CS 70 Discrete Mathematics for CS Spring 2000 Papadimitriou/Russell/Sinclair Prac MT2

This is a set of practice problems for Midterm 2. Most of the problems here are somewhat harder than the ones that will appear in the actual midterm (which will also be considerably shorter than this). If you can solve all of these problems, you are in good shape for the midterm.

1. **(15 pts.) Simple modular arithmetic**
   Solve the following system of equations for x, y and z (modulo the indicated modulus), or show that no solution exists:

$$\begin{aligned} 3x + y + z &= 3 \bmod 11 \\ x + \quad z &= 3 \bmod 11 \\ y + 2z &= 3 \bmod 11 \end{aligned}$$

2. **(20 pts.) The inverse of (p-1)!**
   Let $p \geq 2$ be a prime. Prove that

$$(p-1)! = ((p-1)!)^{-1} \bmod p$$

   [Hint: Consider the set of numbers $\{1^{-1}, 2^{-1}, \ldots, (p-1)^{-1}\}$. What can you say about this set?]

3. **(15 pts.) Self-inverses**
   Let $p \geq 2$ be given. We say that a number x is a *self-inverse* (modulo p) if $x^{-1} = x \bmod p$. For example, 1 is a self-inverse modulo 5 since $1 \cdot 1 = 1 \bmod 5$. The number 4 is another self-inverse modulo 5 since $4 \cdot 4 = 1 \bmod 5$.

   Show that if p is prime, then 1 and p-1 are the only integers (modulo p) that are self-inverses.

4. **(25 pts.) Fields**
   Recall the axioms for fields, which state that $(F, +, \times, 0, 1)$ is a *field*, if

   - F is closed under + and $\times$ (meaning for all $x, y \in F$, we have $x + y \in F, x \times y \in F$).
   - + and $\times$ are associative and commutative
   - For all $x \in F$, $0 + x = x + 0 = x$
   - For all $x \in F$, $1 \times x = x \times 1 = x$
   - For all $x \in F$, $0 \times x = x \times 0 = 0$
   - $\times$ distributes over +
   - Each $x \in F$ has an additive inverse $(-x) \in F$, such that $x + (-x) = 0$.
   - Each $x \in F$, $x \neq 0$ has a multiplicative inverse $x^{-1} \in F$, such that $x \times x^{-1} = 1$.

(a) We know that Z_p (the set of integers modulo p) with the usual addition and multiplication operations modulo p form a field. What axiom or axioms break down in Z_n (the set of integers modulo n), when $n \geq 2$ is composite? Prove your answer holds for all composite $n \geq 2$.

(b) Prove that in *any* field, it is impossible to have $k \neq 0$, $x \neq 0$, but

$$k \times x = 0$$

[Hint: Assume $k \times x = 0$, and use the field axioms to arrive at a contradiction of some other field axiom.]

(c) Prove that for *any* field, $(x^{-1})^{-1}$ (the inverse of x^{-1}) is just x.

5. (30 pts.) Secret sharing and "error correction"

Suppose that a secret code is needed to launch a missile from a submarine, and any 3 of the top 5 officers of a submarine need to agree in order to recover the secret code. (If an attempt is made to launch the missile with an incorrect code, the missile will permanently deactivate itself, and will not launch even if the correct code is later given.) The secret code is implemented using the secret sharing algorithm using polynomials, discussed in class. Hence, the secret is encoded as $f(0)$ for some appropiate-degreed polynomial f over the field GF_p.

(a) Four of the officers have gotten together and decided to launch a missile. But it was recently learned that one of the officers may be a spy, who might try to mislead the others (for example, by giving an incorrect value of $f(i)$), and nobody knows who the spy might be. Is it still possible to recover the secret code?

(b) If your answer to the previous question was yes, how about if only 3 officers were present (one of whom might be a spy)? If your answer to the previous question was no, how about if all 5 officers were present (one of whom might be a spy)?

