23) A set of passwords allow upper case letters and digits.
a) Determine the number of passwords of length 4 that contain at least one digit.
b) Determine the number of passwords of length 4 that contain exactly one digit.
c) Determine the number of passwords of length 4 that contain at most two (i.e. 0, 1, or 2) digits.

24) The *Organization Without a Cool Acronym* (OWCA) encrypts its messages with a Vigenère cipher whose key (e.g. the full text of a book) is longer than any message. This way there is no keyword repetition within the message and the strategy described in class for breaking the messages will not work.
You cleverly have intercepted a whole stack of messages that have been encrypted in this way all with the same key. Describe a strategy that you could use to break the encryption.

25) Remember that $\varphi(n)$ counts the number of $1 \le a < n$ such that $\gcd(a,n) = 1$.
(This problem is intended as help and illustration for problem 26. If you are doing problem 26 in any case you may skip this problem and you will still be given credit for it.)
For each of the following choices of n, find all numbers $1 \le a < n$ such that $\gcd(a,n) = 1$ and use this to determine $\varphi(n)$:

$$3, 5, 9 = 3^2, 25 = 5^2, 27 = 3^3, 12 = 2^2 3$$

26) We want to determine a formula for $\varphi(n)$, namely show that for $n = \prod_i p_i^{e_i}$ one has that $\varphi(n) = \prod_i (p_i - 1) p_i^{e_i - 1}$.
a) Let $n = p^2$ for a prime p. Describe the $1 \le a < n$ such that $\gcd(a,n) \neq 1$. Conclude that $\varphi(p^2) = (p-1)p$.
b) With a similar argument as in a), show that $\varphi(p^k) = (p-1)p^{k-1}$.
c) Assume that $n = u \cdot v$ with $\gcd(u,v) = 1$. Describe those $1 \le a \le n$ such that $\gcd(a,u) \neq 1$.
d) Assume that $n = u \cdot v$ with $\gcd(u,v) = 1$. Using c), determine the number of $1 \le a \le n$ such that $\gcd(a,u) \neq 1$ or $\gcd(a,v) \neq 1$. Use this to show that $\varphi(n) = \varphi(u) \cdot \varphi(v)$. (We say that φ is a *multiplicative number theoretic function*).

27) You have shown in problem 26 that if $n = \prod_i p_i^{e_i}$, then $\varphi(n) = \prod_i (p_i - 1) p_i^{e_i - 1}$. Use this to calculate $\varphi(7920) = \varphi(2^4 3^2 5 \cdot 11)$.

28) You are given the task of determining the minimal height[1] that a certain type of glass will break when dropped[2]. The only tool you have is one glass and a (long) ruler, so you have to rely on

[1] in feet. You know that it is between 1ft and 100ft

[2] Being mathematicians, we assume that there is no disturbance and that indeed there is exactly such a height at which this model of glass always breaks

dropping the glass from different heights and see when it breaks. (And onviouysly the glass is gone then.) You aim to minimize the number of drops required.
a) Explain, why with one glass available, the best you can do is to drop from 1ft, 2ft, 3ft, ...until the glass breaks. (**Hint:** If you were skipping a hight of a ft, how would you be able to distinguish a ft and $a+1$ ft as breaking height?)
b) Now you are given two glasses to use in your experiment. What is the best method (fewest number of steps) to determine the height now. (**Hint:** Consider the two digits of the height.)

Sample Midterm Problems

The following practice problems (not to be handed in) are on a level that they could easily be midterm problems, I would expect a midterm to contain around 5 of such problems. You will be allowed use of a pocket calculator for arithmetic.
(These are problems I assume you all are able to do and I will therefore not provide written solutions.)

1) Find a integer x such that $3x + 17 \equiv 8 \pmod{23}$.

2) Assume that p is a prime and $1 \leq a < p$ and $k > 0$ such that $a^k \equiv 1 \pmod{p}$. Show that $a^{\gcd(k,p-1)} \equiv 1 \pmod{p}$.

3) Show that 2 is a primitive root modulo 101. (You may use without proof that 101 is prime and that $50_{10} = 110010_2$ and that $20_{10} = 10100_2$.) Your answer should include a brief explanation (but not just "that is the method we used in the lecture") why the calculations performed show this fact.

3) Show, usings Fermats little theorem, that $n = 161$ is not prime. You may use without proof that $n - 1 = 2^7 + 2^5$. Explain your calculations.

4) Encrypt the message FORT COLLINS using a Vigenère cipher with keyword HOUSE. (In an exam you would be given a tabula recta.)

5) Let $p = 97$ and $a = 5$. Then (you may use this without proof) a is a primitive root modulo p. Determine $\text{OrderMod}_{97}(5^{10})$ (where $5^{10} \equiv 53 \pmod{97}$).

6) Assume that passwords are of length 4 and may contain upper case, lower case letters and digits. Determine the number of passwords that contain at least least one uppercase and one lowercase letter. Determine the number of passwords that contain exactly two upper case letters.

7) Let $p = 419 = 2 \cdot 11 \cdot 19 + 1$, which is prime. a) What are the possibilities for $\text{OrderMod}_p(a)$ if $\gcd(a, p) = 1$?
b) Using the list from a), determine $\text{OrderMod}_p(40)$.