Carleton College CS 202, Fall 2008, Exam 1

You have 70 minutes.

You may not use any notes or calculator.

Except on the TRUE/FALSE/PUNT questions, always show your work and explain all of your answers. Good work often earns partial credit. A correct answer with no explanation often earns little or no credit.

If you have no idea how to solve a problem, or if you have forgotten a key formula that you think you need to know, then you may ask me for a hint. The hint will cost you some points (to be decided by me as I grade your paper), but will probably help you earn more points overall.

Good luck.

1. One day while walking around the St. Olaf College campus you come to a branch in your path, where you must turn left or right. One direction leads to Rolvaag Library (where you want to go) and the other to the High-Voltage Pain Complex (which you'd rather avoid). A student offers to help. From reading Wikipedia you know that there are two kinds of St. Olaf students: those who always tell the truth, and those who always lie. Given that fact, what single "yes or no" question can you ask the student, to determine immediately which direction leads to the library? Explain.

2. Prove that every odd integer is the difference of two squares.

3. Each part of this problem is a true/false question, but there are three valid answers: TRUE, FALSE, and PUNT. If you answer PUNT, then you receive half credit. Otherwise, if you answer correctly then you receive full credit, and if you answer incorrectly then you receive no credit. No explanation is necessary on this problem. Do not just write T, F, or P; write the entire word, clearly. Parts A-D are about the integers; parts E-H are about logic.

A. $\forall a\ \forall b\ \forall c\ \forall m\ (ac \equiv bc\ (\text{mod } m) \rightarrow a \equiv b\ (\text{mod } m))$

B. $\forall a\ \forall b\ \forall c\ \forall m\ (a \equiv b\ (\text{mod } m) \rightarrow ac \equiv bc\ (\text{mod } m))$

C. $\forall a\ \forall b\ \forall c\ (a|bc \rightarrow (a|b \vee a|c))$.

D. $\forall a\ \forall m\ \exists b\ ab \equiv \gcd(a, m)\ (\text{mod } m)$.

E. The truth table for the compound proposition $(p \rightarrow q) \vee (r \rightarrow \neg q)$ has exactly 6 true rows.

F. $\forall x\ \forall y\ p(x, y)$ is logically equivalent to $\forall y\ \forall x\ p(x, y)$ for all predicates $p(x, y)$ and all domains.

G. $\neg\forall x\ (p(x) \wedge q(x))$ is logically equivalent to $\exists x\ (\neg p(x) \wedge \neg q(x))$ for all predicates $p(x)$ and $q(x)$ and all domains.

H. Let p be the statement "Elvis is 6 years old" and q the statement "Elvis enjoys Disney World." Then the statement "Elvis enjoys Disney World only if Elvis is 6 years old" is $p \rightarrow q$.

4. Compute the inverse of 27 modulo 140. That is, find an integer y such that $0 \leq y < 140$ and $27y \bmod 140 = 1$.

5. This is a 3-part question about RSA. If you can't answer one part, then go on to the next.
A. Let p and q be distinct primes. Prove that $\phi(pq) = (p-1)(q-1)$.

B. Suppose that you've discovered a fast algorithm for computing $\phi(k)$ for any positive integer k. Explain how you could use this to read anyone's RSA-encrypted messages.

C. Suppose instead that you've discovered a fast algorithm for factoring integers. Explain how you could use this to read RSA-encrypted messages.

6. The (n, k) Hamming code encodes k bits into n bits by adding $n - k$ extra bits for error correction. Our example from class used $n = 7$ and $k = 4$ — that is, 3 extra bits. For your reference, the matrices we used are given below. Now, I'm interested in the "next largest" Hamming code — one that uses 4 extra bits to handle errors, instead of 3.

$$E = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}, \quad D = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

A. How big can k and n be, if 4 error-correction bits are used? Explain, of course.

B. Write down D, C, and E matrices for this "next largest" Hamming code. (Note: E is not worth many points, so omit E if you don't have time.)