(c) If N (rather than 3) officers are needed to launch a missle, and if up to 1/4 of the officers present may be spies, with how many officers present (and revealing their keys) can we guarantee that we can recover the secret?

6. (25 pts.) The field of boolean truth values

Let us consider the field GF_2, with 0 interpreted as the Boolean value F and 1 interpreted as T.

(a) To what logical operations do addition and multiplication mod 2 correspond?

(b) To what logical operation does exponentiation (x^y) correspond?

(c) What algebraic function in GF_2 corresponds to the logical operation of negation?

(d) What algebraic function in GF_2 corresponds to the logical operation of disjunction?

(e) Given an evaluator for algebraic expressions in GF_2, describe an algorithm for testing the validity of any Boolean expression.

7. (15 pts.) Secret sharing among 2 persons

Recall the "xor" secret sharing scheme for sharing a secret bit s (either 0 or 1). In this procedure, Alice is given s xor r where r is a random bit, and Bob is given r. To recover the secret s, Alice and Bob need only xor their bits together; however, neither Alice nor Bob knows anything about s by themselves. This can be rewritten in the following equivalent form:

- Give Alice $a = s + r \bmod 2$
- Give Bob $b = r \bmod 2$
- To recover the secret, Alice and Bob calculate a xor b.

Here is a generalization of this scheme. Suppose we have a secret that is an integer s between 0 and $m-1$, for some large m. Then to share the secret between Alice and Bob:

- Give Alice $a = s + r \bmod m$
- Give Bob $b = r \bmod m$

where r is an integer chosen randomly from $\{0, 1, \ldots, m-1\}$.

(a) How can Alice and Bob cooperate to recover the secret?

(b) Show that this system is secure—that, by themselves, neither Alice nor Bob has any information about s.

8. (15 pts.) The importance of key sizes

We have seen in class that when using RSA, it is important to choose large primes p and q—that is, to have large keys. Otherwise, it would be too easy for an adversary to factor $n = pq$, and hence crack the encryption.

Now consider the polynomials secret sharing scheme discussed in class, that works over the field GF_p. For this scheme, is it also true that it is important for security to choose large p? I.e., is it true that if p is too small, then it would be possible for someone to crack this security method (meaning recover information about the secret even without the required number of secret sharers cooperating)? Why or why not?

9. (30 pts.) Dividing polynomials

Let f and g be two non-zero polynomials over the field GF_p. We say f divides g, or $f|g$, if there exists some other polynomial q such that $g(x) = f(x)q(x)$. For example, $x-1$ divides $x^2 + x - 2$, since $x^2 + x - 2 = (x-1)(x+2)$. Given a pair of polynomials f and g such that $f|g$, this problem considers an algorithm for finding the quotient $q = g/f$.

(a) Suppose g is degree n, and f is degree m ($m \leq n < p$). What is the degree of q?

(b) Let k be the number of different values of x at which need to know $q(x)$ in order to exactly recover q via Lagrange interpolation. Based on your answer to (a), what is k?

(c) A general algorithm for finding $q = g/f$ is as follows.

i. Evaluate $f(0), f(1), f(2), \ldots$ until we find k points at which f is non-zero

ii. Evaluate g at the same points, and calculate the quotients $g(i)/f(i)$ at these points.

iii. We must have $q(i) = g(i)/f(i)$ at these points i. Hence, Lagrange interpolation can be used to recover q from these points.

Apply the above algorithm to find $q = g/f$, where $g = (4x^4 + 5x^3 + 5x^2 + 6x + 3)$, $f = (2x^3 + 5x^2 + 3)$, and both are polynomials defined over GF_7.

(d) Determine a set of conditions that will ensure that f has at least k non-zero points (so that step (i) of this algorithm is guaranteed to work).

(e) Is the quotient unique when it exists? (I.e. is it possible for there to be two different polynomials, q and q', such that $g(x) = f(x)q(x) = f(x)q'(x)$?)