17) Again the setup is similar to problem 11, but the source text is from *The House at Pooh Corner*. Also this time the text has been encrypted with a Vigenère cipher with a keyword of length $4 \ldots 7$. (Problem link under homework 3 or `http://www.math.colostate.edu/~hulpke/lectures/m360/prob17.html`). Decrypt the text snippet assigned to you via the CSUID mod 169.
To save you counting by hand you may use the online decryption tool at: `http://www.simonsingh.net/The_Black_Chamber/vigenere_cracking_tool.html`

18) Let $p = 53$ (which is prime).
a) Show that 2 is a primitive root modulo p.
b) Find e, such that $2^e \equiv 3 \pmod{53}$.

19) Let $\gcd(a, p) = 1$ and let $n = \mathrm{OrderMod}_p(a)$. We want to determine $o_k = \mathrm{OrderMod}_p(a^k)$ for $k \geq 1$.
a) Show that $(a^k)^n \equiv 1 \pmod{p}$. Conclude that $o_k | n$.
b) Show that if $k|n$ then $o_k = n/k$.
c) Show that if $\gcd(k, n) = 1$ then $o_k = n$. (**Hint:** From $1 = uk + vn$ conclude that $a \equiv (a^k)^u \pmod{p}$ and thus with a) that $n|o_k$.)
d) Combining b) and c), show that $o_k = \frac{n}{\gcd(n,k)}$
e) Show that there are exactly $\varphi(p-1)$ primitive roots modulo p. (**Hint:** If a is a primitive root, all other primitive roots are powers of a, and all have order n.)

20) A restaurant offers pancakes with "a thousand and one combinations" of toppings. Assuming this count is exact, what can one conclude about the nature of toppings offered??

21) Assuming you want to calculate bionomial coefficients on a computer that cannot handle numbers bigger than a certain absolute value (e.g. 2^{32}), which of the following four methods is preferrable, and why?

a) $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$

b) $\binom{n}{k} = n(n-1)\cdots(n-k+1)/k!$

c) $\binom{n}{0} = 1, \binom{n}{k} = \binom{n}{k-1} \cdot \dfrac{n-k+1}{k}$.

d) $\binom{n}{0} = \binom{n}{n} = 1, \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ (Pascal's Triangle)

22) According to J.L. Borges, *The Library of Babel*[1]:

> is composed of an indefinite and perhaps infinite number of hexagonal galleries, with vast air shafts between, surrounded by very low railings. From any of the hexagons one can see, interminably, the upper and lower floors. The distribution of the galleries is invariable. **Twenty shelves, five long shelves per side, cover all the sides except two**; their height, which is the distance from floor to ceiling, scarcely exceeds that of a normal bookcase. One of the free sides leads to a narrow hallway which opens onto another gallery, identical to the first and to all the rest. To the left and right of the hallway there are two very small closets. In the first, one may sleep standing up; in the other, satisfy one's fecal necessities. Also through here passes a spiral stairway, which sinks abysmally and soars upwards to remote distances. In the hallway there is a mirror which faithfully duplicates all appearances. Men usually infer from this mirror that the Library is not infinite (if it were, why this illusory duplication?); I prefer to dream that its polished surfaces represent and promise the infinite.[...]
>
> There are five shelves for each of the hexagon's walls; **each shelf contains thirty-five books of uniform format; each book is of four hundred and ten pages; each page, of forty lines, each line, of some eighty letters** which are black in color. [...] **The orthographical symbols are twenty-five in number**. [...] These examples made it possible for a librarian of genius to discover the fundamental law of the Library. This thinker observed that all the books, no matter how diverse they might be, are made up of the same [25] elements: the space, the period, the comma, the twenty-two letters[2] of the alphabet. He also alleged a fact which travelers have confirmed: In the vast Library **there are no two identical books**.

a) Following the description as given by the bold sections; How many books does the library contain?
b) Clearly the assertion "perhaps infinite number" of galleries in the first line of the quote is wrong. Can you imagine a configuration for a finite library that still would allow a staircase going up and down from every gallery to another gallery?

Practice Problems: (These problems from the book are not to be handed in, but might be useful in reviewing and in exam preparation): **4.2**, **4.3**, **4.4**, **4.10**, **4.11**,

[1] Ficciones, 1944, here quoted from `http://www.analitica.com/bitblioteca/jjborges/library_babel.asp`

[2] as an Argentinian he is using a Spanish alphabet