Midterm 1

1. *(10 points)*

   - Is it possible for the propositions $P \vee Q$ and $\neg P \vee \neg Q$ to be both false? Justify your answer.
     Solution. No. If $P \vee Q$ is false, then both P and Q are false, so $\neg P \vee \neg Q$ is true.
   - Is it possible for the proposition $P \Rightarrow (\neg P \Rightarrow Q)$ to be false? Justify your answer.
     Solution. No. $A \Rightarrow B$ is true whenever A is false. So for the proposition to be false P must be true. But then $\neg P \Rightarrow Q$ is also true. Thus the proposition is true.

2. *(10 points)* Suppose you are proving a proposition $P(n)$ by induction on n. You successfully prove the induction step, $\forall n, P(n) \Rightarrow P(n+1)$. But then you notice that $P(2501)$ is false. Can you conclude anything about $P(25)$? Justify your answer.

   Solution. You can conclude that $P(25)$ is false. If $P(25)$ were true, you could use that as the base case of your induction and conclude that $\forall n, \geq 25 P(n)$. But since $P(2501)$ is false, this is a contradiction.

3. *(20 points)* Recall that the Fibonacci numbers $F(n)$ satisfy the recurrence $F(n) = F(n-1) + F(n-2)$, with $F(0) = F(1) = 1$. Prove by induction on n that $F(m+n) = F(m)F(n) + F(m-1)F(n-1)$.

   Solution. As suggested, we will prove the proposition

   $$P(n) : F(m+n) = F(m)F(n) + F(m-1)F(n-1)$$

   by induction on n; the natural number m is fixed, but since we're not going to assume anything about it in the proof, our argument will establish the claim for all m and n.

   - **Base case**: We want to prove $P(1)$, but this just says that

     $$F(m+1) = F(m) + F(m-1),$$

     and this holds by definition.
   - **Inductive Step**: We assume that the statement holds for $1, ..., n$, and we want to prove it for $n+1$:

     $$\begin{aligned} F(m+n+1) &= F(m+n) + F(m+n-1) \\ &= F(m)F(n) + F(m-1)F(n-1) + F(m)F(n-1) + F(m-1)F(n-2) \\ &= F(m)(F(n) + F(n-1)) + F(m-1)(F(n-1) + F(n-2)) \\ &= F(m)F(n+1) + F(m-1)F(n), \end{aligned}$$

     which is what we wanted to show.

4. *(15 points)* Evaluate $100^{50^{25^{10^5}}} \bmod 47$.

   Solution. This problem is being graded as an extra-credit problem. The main idea is that if $N = p \cdot q$ then $a^{(p-1)(q-1)} = 1 \bmod N$. So the exponent $50^{25^{10^5}}$ has to be evaluated $\bmod 46 = 2 \cdot 23$. So the exponent 25^{10^5} has to be evaluated $\bmod 22 = 2 \cdot 11$. So the exponent 10^5 has to be evaluated $\bmod 10$, and is therefore 0. So the exponent in the previous line is 1. So the problem is reduced to evaluating $100^{50} \bmod 47 = 6^4 \bmod 47 = 48 \cdot 27 \bmod 47 = 27 \bmod 47$.

5. (*10 points*) 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?

   Solution. Alice's decryption exponent is $3^{-1} \bmod 16 \cdot 10 = 107$. To sign a message c, Alice just decrypts c by computing $c^{107} \bmod 187$.

6. (*15 points*)

   - Suppose two polynomials $P(x)$ and $Q(x)$ of degree d intersect at k points. i.e. there are k values for x such that $P(x) = Q(x)$. What can you say about k?

     Solution. $P(x) - Q(x)$ is a polynomial of degree at most d and therefore can have at most d roots. Thus $k \leq d$.

   - 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:

     Since $P(x)$ is of degree 6, it is uniquely specified by its values at 7 points. Therefore the answers are as follows:

     – $P(6)$.
       q

     – $P(6)$ and $P(7)$.
       q^2.

     – $P(6)$, $P(7)$ and $P(8)$.
       q^2. Since specifying $P(6)$ and $P(7)$ uniquely determines $P(8)$.