-1]$ are cubic residues modulo p.

(b) Prove that, if p is of the form $3k+1$, then exactly $(p-1)/3$ of the integers in the range $[1, p-1]$ are cubic residues modulo p.

89. Determine which of the following congruences are solvable.

(a) $x^2 \equiv 7 \pmod{137}$.

(b) $x^2 \equiv -7 \pmod{137}$.

(c) $x^2 \equiv 7 \pmod{139}$.

(d) $x^2 \equiv -7 \pmod{139}$.

90. Characterize all primes p for which the congruence $x^2 \equiv 17 \pmod{p}$ has a solution.

91. Characterize all primes p for which $\left(\frac{14}{p}\right) = -1$.

92. Show that, if p and q are twin primes, then there exists an integer a such that $p|(a^2-q)$ if and only if there exists an integer b such that $q|(b^2-p)$.

93. Prove that, if p is a prime of the form $4k+3$, then the congruence $x^2 \equiv -(p+1)/4 (\bmod\, p)$ has no solution.

94.

(a) For which primes p can you find integers a and b, relatively prime to p, such that a^2+b^2 is divisible by p?

(b) Same with any prime power p^k instead of p.

(c) Same with any integer n instead of p.

10 Farey Sequences

95. Let a/b and c/d be the fractions closest to $1/2$ in the Farey sequence of order n (that is, $a/b < 1/2 < c/d$). Express a, b, c, d in terms of n.

96. Prove that the length of the Farey sequence of order n is $1 + \sum_{i=1}^{n} \phi(i)$. Find the sum of all elements of the sequence.

97. Find the minimal and the maximal distance between pairs of adjacent Farey fractions in the Farey sequence of order n.