

### 1. Gambler's Ruin

Suppose that a gambler starts playing a game with an initial amount of money  $i$ , where  $0 < i \leq N$ . The game is turn based, where at the end of each turn the gambler either wins \$1 with probability  $p$  or loses \$1 with probability  $1 - p$ . The player will continue to play until he or she is broke (i.e. \$0) or makes it to \$N (the maximum winnable amount)

- (a) Denote  $P_i$  as the probability of winning given that the gambler starts with \$i. Clearly,  $P_0 = 0$  and  $P_N = 1$ . Find  $P_i$  in terms of  $P_{i+1}, P_{i-1}$  and  $p$ .
- (b) Find a relationship for  $P_{i+1} - P_i$  in terms of  $P_i, P_{i-1}$  and  $p$ .
- (c) Using the previous part, find  $P_i - P_{i-1}$  in terms of  $P_1$  and  $p$ .
- (d) Find  $P_i$  in terms  $P_1$  and  $p$
- (e) Using the identity  $\sum_{k=0}^n a^k = \frac{1-a^{n+1}}{1-a}$  for  $a \neq 1$ , find a close form solution for the previous part.
- (f) Find  $P_1$  and then  $P_i$  in terms of  $p$  only

### 2. Recursive Calls

Calculate the greatest common divisor (gcd) of the following pairs of numbers using the Euclidean algorithm.

[Hasty refresher: starting with a pair of input values, keep repeating the operation “Replace the larger value with its remainder modulo the smaller value” over and over, until one of the values becomes zero. At that point, the other value is the gcd of the original two inputs (as well as of every pair of values along the way).

In pseudocode:  $\text{gcd}(x, y) \rightarrow \text{if } y = 0 \text{ then return } x \text{ else return } \text{gcd}(y, x \bmod y)$ ].

- 1. 208 and 872
- 2. 1952 and 872
- 3.  $1952 \times n + 872$  and 1952

### 3. (Combining moduli)

Suppose we wish to work modulo  $n = 40$ . Note that  $40 = 5 \times 8$ , with  $\gcd(5, 8) = 1$ . We will show that in many ways working modulo 40 is the same as working modulo 5 and modulo 8, in the sense that instead of writing down  $c \pmod{40}$ , we can just write down  $c \pmod{5}$  and  $c \pmod{8}$ .

1. What is  $8 \pmod{5}$  and  $8 \pmod{8}$ ? Find a number  $a \pmod{40}$  such that  $a \equiv 1 \pmod{5}$  and  $a \equiv 0 \pmod{8}$ .
2. Now find a number  $b \pmod{40}$  such that  $b \equiv 0 \pmod{5}$  and  $b \equiv 1 \pmod{8}$ .
3. Now suppose you wish to find a number  $c \pmod{40}$  such that  $c \equiv 2 \pmod{5}$  and  $c \equiv 5 \pmod{8}$ . Find  $c$  by expressing it in terms of  $a$  and  $b$ .
4. Repeat to find a number  $d \pmod{40}$  such that  $d \equiv 3 \pmod{5}$  and  $d \equiv 4 \pmod{8}$ .
5. Compute  $c \times d \pmod{40}$ . Is it true that  $c \times d \equiv 2 \times 3 \pmod{5}$ , and  $c \times d \equiv 5 \times 4 \pmod{8}$ ?

#### 4. Short Answer: Modular Arithmetic

1. What is the multiplicative inverse of  $3 \pmod{7}$ ?
2. What is the multiplicative inverse of  $n - 1$  modulo  $n$ ? (An expression that may involve  $n$ . Simplicity matters.)
3. What is the solution to the equation  $3x = 6 \pmod{17}$ ? (A number in  $\{0, \dots, 16\}$  or “No solution”.)
4. Let  $R_0 = 0; R_1 = 2; R_n = 4R_{n-1} - 3R_{n-2}$  for  $n \geq 2$ . Is  $R_n = 2 \pmod{3}$  for  $n \geq 1$ ? (True or False)
5. Given that  $\text{extended-gcd}(53, m) = (1, 7, -1)$ , that is  $(7)(53) + (-1)m = 1$ , what is the solution to  $53x + 3 = 10 \pmod{m}$ ? (Answer should be an expression that is interpreted  $\pmod{m}$ , and shouldn't consist of fractions.)