Practice problems 3

1. (a) Is it possible for the propositions $P \vee Q$ and $\neg P \vee \neg Q$ to be both false? Justify your answer.
   (b) Is it possible for the proposition $P \Rightarrow (\neg P \Rightarrow Q)$ to be false? Justify your answer.
   (c) Prove or disprove: $((P \implies Q) \implies R) \implies ((R \implies Q) \implies P)$ is a tautology.

2. Prove by induction: $5x \leq x^2 + 6$ for all $x \in \mathbf{N}$.

3. (a) Let X be uniformly distributed on $\{0, 1, \ldots, 16\}$. What is $\Pr[2X+7 \equiv 0 \pmod{17}]$?
   (b) Let X be uniformly distributed on $\{0, 1, \ldots, 32\}$. What is $\Pr[2X+7 \equiv 0 \pmod{33}]$?
   (c) Let X be uniformly distributed on $\{0, 1, \ldots, 32\}$. What is $\Pr[3X+12 \equiv 0 \pmod{33}]$?
   (d) Let X be uniformly distributed on $\{0, 1, \ldots, 40\}$. What is $\Pr[X^2+40 \equiv 0 \pmod{41}]$?

4. Circle TRUE or FALSE. You do not need to justify your answers on this problem. $\mathbf{N}$ denotes the set of natural numbers, $\{0, 1, 2, \ldots\}$.

   (a) TRUE or FALSE: Let p be prime; then we're guaranteed that $x^{p-1} \equiv 1 \pmod{p}$ for all $x \in \mathbf{N}$.
   (b) TRUE or FALSE: Let $p \in \mathbf{N}$ be such that $x^{p-1} \equiv 1 \pmod{p}$ holds for every $x \in \mathbf{N}$ with $\gcd(x, p) = 1$; then p is guaranteed to be prime.
   (c) TRUE or FALSE: Let S, T be arbitrary sets; then we're guaranteed that $|S \cup T| = |S| + |T|$.
   (d) TRUE or FALSE: Let A, B be events; then we're guaranteed that $\Pr[B \mid A] = \Pr[A \text{ and } B]/\Pr[B]$.

5. (a) What is $70^{2003} \bmod 11$? Simplify your answer to an integer between 0 and 10. (Reminder: *no calculators allowed!* You should be able to do this in your head, in any case.)
   (b) What is $70^{2003} \bmod 77$? Simplify your answer to an integer between 0 and 76.

6. Alice has chosen her modulus for RSA to be $N = 187 = 17 \cdot 11$. She wishes to use an encryption exponent 3. What is her decryption exponent. Now suppose she wishes to sign a contract c. How would she accomplish this?

7. Consider a variant on RSA, where the modulus n is chosen to be a product of just *one* prime (i.e., $n = p$).

   In other words, Bob's public key is (n, e), where n is prime and e is an encryption exponent satisfying $1 < e < n$. Bob's private key is d, the decryption exponent, satisfying $1 < d < n$. To encrypt a message m, Alice computes $c = m^e \bmod n$. To decrypt, Bob computes $c^d \bmod n$.

   (a) To make this work, this variant needs a key generation procedure. How can Bob choose e and d so that the decryption algorithm will correctly recover the message that Alice encrypted?
   (b) This scheme is insecure. Explain why.

8. Let $P(x)$ be an unknown polynomial of degree 6 over the field $GF(q)$. Suppose that you are given the values $P(1), P(2), P(3), P(4), P(5)$. As a function of q, how many possible (combinations of) values are there for:

(a) $P(6)$.
(b) $P(6)$ and $P(7)$.
(c) $P(6)$, $P(7)$ and $P(8)$.

9. $p_1(x)$ is a polynomial of degree 8 and $p_1(x)$ and $p_2(x)$ agree at 17 points. What can you say about the degree of $p_2(x)$?

10. You were given the values of a polynomial $p_1(x)$ of degree 5 at 13 points, but unfortunately you mistyped 4 of them (you don't remember which). Suppose you are able to find a polynomial $p_2(x)$ which agrees with $p_1(x)$ at 9 points. Is $p_2(x)$ necessarily equal to $p_1(x)$? Prove or give a counter-example.

11. Let u and v be vertices of the n-dimensional hypercube, such that the distance between u and v is k.

    (a) How many different paths of length k are there between u and v?
    (b) How many different paths of length $k+1$ are there between u and v?

12. Let A, B be finite sets, with $|A| = m$ and $|B| = n$. How many distinct functions $f : A \to B$ are there from A to B?

13. For each square of a 8×8 checkerboard, flip a fair coin, and color that square black or red according to whether you get heads or tails. Assume that all coin flips are independent.

    A *same-color row* is a row on the board where all squares in the row have the same color (i.e., all red, or all black). Let the random variable X denote the number of same-color rows.

    (a) If all coin tosses come up heads, what is the value of X?
    (b) Calculate $\Pr[X = 0]$. (You do not need to simplify your answer.)
    (c) Calculate $\mathrm{E}[X]$.
    (d) Calculate $\mathrm{Var}[X]$.
    (e) Show that $\Pr[X \geq 3] \leq 1/48$.

14. Let A and B be events with $P(A) = 3/8$, $P(B) = 5/8$ and $P(A \cup B) = 3/4$. Find $P(A|B)$ and $P(B|A)$.

15. Suppose events A, B are independent, and moreover events B, C are independent. Are we guaranteed that events A, C are independent? Why or why not?

16. A lie detector test is known to be 80% reliable when the person is guilty and 95% reliable when the person is innocent. If a person was chosen from a group of suspects of which only 1% have ever committed a crime, and the test indicates that he is guilty, what is the probability that he is innocent?

17. Which of the following sets are uncountable? Which are countable? Why?

    (a) The set of all reals which are larger than 10.
    (b) The intersection of the set of all reals and the set of all integer.
    (c) The set of all odd integers.

18. Someone claims to be able to write programs for the following tasks. Which one cannot be done? Why? Which one can be done? How?

(a) A program that determines if two programs are equivalent.

(b) A program that determines if any given program prints HELLO.

(c) A program that can check if any given program runs within 10 steps and output the number 10.

(d) A program that determines if any given program takes no input and terminates after it outputs some number.

(e) A program that takes two programs and determines that they both run within 10000 steps and output HELLO.

19. Prove that it is undecidable to determine, given a program P, whether when running with no input, P halts and outputs HELLO.