Question 1. [10 pts each] Given the information

$$10^{44460} \equiv 32287 \pmod{44461}$$

$$10^{50850} \equiv 1 \pmod{50851}$$

(a) What can you conlcude about whether 44461 is prime or composite, and why?

44461 must be composite.
If it were prime, then Fermat's theorem would imply $10^{44460} \equiv 1 \pmod{44461}$

(b) What can you conclude about whether 50851 is prime or composite, and why?

No conclusion can be drawn. Fermat's theorem does not exclude the possibility that $a^{n-1} \equiv 1 \pmod{n}$ for some choices of a and composite n.

(In fact, $50851 = 211 \cdot 241$ is composite.)

Question 2. [15 pts] The parliament of an unnamed country has 57 members from the Workers Party and 72 from the Fat Cats Party. How many ways are there to select an 11 member committee, including a chairperson, if the chairperson must be a member of the majority party, and the other 10 members must be evenly split between the two parties?

Express the answer as a formula for the number. You do not actually have to evaluate the formula.

$$\underset{\substack{\uparrow\\ \text{pick chair}}}{72} \cdot \underset{\substack{\uparrow\\ \text{pick 5 other}\\ \text{Fat Cats}}}{C(71,5)} \cdot \underset{\substack{\uparrow\\ \text{pick 5 Workers}}}{C(57,5)}$$

Question 3. [20 pts] Consider the following game. Two players start with a pile of n pebbles. They take turns removing pebbles from the pile. At each turn, a player is allowed to take either one or two pebbles. The player who takes the last pebble loses.

Use strong induction to prove that, for every positive integer n, the first player has a winning strategy if $n \equiv 0$ or $n \equiv 2 \pmod 3$, and the second player has a winning strategy if $n \equiv 1 \pmod 3$.

If $n=1$, the first player loses, so the second player has a winning strategy.

If $n>1$, we assume by induction that we know who has the winning strategy in games with $m<n$ pebbles.

If $n>1$ and $n \equiv 0 \pmod 3$, the first player can take 2 pebbles. If $n>1$ and $n \equiv 2 \pmod 3$, the first player can take 1 pebble. Either way, this leaves the other player with $m \equiv 1 \pmod 3$ pebbles, $m<n$. The first player, who is now in the position of second player after taking his or her turn, then has a winning strategy by induction.

If $n>1$ and $n \equiv 1 \pmod 3$, then either choice by the first player leaves the second player, who is now in the position of first player, with $m<n$ pebbles and $m \equiv 0$ or $m \equiv 2 \pmod 3$. Hence, by induction, the original second player has a winning strategy.

Note that the actual strategy can be summarized as 'always try to leave your opponent with a number of pebbles $n \equiv 1 \pmod 3$, if possible.'

Question 4. [20 pts] Find all solutions of $x^2 \equiv 1 \pmod{143}$. Note that $143 = 11 \cdot 13$.

By CRT, we need $x \equiv \pm 1$ mod 11 and $x \equiv \pm 1$ mod 13. There will be four congruence classes (mod 143) that are solutions. To find them, first solve

	(mod 11)	(mod 13)
a	1	0
b	0	1

for $a = 13k$ where $\underset{2k}{\underset{\equiv}{13k}} \equiv 1 \pmod{11}$: $k=6$, $a=78$

$b = 11\ell$ where $\underset{-2\ell}{\underset{\equiv}{11\ell}} \equiv 1 \pmod{13}$: $\ell = -7$, or $\ell = 6$, $b = 66$

Then $x \equiv \pm a \pm b \pmod{143}$ gives the four (congruence classes of) solutions:

$x \equiv a+b = 144 \equiv 1 \pmod{143}$

$x \equiv -a-b = -144 \equiv -1 \pmod{143}$

$x \equiv a-b = 12 \pmod{143}$

$x \equiv b-a = -12 \equiv 131 \pmod{143}$.

Question 5. [5 pts each] To construct a pair of public and private keys for the RSA encryption system, you start by choosing two large prime numbers p and q. Your public key (which you reveal) consists of a modulus n and an exponent e. Your private key (which you keep secret) is an exponent d. Answer the following questions.

(a) What is the modulus n, in terms of p and q?

$n = pq$

(b) You choose e and d to be inverses $ed \equiv 1 \pmod{m}$. What is the integer m, in terms of p and q?

$m = (p-1)(q-1)$

(c) I want to send you a message x (expressed as an integer $0 \leq x < n$), encrypted so that only you can read it. How do I use your public key (n, e) to encrypt x?

$E(x) = x^e \underline{\text{mod}}\ n$

(d) When you receive my encrypted message, how do you find find the original message x?

From $y = E(x)$ get $x = D(y) = y^d \underline{\text{mod}}\ n$.

(e) Briefly explain why it is difficult for anyone to discover your private key d if they only know your public key (n, e).

To find d from e we need to know $m = (p-1)(q-1)$, and to find m we would need to factor n. Factoring products of large primes is believed to be infeasible.