ArsDigita University
Month 2: Discrete Mathematics - Professor Shai Simonson

Problem Set 7 – Generating functions, Number Theory, Cryptography

1. Compute by hand, the smallest positive integers x, y, u, v such that $ax-by = bu-av = \gcd(a,b)$ for each pair a, b below. Use the Euclidean algorithm and back tracking. Turn in your answers only for a and d.

   a. 99, 101
   b. 10, 35
   c. 7, 12
   d. 36, 42

2. Write a recursive Scheme function to do the computation above and show the answer for the pair of numbers 233987973 and 41111687.

3. In each of the following expressions, what is the coefficient in front of the term whose exponent is 4?

   a. $(1+x+x^2+x^3+x^4)^3$
   b. $(1+x^2+x^4)^2(1+x+x^2)^2$
   c. $(1+x+x^2+x^3+x^4+\ldots)^3$

4. Find a generating function that will help determine the number of 5-combinations of the letters H, E, L, P in which L and P appear at most once, but H and E can appear multiple times.

5. What is the coefficient in front of x^n in the polynomial expansion of $1/(1-10x+21x^2)$?

6. Prime Numbers

   a. How many distinct divisors are there for p^a, where p is a prime?
   b. How many distinct divisors are there for an arbitrary number m? Hint: Factor m into its prime factors so that $m = p_1^{a1}p_2^{a2}\ldots p_n^{an}$.

7. What is the generating function for c_k, the number of ways to make change for k cents using pennies, nickels, dimes and quarters?

8. Use the function in the previous problem to help solve the following counting problems:

   a. How many ways are there to make change for \$1 using pennies, nickels, dimes and quarters, but no more than ten pennies?
   b. Same question but at least one of each coin must be used.

9. RSA encryption. Let $p=13$ and $q=11$.

    a. Calculate an appropriate public code, and private code for doing RSA encrypting.
    b. Assuming that each character in a message is represented by its ASCII value (an assigned table of integers from 0 to 127, can be found in many texts), encode the message "Too much work!".

10. Cracking the UFO Message.

    A public code is found etched on a rock on Mars: (7, 1147). The message {128, 1040, 129, 1144, 788, 735, 570, 875} is received from outer space on one of the billion machines running the Extraterrestrial Life Detector Screen Saver distributed among the world's PC's. Assuming that this message was encrypted with the public code found on Mars, crack the code and decode the numbers.

11. Let R be the set of all pairs (a, b) where a and b are mathematicians that have been co-authors on a paper.

    a. Prove whether or not R is an equivalence relation.
    b. Describe the meaning of $R \circ R$.
    c. Describe the transitive closure of R. Prove that this is an equivalence relation.
    d. Give an example that shows that R does not necessarily *partition* a set of mathematicians.
    e. Let x be the mathematician Paul Erdos, and E be the subset $\{(a,b)\}$ of R, where $a=x$. The *Erdos number* of a mathematician w, is the smallest n, for which (x,w) is contained in E^n. Use the web to find the Erdos number of Shai Simonson, Kenneth H. Rosen, Philip Greenspun, Ron Graham, Donald Knuth, and Tara Holm.

12. **Optional:** The *Boolean product* of two binary matrices is defined analogous to matrix multiplication except with addition replaced by OR, and multiplication replaced by AND.

    a. Consider a directed graph $G=(V,E)$ where E is the relation consisting of its set of edges. Is E an equivalence relation on V? Prove or give a counterexample.
    b. Let A be the binary adjacency matrix representation of G. Prove by induction that E^n equals the Boolean product of A with itself n times.
    c. What is the meaning of the ij^{th} entry in the product of A with itself n times?
    d. Contrast this with the meaning of the ij^{th} entry in the regular matrix product of A with itself n times.