

1. Prove or refute for  $j, n \in \mathbb{N}_0$  with  $j \leq n$ ,

$$\sum_{i=j}^n \binom{i}{j} = \binom{n+1}{j+1}.$$

2. Prove or refute for  $n, x \in \mathbb{N}, k \in \mathbb{N}_0, x \bmod n = 1 \Rightarrow x^k \bmod n = 1$ .
3. Prove or refute for  $n \in \mathbb{N}, x, y \in \mathbb{N}_0, (x \times y) \bmod n = ((x \bmod n) \times (y \bmod n)) \bmod n$ .
4. Prove or refute for  $n, y \in \mathbb{N}, x \in \mathbb{N}_0, (x/y) \bmod n = ((x \bmod n)/(y \bmod n)) \bmod n$ .
5. Prove or refute, for  $n \in \mathbb{N}, i, j \in \mathbb{N}_0$ , and  $m \in \{0, 1, 2, \dots, n-1\}$ , then

$$m^{i+j} \bmod n = ((m^i \bmod n) \cdot (m^j \bmod n)) \bmod n$$

6. Prove, for  $x \in \mathbb{R}$ , the *indispensable* formula

$$\sum_{k=0}^n x^k = \begin{cases} n+1, & \text{if } x = 1, \\ \frac{x^{n+1} - 1}{x - 1}, & \text{otherwise.} \end{cases}$$

(Letting  $x = 2$ , the above evaluates to the total number of nodes in a symmetric binary tree of depth  $n$ , among other things.) Then, for the case  $|x| < 1$ , evaluate the limit,

$$\sum_{k=0}^{\infty} x^k = \lim_{n \rightarrow \infty} \sum_{k=0}^n x^k = ?$$

(The above is called a *geometric series*.)

7. Let  $m, n, q$ , and  $r$  denote any four natural numbers that satisfy,  $m = qn + r$ ; hence,  $q = \lfloor m/n \rfloor$  and  $r = m \bmod n$ . Prove that

$$\gcd(m, n) = \gcd(n, r).$$

The above theorem is the basis for Euclid's recursive algorithm, here written in pseudocode:

```
int gcd(int m, int n) {
  if (m < n) {           // swap m and n
    int t ← m;
    m ← n;
    n ← t;}
  int r ← m mod n; // compute the remainder
  if (r ≡ 0) {
    return n;         // Eureka!
  } else {
    return gcd(n, r); // recursion
  }
}
```

8. Apply Euclid's recursive algorithm to find the greatest common divisor of 77639912 and 4504864. Show each step of your computation. (You may use a calculator to perform your divisions.)

9. The Fibonacci numbers  $F_n$  are defined by the recursion relation,

$$F_{n+2} = F_{n+1} + F_n, \text{ for } n \in \mathbb{N}_0,$$

with  $F_0 = 0$  and  $F_1 = 1$ . How many applications (or iterations) of Euclid's algorithm are required to evaluate  $\gcd(F_{k+1}, F_k)$  for an arbitrary  $k \in \mathbb{N}_0$ . What is the ultimate answer? *Extra credit* for answering the above for  $\gcd(F_j, F_k)$ , for arbitrary  $j, k \in \mathbb{N}_0$ .

10. The Towers of Hanoi puzzle is described in among other places on pages II:DT:18–20. Let  $M(n)$  denote the minimum number of moves required to transfer  $n \in \mathbb{N}$  disks from the initial pole to the goal pole for a puzzle with three poles. Show that  $M(n)$  satisfies the recursion relation

$$M(n + 1) = 2M(n) + 1,$$

with  $M(1) = 1$ . Use induction to prove that

$$M(n) = 2^n - 1.$$

How many years are needed to solve the puzzle with  $n = 64$  disks, if one can perform exactly one move per second? Compare this number with scientific estimates of the age of the universe.