1. “If \( k > 1 \) then \( 2^k - 1 \) is not a perfect square.” Which of the following is a correct proof?

(a) If \( 2^k - 1 = n^2 \) then \( 2^k - 1 = (n - 1)^2 \) and \( \frac{n^2 + 1}{(n-1)^2+1} = \frac{2^k}{2} = 2. \) But this latter ratio is 2 if and only if \( n = 1 \) or \( n = 3. \) Thus, \( 2^k - 1 = n^2 \) leads to a contradiction.

(b) If \( 2^k - 1 = n^2 \) then \( 2^k = n^2 + 1. \) Since 2 divides \( n^2, \) 2 does not divide \( n^2 + 1. \) This is a contradiction since obviously 2 divides \( 2^k. \)

(c) \( 2^k - 1 \) is odd and an odd number which is a perfect square can’t differ from a power of two by one.

(d) \( 2^k - 1 \) is odd and an odd number can never be a perfect square.

(e) If \( 2^k - 1 = n^2 \) then \( n \) is odd. If \( n = 2j + 1 \) then \( 2^k - 1 = (2j + 1)^2 = 4j^2 + 4j + 1 \) which implies that \( 2^k, k > 1 \) is divisible by 2 but not by 4. This is a contradiction.

2. The repeating decimal number \( 3.14159265265265\ldots \) written as a ratio of two integers \( a/b \) is

(a) 313845111/999900000
(b) 313844841/99900000
(c) 313845006/99990000
(d) 313845106/99900000
(e) 313845123/99000000

3. Which of the following statements is true:

(a) A number is rational if and only if its square is rational.
(b) An integer \( n \) is odd if and only if \( n^2 + 2n \) is odd.
(c) A number is irrational if and only if its square is irrational.
(d) A number \( n \) is odd if and only if \( n(n + 1) \) is even
(e) At least one of two numbers \( x \) and \( y \) is irrational if and only if the product \( xy \) is irrational.

4. Which of the following statements is true:

(a) A number \( k \) divides the sum of three consecutive integers \( n, n + 1, \) and \( n + 2 \) if and only if it divides the middle integer \( n + 1. \)

(b) An integer \( n \) is divisible by 6 if and only if it is divisible by 3.

(c) For all integers \( a, b, \) and \( c, \) \( a \mid bc \) if and only if \( a \mid b \) and \( a \mid c. \)

(d) For all integers \( a, b, \) and \( c, \) \( a \mid (b + c) \) if and only if \( a \mid b \) and \( a \mid c. \)
(e) If \( r \) and \( s \) are integers, then \( r \mid s \) if and only if \( r^2 \mid s^2 \).

5. For all \( N \geq 0 \), if \( N = k(k+1)(k+2) \) is the product of three consecutive non-negative integers then for some integer \( s > k \), \( N \) is divisible by a number of the form

(a) \( s^2 - 1 \)
(b) \( s^2 - 2 \)
(c) \( s^2 \)
(d) \( s^2 + 1 \)
(e) \( s^2 + 2 \)

6. To one percent accuracy, the number of integers \( n \) in the list \( 0^4, 1^4, 2^4, \ldots, 1000^4 \) such that \( n \% 16 = 1 \) is

(a) 20 percent
(b) 50 percent
(c) 30 percent
(d) 35 percent
(e) 25 percent

7. Which of the following statements is TRUE:

(a) For all odd integers \( n \), \( \lceil n/2 \rceil = \frac{n+1}{2} \).
(b) For all real numbers \( x \) and \( y \), \( \lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil \).
(c) For all real numbers \( x \), \( \lceil x^2 \rceil = (\lceil x \rceil)^2 \).
(d) For all real numbers \( x \) and \( y \), \( \lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil \).
(e) For all real numbers \( x \) and \( y \), \( \lfloor xy \rfloor = \lfloor x \rfloor \lfloor y \rfloor \).

8. Which of the following statements is logically equivalent to the statement, “If \( a \) and \( b \neq 0 \) are rational numbers and \( r \neq 0 \) is an irrational number, then \( a + br \) is irrational.”

