Final review problems

(Try solving them before coming to the review session, Sun, 05/13, 5-8pm, 306 Soda)

1. The famous (and thus far unproven) Twin Prime Conjecture states that, among set of positive integers $\mathbb{N}$, there are infinitely many numbers a such that both a and $a+2$ is prime. Let $P(n)$ be the proposition that integer n is prime.
   (a) Write out a statement of this conjecture in first-order logic, using this proposition and basic arithmetic comparisons/operations ($+$, $=$, $>$, etc).
   (b) Negate the above formula, "simplify" it using deMorgan's laws (that is, move the negation inside all of the quantifiers).

2. Prove that, for every odd positive integer n, the sum $1 + 3 + 5 + \ldots + n$ of the odd numbers up to n is a perfect square.

3. Prove that, given any positive integer n that is not divisible by 2 or 5, at least one of the numbers $1, 11, 111, \ldots, \underbrace{111\ldots111}_{n \text{ ones}}$ is divisible by n. Hint: use the pigeonhole principle; note that, e.g. $11111 - 11 = 11100 = 111 \cdot 100$.

4. Solve:

$$\begin{cases} 7a + 20b = 3 \\ 12a + 30b = 1 \end{cases} \pmod{37}$$

5. **Secret breach** (Due to Ofer Sadgat)
   Consider the following 2-out-of-3 secret sharing scheme. We have a secret s in $\{0, \ldots, 11\}$, so we pick at random an a from $\{0, \ldots, 11\}$, and define the line $f(x) = ax + s \bmod 12$. The three players get $f(1) = a + s$, $f(2) = 2a + s$, and $f(3) = 3a + s$.

   The second player receives the share 3, and now knows that the secret is an odd number. What went wrong?

6. **Fake lines**
   Let's call a polynomial $f(x)$ of degree d ($d \geq 3$) over $\mathbb{Z}_p$ a "fake line" if at least $d-1$ of the d points $\{(1, f(1)), (2, f(2)), \ldots, (d, f(d))\}$ lie on a line.

   How many fake lines of degree 8 over $\mathbb{Z}_{19}$ are there?

7. **Petersen graph**
   Does the Petersen graph (see, e.g., the top left diagram at `http://mathworld.wolfram.com/PetersenGraph.html`) have a Hamiltonian cycle? How about an Eulerian tour?

8. **Paths**
   (a) Prove that, given a connected graph G, the shortest path between vertices u and v is always a simple path (that is, the path visits no vertex twice).
   (b) Given a specific graph G, is the set of paths finite, countably infinite, or uncountable?
   (c) Given a specific graph G, is the set of simple paths finite, countably infinite, or uncountable?

9. **n-dimensional chess**
   Martian n-dimensional chess is played on an n-dimensional hypercube, with pieces placed at the nodes. Vaguely similarly to earthling chess, a rook placed at a certain node v can attack any other node that's connected by v by an edge. Prove that, for $n \geq 5$, there is no way to place n rooks on the n-dimensional hypercube so that all nodes are either occupied by a rook or can be attacked by one.

10. How many solutions are there to $x_1 + x_2 + x_3 + x_4 + x_5 = 306$ if all the variables must be positive integers? Hint: Think of $x_1 = a$ as referring to, say, a "bag" of a marbles.

11. What is the probability that a five-card poker hand (from the standard deck with 4 suits and 13 kinds of card in each suit) contains cards of five different kinds, but is neither a flush nor a straight? A flush is 5 cards of the same suit. A straight is 5 cards that can be arranged so that their kinds are consecutive (2,3,4,5,6 or 9,10,J,Q,K, but *not* Q,K,A,2,3).

12. **Elbonian family planning**
    In Elbonia, 80% of parents who have a son as a first child go on to have a second child, but only 50% of parents who have a daughter as a first child go on to have a second child. Your Elbonian penpal writes you that she is a second child. What is the probability that her older sibling is a sister? Assume that each child is equally likely to be a boy or a girl.

13. **Bonferroni's Inequality**
    Prove that, for any events E and F, $\Pr[E \cap F] \geq \Pr[E] + \Pr[F] - 1$.

