CS 70 Discrete Mathematics and Probability Theory
Summer 2016 Psomas, Dinh an Ye Discussion 7A Sol

1. Gambler's Ruin

Suppose that a gambler starts playing a game with an initial amount of money i, where $0 < i <= N$. 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.

$P_i = pP_{i+1} + (1-p)P_{i-1}$

This corresponds to the case of winning or losing the first round.

(b) Find a relationship for $P_{i+1} - P_i$ in terms of P_i,P_{i-1} and p.

$P_{i+1} - P_i = \frac{1-p}{p}(P_i - P_{i-1})$

Hint: $P_i = (p + (1-p))P_i$

(c) Using the previous part, find $P_i - P_{i-1}$ in terms of P_1 and p.

$P_i - P_{i-1} = \frac{1-p}{p}(P_{i-1} - P_{i-2}) = (\frac{1-p}{p})^2(P_{i-2} - P_{i-3}) \ldots = (\frac{1-p}{p})^{i-1}P_1$ (since $P_0 = 0$)

(d) Find P_i in terms P_1 and p

$P_i = (P_i - P_{i-1}) + (P_{i-1} - P_{i-2}) + \ldots + (P_1 - P_0) = P_1 \sum_{j=0}^{i-1}(\frac{1-p}{p})^j$

(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.

$P_i = P_1 \sum_{j=0}^{i-1}(\frac{1-p}{p})^j = \frac{1-(\frac{1-p}{p})^i}{1-\frac{1-p}{p}}P_1$ if $p \neq 1/2$

$P_i = iP_1$ if $p = 1/2$

(f) Find P_1 and then P_i in terms of p only

$P_N = 1 = \frac{1-(\frac{1-p}{p})^N}{1-\frac{1-p}{p}}P_1$

Therefore,

$P_1 = \frac{1-\frac{1-p}{p}}{1-(\frac{1-p}{p})^N}$ if $p \neq 1/2$

$P_1 = \frac{1}{N}$ if $p = 1/2$

Finally,

$P_i = \frac{1-(\frac{1-p}{p})^i}{1-\frac{1-p}{p}}P_1 = \frac{1-(\frac{1-p}{p})^i}{1-\frac{1-p}{p}}\frac{1-\frac{1-p}{p}}{1-(\frac{1-p}{p})^N} = \frac{1-(\frac{1-p}{p})^i}{1-(\frac{1-p}{p})^N}$

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: $\gcd(x,y) \rightarrow$ if $y = 0$ then return x else return $\gcd(y, x \mod y)$].

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

This is supposed to be a quick refresher for the gcd algorithm, and attempts to show how gcd creates recursive calls of other gcd that we can use to shortcut. Answer: 8 for all of these. The first answer students should calculate by hand, the second answer will reduce to the first after one step, and the third answer will reduce to the second in one step.

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 $a \equiv 0 \pmod 8$.

   $8 \equiv 3 (\text{mod } 5)$ and $8 \equiv 0 (\text{mod } 8)$. We can find such a number by considering multiples of 8, i.e. 0, 8, 16, 24, 32, and find that if $a = 16$, $16 \equiv 1 (\text{mod } 5)$. Therefore 16 satisfies both conditions.

2. Now find a number $b \pmod{40}$ such that $b \equiv 0 \pmod 5$ and $b \equiv 1 \pmod 8$.

   We can find such a number by considering multiples of 5,i.e.0,5,10,15,20,25,30,35, and find that if $b = 25$, $25 \equiv 1 (\text{mod } 8)$, so it satisfies both conditions.

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.

   We claim $c \equiv 2a + 5b \equiv 37 (\text{mod } 40)$. To see that $c \equiv 2 (\text{mod } 5)$, we note that $b \equiv 0 (\text{mod } 5)$ and $a \equiv 1 (\text{mod } 5)$. So $c \equiv 2a \equiv 2 (\text{mod } 5)$. Similarly $c \equiv 5b \equiv 5 (\text{mod } 8)$.

4. Repeat to find a number $d \pmod{40}$ such that $d \equiv 3 \pmod 5$ and $d \equiv 4 \pmod 8$.

   We can repeat the same procedure as above, and find that $d = 3a + 4b \equiv 28 (\text{mod } 40)$.

5. Compute $c \times d \pmod{40}$. Is it true that $c \times d \equiv 2 \times 3 \pmod 5$, and $c \times d \equiv 5 \times 4 \pmod 8$?

   $c \times d = 37 \times 28 \equiv 36 \text{ (mod } 40)$. Note that if $a \equiv b \text{ (mod } n)$ and $c \equiv d \text{ (mod } n)$ then $a \times c \equiv b \times d \text{ (mod } n)$.Therefore we can multiply $c \equiv 2 \text{ (mod } 5)$ and $d \equiv 3 \text{ (mod } 5)$ to get $c \times d \equiv 2 \times 3 \text{ (mod } 5)$. Similarly we can multiply these equations (mod 8) and get $c \times d = 5 \times 4 \text{ (mod } 8)$.

4. Short Answer: Modular Arithmetic

1. What is the multiplicative inverse of $3 \pmod 7$?
   $5 \pmod 7$.
   $(3)(5) = 15 = 1 \pmod 7$

2. What is the multiplicative inverse of $n-1$ modulo n? (An expression that may involve n. Simplicity matters.)

   $n-1 \pmod{n}$.
   Its $-1 \pmod{n}$! Or $(n-1)(n-1) = n^2 - 2n + 1 = 1 \pmod{n}$.

3. What is the solution to the equation $3x = 6 \pmod{17}$? (A number in $\{0,\ldots,16\}$ or "No solution".)

   2.
   Muliply both sides by 6 the multiplicative inverse of 3 and reduce.

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)

   True.
   Take the recursive formula modulo 3. This is a warmup question for the next problem.

5. Given that $extended - gcd(53,m) = (1,7,-1)$, 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 consists of fractions.)

   $x = 49 \pmod{m}$
   Follows from 7 being multiplicative inverse of $53 \pmod{m}$.