(a) If \( a \) and \( b \neq 0 \) are rational and \( r \neq 0 \) is real, then \( a + br \) is rational only if \( r \) is irrational.
(b) If \( a \) and \( b \neq 0 \) are rational and \( r \neq 0 \) is real, then \( a + br \) is irrational only if \( r \) is irrational.
(c) If \( a \) and \( b \neq 0 \) are rational and \( r \neq 0 \) is real, then \( r \) is rational only if \( a + br \) is rational.
(d) If \( a \) and \( b \neq 0 \) are rational and \( r \neq 0 \) is real, then \( a + br \) is rational only if \( r \) is rational.
(e) If \( a \) and \( b \neq 0 \) are rational and \( r \neq 0 \) is real, then \( a + br \) is irrational only if \( r \) is rational.

9. The number of primes of the form \( |n^2 - 6n + 5| \) where \( n \) is an integer is

(a) 0  (b) 1  (c) 2  (d) 3  (e) 4
10. The Euclidean Algorithm is used to produce a sequence $X_1 > X_2 > \cdots > X_{k-1} > X_k = 0$ of positive integers where each $X_t$, $2 < t \leq k$, is the remainder gotten by dividing $X_{t-2}$ by $X_{t-1}$. If $X_{k-1} = 45$ then the set of all (positive) common divisors of $X_1$ and $X_2$ is
   
   (a) $\{1, 3, 5\}$
   
   (b) $\{1, 3, 5, 9, 15, \}$
   
   (c) $\{1, 9, 15, 45\}$
   
   (d) $\{1, 3, 5\}$
   
   (e) $\{1, 3, 5, 9, 15, 45\}$

11. Let $L$ be the least common multiple of 175 and 105. Among all of the common divisors $x > 1$ of 175 and 105, let $D$ be the smallest. Which is correct of the following:
   
   (a) $D = 5$ and $L = 1050$
   
   (b) $D = 5$ and $L = 35$
   
   (c) $D = 7$ and $L = 525$
   
   (d) $D = 5$ and $L = 525$
   
   (e) $D = 7$ and $L = 1050$

12. The Euclidean Algorithm is used to produce a sequence $X_1 > X_2 > X_3 > X_4 > X_5 = 0$ of positive integers where $X_t = q_{t+1}X_{t+1} + X_{t+2}, t = 1, 2, 3$. The quotients are $q_2 = 3$, $q_3 = 2$, and $q_4 = 2$. Which of the following is correct?
   
   (a) $\gcd(X_1, X_2) = -2X_1 + 6X_2$
   
   (b) $\gcd(X_1, X_2) = -2X_1 - 6X_2$
   
   (c) $\gcd(X_1, X_2) = -2X_1 - 7X_2$
   
   (d) $\gcd(X_1, X_2) = 2X_1 + 7X_2$
   
   (e) $\gcd(X_1, X_2) = -2X_1 + 7X_2$

Answers: 1 (e), 2 (d), 3 (b), 4 (e), 5 (a), 6 (b), 7 (a), 8 (d), 9 (c), 10 (e), 11 (d), 12 (e).
<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>$k \mid n$</td>
<td>$k$ divides $n$; $n/k \in \mathbb{Z}$</td>
<td>NT-2</td>
</tr>
<tr>
<td>Function (particular)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\lfloor x \rfloor$</td>
<td>greatest integer</td>
<td>NT-9</td>
</tr>
<tr>
<td>$\lceil x \rceil$</td>
<td>ceiling</td>
<td>NT-9</td>
</tr>
<tr>
<td>$\gcd(a, b)$</td>
<td>greatest common divisor</td>
<td>NT-16</td>
</tr>
<tr>
<td>$\phi(n)$</td>
<td>Euler $\phi$</td>
<td>NT-19</td>
</tr>
<tr>
<td>$\text{lcm}(a, b)$</td>
<td>least common multiple</td>
<td>NT-16</td>
</tr>
<tr>
<td>$x \mod d$</td>
<td>$x$ mod $d$</td>
<td>NT-7</td>
</tr>
<tr>
<td>$\mathbb{N}$</td>
<td>(Natural numbers)</td>
<td>NT-1</td>
</tr>
<tr>
<td>$\mathbb{Q}$</td>
<td>(Rational numbers)</td>
<td>NT-1</td>
</tr>
<tr>
<td>$\mathbb{R}$</td>
<td>(Real numbers)</td>
<td>NT-1</td>
</tr>
<tr>
<td>Sets of numbers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\mathbb{N}$</td>
<td>(Natural numbers)</td>
<td>NT-1</td>
</tr>
<tr>
<td>$\mathbb{N}^+$</td>
<td>(Positive integers)</td>
<td>NT-1</td>
</tr>
<tr>
<td>$\mathbb{N}_2^+$</td>
<td>${n \in \mathbb{Z} \mid n \geq 2}$</td>
<td>NT-1</td>
</tr>
<tr>
<td>$\mathbb{P}$</td>
<td>(Prime numbers)</td>
<td>NT-2</td>
</tr>
<tr>
<td>$\mathbb{Q}$</td>
<td>(Rationals)</td>
<td>NT-1</td>
</tr>
<tr>
<td>$\mathbb{R}$</td>
<td>(Real numbers)</td>
<td>NT-1</td>
</tr>
<tr>
<td>$\mathbb{Z}$</td>
<td>(Integers)</td>
<td>NT-1</td>
</tr>
<tr>
<td>$d\mathbb{Z} + k$</td>
<td>(residue class)</td>
<td>NT-6</td>
</tr>
<tr>
<td>$\mathbb{Z}$</td>
<td>(Integers)</td>
<td>NT-1</td>
</tr>
</tbody>
</table>
Subject Index

