**Department of Mathematics**

**University of British Columbia**

**MATH 342 Final Exam**

**April 28, 2014 8:30 AM - 11:00 AM**

Family Name: ______________________ Initials: ______

I.D. Number: ______________ Signature: ______________________

| Problem | **Mark** | **Out of** |
|---|---|---|
| 1 | | 10 |
| 2 | | 10 |
| 3 | | 10 |
| 4 | | 10 |
| 5 | | 10 |
| 6 | | 10 |
| 7 | | 10 |
| 8 | | 10 |
| Total | | 80 |

CALCULATORS, NOTES OR BOOKS ARE NOT PERMITTED.

THERE ARE 8 PROBLEMS ON THIS EXAM.

**JUSTIFY YOUR ANSWERS.**

1.

Find the following principal remainders, (the principal remainder of $a$ mod $q$ is the unique element $b \in \{0, 1, \ldots, q-1\}$ s.t. $a = b$ mod $q$).

(a) $10^{3849197491}$ mod 11

(b) $(60)^{11}$ mod 11

(c) $(1100005)(223347)$ mod 11

2.

Let $C$ be the linear code over $F_5$ spanned by $\{01234, 13024, 12340\}$.

(a) Find bases for $C$ and $C^{\perp}$.

(b) Find the length, dimension, and minimum distance of $C$ and $C^{\perp}$.

(c) Find the number of cosets of $C$ and $C^{\perp}$.

(d) For each coset of $C^{\perp}$ with coset leader of weight at least 2, find a coset leader.

3.

Let $A$ be an $m \times n$ matrix with entries 0 and 1. We say that $A$ is *even* if the number of 1's in each row is even and the number of 1's in each column is even.

Let $A$ and $B$ be distinct even $m \times n$ matrices. Show that $A$ and $B$ must differ in at least four entries.

Note: the integer 0 is even.

4.

Which of the following polynomials is (are) irreducible over $F_2$?

(a) $f(x) = x^5 + x^2 + 1$

(b) $g(x) = x^5 + x + 1$

5.

Recall the definition of characteristic of a finite field $F$: the smallest positive integer $q$ such that $q \cdot 1 = 0$ (recall that for an element $a \in F$, $q \cdot a$ denotes the sum of $q$ copies of $a$).

(a) Show that if $F$ is a finite field with characteristic $q$, then for all nonzero elements $a \in F$, $q$ is the smallest positive integer such that $q \cdot a = 0$

(b) For any prime $p$ and positive integer $n$, what is the characteristic of $F_{p^n}$?

6.

Let $a$ be a primitive element of $F_{27}$.

(a) Find all positive integers $n$ such that $a^n = a^3$.

(b) Find all powers of $a$ that are primitive.

7.

In this problem, note the "round brackets" $(n, M, d)$ (*not* square brackets $[n, k, d]$).

(a) i. Find a (3,4,2) binary code.
  ii. Find a (5,4,3) binary code.
  iii. Use parts i and ii to find a (8,4,5) binary code.

(b) Show that $A_2(8, 5) = 4$.

8.

Let $C$ be a binary code of length $n$ with at least two codewords. Let $t$ be a positive integer such that the Hamming balls of radius $t$, centered at the codewords, are pairwise disjoint and completely cover $F_2^n$. Show that $d(C) = 2t + 1$.