CS 70 Discrete Mathematics for CS Fall 2004 Rao Practice Problems

You should also look at the problem set problems as well!! And read the notes.

1. Prove by induction that $\sum_{i=0}^{n} i = (n+1)n/2$.
2. Use induction to prove that $n^5 - n$ is divisible by 5, whenever n is a nonnegative integer.
3. Rosen. Problem 40.
4. Rosen page 225 question 6.
   (a) State the well-ordering property for the set of positive integers.
   (b) Use this property to show that every positive integer can be written as the product of primes
5. Rosen page 199, problem 22 Prove by induction that 6 divides $n^3 - n$ whenever n is a nonnegative integer.
6. **Euclid's argument**
   Consider the following result, first proved many centuries ago.

   Theorem 1 (Euclid) *There exist infinitely many primes.*

   Proof: Assume to the contrary that there exist finitely many primes. Let these primes (in increasing order) be $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ..., p_k. Let $q_k = p_1 p_2 p_3 \cdots p_k + 1$. Note that q_k is a new number not in the list of primes $p_1, \ldots, p_k$. At the same time, it is not divisible by p_i for any i, since $q_k \equiv p_1 p_2 p_3 \cdots p_k + 1 \equiv 1 \pmod{p_i}$, which would mean that q_k is a new prime different from $p_1, \ldots, p_k$, which is a contradiction. This completes the proof. □

   Let $p_1, \ldots, p_k$ represent the first k primes. Are we guaranteed that $p_1 p_2 p_3 \cdots p_k + 1$ is always prime for all $k \geq 1$? Is the above proof valid? Explain.
7. **Stable marriage**
   (a) Consider the following situation. After we find the pairing using the boy-optimal algorithm we described in class, one of the boys b, who gets paired up with some girl g, changes his mind. I.e., he changes his preference by moving g higher up in his list.
   Is the current pairing stable? Is it still boy-optimal? Prove or disprove these statements.
   (b) Prove or disprove that any boy optimal stable pairing is girl pessimal.
   (c) Prove that the traditional marriage algorithm is boy optimal.
8. **Number theory**
   (a) True or false? You should give some explanations.
      i. 2 has an inverse modulo 6.
      ii. $\gcd(32, 1387) = 1$.

(b) Find an inverse of 3 modulo 17.

(c) Find an inverse of 144 mod 171.

(d) Solve this equation: $9x = 2 \bmod 40$.

(e) (Rosen page 165, problem 11.) Find $\gcd(2n+1, 3n+2)$, where n is a positive integer.

(f) Which integers leave a remainder of 1 when divided by 2, leave a remainder of 2 when divided by 3, and leave a remainder of 3 when divided by 5? (Chinese remainder theorem. HW 4.)

(g) A *least common multiple* of positive integers a and b, denoted by $\text{lcm}(a,b)$, is the smallest positive integer that is divisible by a and b. Prove that $ab = \gcd(a,b)\text{lcm}(a,b)$.

(h) (Rosen page 149,problem 15.) Show that if p is prime, the only solution of $x^2 - 1 = 0 \bmod p$ are integers x such that $x = 1 \bmod p$ or $x = -1 \bmod p$.

(i) What is $a^{(p-1)(q-1)} \bmod pq$ for a relatively prime to p and q and p and q are primes?

(j) Show that $a^x \bmod p = a^{x \bmod (p-1)} \bmod p$. You may use Fermat's Little Theorem.

9. **RSA**

(a) Describe the RSA encryption and decryption scheme. (Assume p and q are prime. Let $n = pq$. Use x as a message, (e,n) as a public key, and (d,n) as a private key.)

(b) Analyze the encryption and decryption times for RSA.

(c) Compare decoding and encoding time. Usually $e = 3$, why?

10. (a) Prove that any degree 1 polynomial over a field F has at most 1 zero. What is the maximum number of points where two distinct degree 1 polynomials can intersect?

(b) If at least d points on a degree $\leq d-1$ polynomial have value 5, what is the polynomial?

(c) Given pairs $(x_1,y_1),(x_2,y_2)$, describe a degree 1 polynomial that hits these points.

11. **Applications of polynomials.**

(a) Describe a method to share a secret with b bits with n people such that each person is given at most $b/k+1$ bits and any k of the people can reconstruct all of the bits, and any $k-1$ people won't know anything about the first b/k bits of the secret. (Use a Galois Field, $GF(p)$ for your field, and state how big p should be.)

(b) Say, you receive $(1,3),(2,4),(3,7)$ and $(4,9)$ for a degree 1 polynomial code. Which point is corrupted? (Hint: drop each and see if the other three are on a line.) If at most 2 points are corrupted in a degree $n-1$ polynomial code, extend this simple algorithm for finding the original message. Extend this algorithm to correct k points. Assuming that finding a degree n polynomial that fits n points takes x time, how long would your algorithm take.

(c) Review the notes on error correction, why is the Welsh-Berlekemp method better than your simple method above when the number of errors k becomes larger.

i. What is the number of possible legal number of messages for degree $n-1$ polynomial code over a field of size f where the message consists of the value of the polynomial on $n+2k$ points?

ii. Consider a noisy channel that can choose k places to change, and change them to any character. How many actions can the channel take?

iii. If you recover the original message, can you figure out exactly what the channel did as well?

iv. How many bits must the received message contain to decode?

12. (a) Show that a Gray code exists for any b-bit strings.

(b) Show that any graph where every node has degree larger than $n/2$ has a Hamiltonian cycle.

(c) For what values of n does the dimension n hypercube (with 2^n nodes) have an Eulerian path.