Algebraic number theory NT-3
Algorithm
  Euclidean NT-18
Arithmetic
  modular NT-6

Ceiling function (= least integer) NT-9
Ciphertext NT-13
Composite number NT-2
Countable set NT-5
Cryptography NT-13
  Diffie-Hellman protocol NT-22
  PGP NT-20
  public key NT-21
  RSA protocol NT-23
  symmetric encryption NT-20
  trapdoor function NT-21

Diagonal argument NT-6
Diffie-Hellman protocol NT-22
Discrete logarithm NT-21
  Diffie-Hellman and NT-22
Divisible by: \( k \mid n \) NT-2

Espionage NT-15
Euclidean algorithm NT-18
Euler \( \phi \) function NT-19
  RSA protocol and NT-23
Even integer NT-1

Factoring
  RSA and NT-23
  uniqueness of NT-3
Fermat’s Last Theorem NT-3

Floor function (= greatest integer) NT-9
Function
  ceiling (= least integer: \([x]\)) NT-9
  Euler \( \phi \) NT-19
  Euler \( \phi \) and RSA protocol NT-23
  floor (= greatest integer: \([x]\)) NT-9
  greatest common divisor
    (= gcd) NT-16
  greatest integer NT-9
  least common multiple
    (= lcm) NT-16
  least integer NT-9
  one-way (= trapdoor) NT-21
  trapdoor NT-21

Greatest common divisor
  (= gcd) NT-16
  Euclidean algorithm NT-18
  Greatest integer function NT-9

Irrationality of square root NT-4

Key (cryptography) NT-13
  Diffie-Hellman NT-22
  RSA and public NT-23
  trapdoor function and NT-21

Least common multiple
  (= lcm) NT-16
Least integer function NT-9
Logarithm
  discrete and Diffie-Hellman NT-22
Index

Mod as binary operator NT-7
Mod as equivalence relation NT-7
Modular arithmetic NT-6

Number
composite NT-2
integer $\mathbb{Z}$ NT-1
irrational: $\mathbb{R} - \mathbb{Q}$ NT-1
natural $\mathbb{N}$ NT-1
prime: $\mathbb{P}$ NT-2
rational: $\mathbb{Q}$ NT-1
real: $\mathbb{R}$ NT-1
square root is irrational NT-4
unique prime factorization NT-3

Number theory
algebraic NT-3
nonunique factorization NT-3

Odd integer NT-1
One-way (= trapdoor) function NT-21

Perfect square NT-4
PGP (= Pretty Good Privacy) NT-20
Plaintext NT-13
Prime factorization NT-3
uniqueness of NT-3
Prime number NT-2
infinitely many NT-4
unique factorization into NT-3
Public key cryptography NT-21
PGP NT-20
RSA protocol NT-23

Residue class (modular arithmetic) NT-6
RSA protocol NT-23

Set
   countable NT-5
Symmetric encryption NT-20

Theorem
   Unique Factorization NT-3
Trapdoor function NT-21
discrete logarithm NT-22

Unique prime factorization NT-3

Index-4