March 16, 2006

Physics 681-481; CS 483: Discussion of #4

I.

(a) According to Eq. (1) in Assignment #4, the probability of finding 2 linearly independent vectors (doing arithmetic modulo 2) among a random set of four 3-vectors of 0's and 1's orthogonal to the vector $a = 111$, is

$$q = \left(1 - \tfrac{1}{8}\right)\left(1 - \tfrac{1}{16}\right) = \tfrac{105}{128}. \qquad (n = 3,\ x = 1) \tag{1}$$

To check this note that the four vectors orthogonal to 111 are 000, 110, 101, and 011. Any two distinct nonzero vectors from this set are linearly independent, so the number of the $4^4 = 256$ different quartets *without* two linearly independent vectors, is just the number of quartets containing at most one kind of nonzero vector. To enumerate these note that:

(a) There is just 1 way to have four zero vectors (000).

(b) There are 12 ways to have one nonzero vector and three zero vectors: the nonzero vector can be either the first, second, third, or fourth vector in the quartet, and it can have one of the three forms (110), (101), or (011)).

(c) There are 18 ways to have two identical nonzero vectors and two zero vectors: there are $4 \times 3/2 = 6$ possibilities for the two zero vectors, and for each of these the two identical nonzero vectors can both have one of the three forms (110), (101), or (011)).

(d) There are 12 ways to have three identical nonzero vectors and one zero vector: 4 choices for the zero vector and for each of these three choices for the three identical nonzero vectors.

(e) There are 3 ways to have four identical nonzero vectors.

Adding these up we have 1+12+18+12+3 = 46 quartets that fail to contain at least two independent vectors. This leaves 256-46 = 210 quartets containing at least two independent vectors. So the probability of finding two independent vectors (and therefore learning the value of a) in four attempts is $\frac{210}{256} = \frac{105}{128}$, which agrees with (1) above.

II.

(a) If Bob announces $N = 55$ and $c = 17$ and Alice's message is $a = 9$, then her encoded message is

$$b = a^c \pmod N = 9^{17} \pmod{55}. \tag{2}$$

Using $\equiv$ to denote equality modulo 55, and noting that

$$9^{17} = 9^{16} \times 9$$

we have (mod 55)

$$9^2 = 81 \equiv 26; \quad 9^4 \equiv (26)^2 = 676 \equiv 16; \quad 9^8 \equiv (16)^2 = 256 \equiv -19; \quad 9^{16} \equiv (19)^2 = 361 \equiv 31; \tag{3}$$

and therefore

$$b = 9^{17} \equiv 9 \times 31 = 279 \equiv 4. \tag{4}$$

(b) Bob's decoding number d is the inverse of 17 modulo $(11-1)(5-1) = 40$. We can find d using the Euclidean algorithm as follows:

$$40 - 2 \times 17 = 6; \tag{5}$$

$$17 - 2 \times 6 = 5; \tag{6}$$

$$6 - 5 = 1. \tag{7}$$

Using (6) to eliminate 5 from (7) we find

$$1 = 3 \times 6 - 17. \tag{8}$$

Using (5) to eliminate 6 from (8) we find

$$1 = 3 \times 40 - 7 \times 17. \tag{9}$$

So

$$d \equiv -7 \equiv 33 \text{ (mod 40)}. \tag{10}$$

Getting back to arithmetic modulo 55, we have

$$4^{33} = 4^{32} \times 4, \tag{11}$$

and we have (mod 33)

$$4^2 = 16; \quad 4^4 \equiv (16)^2 = 256 \equiv -19; \quad 4^8 \equiv (19)^2 = 361 \equiv -24;$$
$$4^{16} \equiv (24)^2 = 576 \equiv 26; \quad 4^{32} \equiv (26)^2 = 676 \equiv 16. \tag{12}$$

So

$$b^d \equiv 4^{33} \equiv 4 \times 16 = 64 \equiv 9 = a. \tag{13}$$

(c) Since $55 = 5 \times 11$, the order of G_{55} is (11-1)(5-1) = 40, so r divides 40 and is either 2, 4, 5, 8, 10, 20, or 40. Eq. (12) reveals that r is not 2, 4, or 8. We also have

$$4^5 \equiv 4 \times 4^4 \equiv 4 \times (-19) = -76 \equiv 34, \tag{14}$$

so r is not 5. But

$$4^{10} \equiv (4^5)^2 \equiv 34^2 \equiv (-21)^2 = 441 \equiv 1, \tag{15}$$

so $r = 10$.

(d) The decimal system makes it child's play to find inverses modulo 10: Since $3 \times 7 = 21$, 3 is the inverse of 17 modulo 10. So Eve calculates $4^3 = 64 \equiv 9$ and she has recovered Alice's message.