14. **Calvinball**
    In a particular round of Calvinball, it is declared that the object of the game is to hit Hobbes in the back of his head with a Nerf gun, and that the game must proceed in rounds of 10 shots until at least 8 out of 10 shots hit their target. Given that Calvin hits the target with probability 20%, what's the probability that he will win the game on the third round?

15. **Tresette**
    Italian card games are played with a deck that contains 40 cards; there are 4 suits, and each suit has cards numbered 1 to 10. The game Tresette is played by four players, that get 10 cards each (randomly shuffled).

    The 3s are the most desirable cards. If you are served three or four 3s, you gain extra points at the end of the game. What is the probability of being served three or four 3s?

16. Springfield has $1,000,000$ people who commute to work and who have a choice between driving or taking the bus. On any given day, there is a probability 20% that it rains and 80% that there is good weather. When it rains, each person, independently, decides to take the bus with probability 30%, or drive with probability 70%. On a sunny day, each person independently decides to drive with probability 50% and to take the bus with probability 50% the bus.

    (a) Let X_i be the indicator random variable that is 1 if person i takes the bus and 0 otherwise. Are X_i and X_j independent?

    (b) What is the expectation and the standard deviation of the number of people who take public transportation? Remember that, in general, $\mathrm{Var}[\sum_{i=1}^n X_i] = \sum_{i=1}^n \mathrm{Var}[X_i] + 2\sum_{i<j} \mathrm{Cov}(X_i, X_j)$, where the covariance of X_i and X_j is defined by $\mathrm{Cov}(X_i, X_j) = \mathrm{E}[X_i X_j] - \mathrm{E}[X_i]\mathrm{E}[X_j]$.

    (c) Suppose it rains. Is the above scenario identical to numbering the residents of Springfield from 1 to $1,000,000$, in an order chosen uniformly at random from the set of all possible numberings, and having those numbered 1 through $300,000$ take the bus, while having the others drive?

17. **Rabbit disaster**

    Once, after building new enclosures for his rabbits, Old McDonald forgets to lock the hatch between the male rabbit enclosure and the female rabbit enclosure. He notices this the following morning, but, rabbits being rabbits, this is far too late. There are currently 30 female rabbits and 30 male ones, and rabbits are known to average 3.5 offspring per litter, with a standard deviation of 0.8. As things stand, it's basically guaranteed that each female will have produced a litter in a month.

(a) Using the normal approximation, what can you say about the largest likely number of rabbits in a month, at the 97.7% confidence level?

(b) Given that the new rabbit enclosure fits at most 200 rabbits, bound the probability that a new enclosure will be needed in a month using, if you can:

   i. the Markov bound

   ii. the Chebyshev bound

   iii. the Chernoff bound

18. **Pushing the envelope: Chebyshev**
What happens if we decide to improve on Chebyshev's bound by using $(X - \mathrm{E}[X])^4$ instead of $(X - \mathrm{E}[X])^2$?

19. **Pushing the envelope: Chernoff**
What happens if we decide to get an even stronger bound than Chernoff by applying Markov to $\Pr[2^{\alpha^X} > 2^{\alpha^{\alpha\mu}}]$? (NB: In all modern mathematical texts, the notation a^{b^c} **always** refers to $a^{(b^c)}$.)

20. **Countability**
Decide whether each of these is finite, countably infinite, or uncountable:

(a) The set of all bit strings $(\{\text{emptystring}, 0, 1, 00, 01, \ldots\})$.

(b) The set of all possible URLs.

(c) The set of all possible GPAs (assuming they're not rounded).

(d) The set of all possible Berkeley transcripts.

(e) The set of all possible ways to order the sand grains at Stinson beach ("this one is grain #1, this one is grain #2, etc.").

(f) The set of all possible ways to assign an integer to all sand grains at Stinson beach.

(g) The set of all possible ways to assign "good" and "bad" to each possible bit string.

(h) The set of all polynomials with integer coefficients.

(i) The set of all distinct polynomials with coefficients modulo 101 (note that this includes only polynomials up to degree 99; though we haven't proven this in CS70, $x^{100} \equiv x^0 \pmod{101}$).