COSC 6111 Advanced Design and Analysis of Algorithms
Jeff Edmonds
Assignment: Algebra

First Person:
Family Name:
Given Name:
Student #:
Email:

Second Person:
Family Name:
Given Name:
Student #:
Email:

Problem Name	If Done Old Mark	Check if to be Marked	New Mark
1 Field Proofs			
2 Linear Transformations			
3 Integrating			
4 Generating Functions			
5 Prime Factors			

1. Considering any *Field*, i.e. set of objects and arbitrary operations + and $\times$ meeting all the requirements.

   (a) The rule $\forall a, a \times 0 = 0$ is included in the list of rules in brackets, because it can be proved from the other rules. Provide such a proof.

   (b) The values a and b are called *zero divisor* iff neither are zero and their product is zero. Prove that such objects don't exist in a field.

2. Linear Transformations: We want to better understand a linear transformation from the $\langle u, v\rangle$ plane to the $\langle x, y\rangle$ plane.

   (a) Find the 2×2 matrix T that maps the vector $\langle u, v\rangle = \langle 1, 0\rangle$ to $\langle x, y\rangle = \langle 3, 1\rangle$ and $\langle u, v\rangle = \langle 0, 1\rangle$ to $\langle x, y\rangle = \langle 1, 1\rangle$.

   (b) Invert the matrix T giving that T^{-1} maps points $\langle x, y\rangle$ to points $\langle u, v\rangle$. Do not use a program to invert it. In fact, don't even look up how to invert a matrix. Try to remember and/or figure it out on your own. Show your work. Be sure to give me a loop invariant for your algorithm.

   (c) Map the following objects from the $\langle u, v\rangle$ plane giving the equations for and a plotting of the corresponding objects in the $\langle x, y\rangle$ plane.

      i. the unit square, i.e. the equations $u = 1$ and $v = 1$. (Plot but don't derive for $u = -1$ and $v = -1$).

      ii. the unit circle, i.e. $u^2 + v^2 = 1$.

      iii. the axis, i.e. the equations $u = 0$ and $v = 0$ (plot but don't derive).

      The square gets transformed to a parallelogram not a rectangle because the two vectors being mapped to are not perpendicular. Curious, does the circle get mapped to a skewed more parallelogram shape or does it manage somehow to keep a more symmetrical ellipse shape?

   (d) Note in two ways where the point $\langle u, v\rangle = \langle 1, 1\rangle$ gets mapped to. In the first way, apply the matrix T to it. In the second way, look at the arrow vector of where it is mapped as the sum of other arrow vectors.

   (e) Now give the equation for this eclipse when it is translated so its center is moved from $\langle 0, 0\rangle$ to $\langle a, b\rangle$. No need to simplify it.

3. What is the linear algebra basis of functions needed for differentiating $f(x) = x^3e^{2x}$? Give the matrix for differentiating. Don't bother inverting it.

4. Generating Functions

   (a) Use generating functions to count the number $p(n)$ of lists of integers at least one that add up to the value n. For example, $p(5) = 16$ because

      - 5
      - $4 + 1$ and $1 + 4$
      - $3 + 2$ and $2 + 3$
      - $3 + 1 + 1$, $1 + 3 + 1$, and $1 + 1 + 3$
      - $1 + 2 + 2$, $2 + 1 + 2$, and $2 + 2 + 1$
      - $2 + 1 + 1 + 1$, $1 + 2 + 1 + 1$, $1 + 1 + 2 + 1$, and $1 + 1 + 1 + 2$
      - $1 + 1 + 1 + 1 + 1$

      As in the slides, $P(0) = 1$ because there is the one empty list that adds to zero.

      Hint: Let T be the infinite set of all lists of integers at least one. For each such list, $L \in T$, let $n(L)$ be the sum of the integers in the list. Let I be the set of integers at least one. What is

$P_I = \sum_{L\in I} x^{n(L)}$? What is $P_T = \sum_{L\in T} x^{n(L)}$ in terms of P_T and P_I? Solve this relation giving an equation for P_T. What is its Taylor expansion? Compare these coefficients with your hand computed values for $P(0), \ldots, P(5)$.

