Exercises E1: Basics, Probability, Permutations, Combinatorics, Classic Ciphers

August 31, 2006

1 Limbering Up

0. The splash webpage for this course has a cipher. What's the plaintext? (hint: You don't have to know French).

2 From *Making, Breaking Codes* by Paul Garrett

Original problem numbers in parens. There are Optional (extra credit) problems and DOUBLE and TRIPLE point scores. Garrett has sample answers in an appendix.

1. Find the reduction mod 73 of 1000. (1.2.04)

2. (Optional) Find the reduction mod 399 of -997. (1.2.13)

3. Prove in general that if r is the reduction of N mod m, and if $r \neq 0$, then $m - r$ is the reduction of $-N$ mod m. (1.2.17)

4. DOUBLE POINTS. Estimate how much easier it would be to find an 8-character one-time pad key knowing that it is an English word, rather than an arbitrary string of 8 characters (among a – z coded as 0 – 25). (1.3.07)

5. How many different ways are there to order the set $\{1,2,3,4\}$? (2.1.02)

6. (Optional) How many subsets of $\{1,2,3,4,5,6,7\}$ have exactly 4 elements? (2.1.07)

7. How many different choices are there of an *unordered* pair of *distinct* numbers from the set $\{1,2,...,9,10\}$? How many choices of *ordered* pairs? (2.1.10)

8. (Optional) How many pairs of disjoint subsets each with three elements are there in the set $\{1,2,...,7,8\}$? (2.1.12)

9. What is the probability of exactly 3 heads out of 10 flips of a fair coin? (2.2.01)

10. If there are 3 red balls and 7 blue ones in an urn, what is the probability that in two trials (draw one ball per trial) two red balls will be drawn? (2.2.06)

11. What is the probability that in a roll of two fair dice, the upper faces of the two dice sum to either 7 or 8? (2.2.10)

12. *The Birthday Paradox* Show that the probability is greater than 1/2 that, out of a given group of 23 people, at least two will have the same birthday. (2.2.12)

13. (Optional) TRIPLE POINTS. Suppose two real numbers are chosen "at random" (technically, from a uniform distribution) between 0 and 1. What is the probability that their sum is greater than 1? What is the probability that their product is greater than 1/2? (2.2.14).

14. (Optional) Decrypt the affine cipher with ciphertext 'LBBKL BJMKB OLTQW TXIKT WKIBJ AABN'. (2.4.02)

15. (Optional) An affine cipher $E_{a,b}(x) = (ax + b) \bmod 26$. Show that a two-round affine cipher can in some cases have no net effect by showing that $E_{25,25}(E_{25,25}(x)) = x$. (1.4.20)

16. Express the following permutation as a product of disjoint cycles, and determine the order. (3.3.03)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 7 & 1 & 5 & 6 \end{pmatrix}$$

17. Compute the product (3.3.06)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 4 & 7 & 1 & 3 & 6 \end{pmatrix} \times \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 5 & 7 & 1 & 4 & 6 \end{pmatrix}$$

18. (Optional) How many distinct 3-cycles are there in the symmetric group S_5 of permutations of five things? (3.3.08)

19. Show that when a good riffle shuffle on a deck of 50 cards is executed just 8 times in a row, then all cards return to their original positions. (3.4.01)

20. (Optional) Determine the cycle decomposition of a good riffle shuffle on a deck of 18 cards. (3.4.07)

21. Find the cycle decomposition of the 3-by-7 (left-to-right, top-to- bottom) block interleaver. (3.5.04)

22. (Optional) Show that a 2-by-n left-to-right, bottom-to-top block interleaver has the same effect as a good riffle shuffle. Likewise that a 2-by-n left-to-right, top-to-bottom block interleaver has the same effect as a bad riffle shuffle. (3.5.05)

3 From Trappe and Washington

Section 2.13
Exercises: 1, 4, 5, 6, 7, 8.