Use

```
maple
  solve(p^2*x + 1 = p,p);
  op(2,[solve(p^2*x + 1 = p,p)]);
  taylor(op(2,[solve(p^2*x + 1 = p,p)]),x=0,6);
http://www.wolframalpha.com
  p^2*x + 1 = p solve for p
  taylor (1-sqrt(1-4x))/2x
  Hit "More Terms"
```

(b) Redo the last question, but include zero in the possible integers, i.e. use generating functions to count the number $p(n)$ of lists of integers at least zero that add up to the value n. What for example should $p(0)$ be? How is this expressed in the generating function?

5. The number of prime numbers in the range $[1..N]$ is very close to $\frac{N}{\ln N}$. Of the 2^n numbers that have n-bits, the number of them that are prime is $\frac{2^n}{\ln 2^n} = \frac{c2^n}{n}$, where $c = \frac{1}{\ln 2} = 1.44$. The density of the primes is such that if N is "randomly" chosen then the probability that it is prime is very close to $\frac{1}{\ln N}$. It turns out that these primes are distributed fairly randomly. In understanding this distribution, it is sometimes useful to assume that each value N is independently chosen to be "prime" with probability $\frac{1}{\ln N}$.

   (a) Consider numbers of the form p^2, where p is prime. If p^2 is an n-bit number, how many bits are in p? How many n-bit numbers are of the form p^2? What is the probability that a "random" N is of the form p^2? How does this compare with the probability that N is prime? How about of the form p^r for some constant r?

   (b) Let $r \in [0, n]$ be some fixed value. How many n-bit numbers are of the form $p \cdot q$, where p is an r-bit prime and q is an $(n-r)$-bit prime? What is the probability that a "random" N has this form $p \cdot q$ with both prime? How does this probability depend on r? For which values of r is this probability maximized and minimized? How does this compare with the probability that N is prime?

   (c) Let $\omega(N)$ denote the number of prime factors of N and let $\omega'(N)$ denote the number of distinct ones. The prime factorization of 12 is $2 \cdot 2 \cdot 3$, giving $\omega(12) = 3$ and $\omega'(12) = 2$. It is fun that both the expected number of prime factors $\omega = \mathrm{Exp}(\omega(N))$ and the expected number of distinct prime factors $\omega' = \mathrm{Exp}(\omega'(N))$ of a "random" N are both with one or two of $\ln\ln N$.

      i. Choose N randomly. Let I_i be the 0/1 indicator variable that is one iff i is prime and divides evenly into N. What is the number $\omega'(N)$ of distinct prime factors of N as a function of the I_i? How about ω'?

      ii. For a random i, what is $\Pr(i \text{ is prime})$? What is $\Pr(i \text{ is a factor of } N)$? Assuming that these two events are independent, what is $\mathrm{Exp}(I_i)$.

      iii. Show that $\omega' = \mathrm{Exp}(\omega'(N)) \approx \ln\ln N$. Convert the sum to an integral and differentiate $\ln\ln N$ to prove the integral.

      iv. Let p be a prime number. Let $I_{\langle p,r\rangle}$ be the 0/1 indicator variable that is one iff p^r divides into a randomly chosen N. Let J_p be the number of times that p divides into N. What is J_p as a function of the $I_{\langle p,r\rangle}$?

      v. What is $\Pr(I_{\langle p,r\rangle} = 1)$? What is $\mathrm{Exp}(J_p)$? Simplify the expression for this last value.

      vi. If $i = p$ is prime then let $J'_i = J_p$ be the number of times that p divides into N, else let $J'_i = 0$. What is $\mathrm{Exp}(J'_i)$?

      vii. Show that the expected number ω of prime factors of N is not more than one more than the expected number ω' of distinct prime factors.