Announcements:

- The second midterm (Q & A) from Spring '96 is on the Web page and at Copy Central.
- For the exam on October 30, the class will be divided as before. *Students who went to 1 Leconte last time will go to 10 Evans this time.* Students who were in Haas last time are again in Haas.
- I posted the homework for the Lenstra Notes. Homework due tomorrow: the first five questions in those notes.

If $f : S \to \mathbf{R}$ is a random variable, its expected value $E(f)$ is

$$\sum_{x \in S} f(x)p(x) = \sum_r r \cdot p(f = r).$$

Recall that $p(f = r) = \sum p(x)$, where the sum is taken over all x such that $f(x) = r$. We have seen, for instance, that the simple identity $E(f + g) = E(f) + E(g)$ can be very useful. (We took f to be the value of the first die and g to be the value of the second.)

Here is another example which illustrates the power of this method and also the utility of regarding events as random variables. To do the latter, we recall that to each event E we can associate its characteristic function χ_A. Then $E(\chi_A) = p(A)$.

The problem, done out in the notes, is the following. Let n be a positive integer (e.g., $n = 10$) and let S be the set of 1-1 onto maps from $\{1, \dots, n\}$ to itself. Thus S has $n!$ elements. Consider the random variable $f : S \to \mathbf{R}$ which attaches to $b \in S$ the number of fixed points of b. Thus $f(b) = 0$ if and only if b is a derangement, while $f(b) = n$ if and only if b is the identity. What is $E(f)$?

For each i, let A_i be the set of b that fix i. The main point, simple but very useful, is that

$$f = \chi_{A_1} + \cdots + \chi_{A_n}.$$

Thus $E(f)$ is the sum of the $E(\chi_{A_i})$. These latter numbers are equal by symmetry.

We calculate: $E(\chi_{A_i}) = p(A_i) = \#(A_i)/n!$. Clearly, $\#(A_i) = (n-1)!$. Thus $E(f) = \dfrac{1}{n} + \cdots \dfrac{1}{n}$ (n times), so that $E(f) = 1$. This means that the "average" permutation fixes 1 element!

In the next key problem, we flip a biased coin n times. The coin has two faces: 0 and 1. Assume that the probability of getting a "1" on any given flip is p $(0 < p < 1)$ and that the probability of getting a "0" is $q = 1 - p$. The outcome of n flips can be represented as a binary string of length n. The sample space attached to this situation is the set S of length-n binary strings. The probability function $P : S \to [0, 1]$ takes a string to $p^k q^{n-k}$, where k is the number of 1's in the string.

For each i, let A_i be the set of strings with a 1 in the ith place. It is clear from the construction of the problem that $P(A_i) = p$. If you try to verify this in a clumsy way, you get a sum like

$$\sum_{k=1}^{n} \binom{n-1}{k-1} p^k q^{n-k}$$
$$= \sum_{j=0}^{n-1} \binom{n-1}{j} p^{j+1} q^{n-1-j}.$$

If you factor out one p, what's left is $(p+q)^{n-1}$ (by the binomial theorem), and this is just 1. Hence $P(A_i)$ is most definitely p.

Remember that $P(A_i) = E(\chi_{A_i})$ as in the previous example. Hence if $f = \sum \chi_{A_i}$, $E(f) = np$. But f is just the function that takes a string to the number of 1's in the string. So the expected number of 1's is np.

In Rosen's book, one proves this by a direct calculation which uses the binomial theorem as in a previous slide. Lenstra does this as well, to give an alternative proof. Here is how that works. First, we note that $P(f = k)$ is $\binom{n}{k} p^k q^{n-k}$ because there are $\binom{n}{k}$ strings with exactly k 1's. Next,

$$E(f) = \sum_k k \cdot P(f = k).$$

This gives

$$E(f) = \sum_{k=0}^{n} k \binom{n}{k} p^k q^{n-k}$$
$$= np \sum_{k=1}^{n} \binom{n-1}{k-1} p^{k-1} q^{n-k}.$$

In going from the first line to the second, we tossed out the term with $k = 0$ because it's 0 anyway, we factored out a p as before, and we noted that $k\binom{n}{k} = n\binom{n-1}{k-1}$. (This is a simple factorial manipulation.)

Now let $j = k - 1$ again. Then

$$E(f) = np \sum_{j=0}^{n-1} \binom{n-1}{j} p^j q^{n-1-j} = np.$$

Here, we again recognized a binomial theorem expression for $(p+q)^{n-1}$.

A final example of this ilk. You shoot at a target until you get a hit; the probability of getting a hit on any shot is p. What is the expected number of shots?

The sample space is the set S of positive integers, with $n \in S$ corresponding to $n-1$ misses followed by a hit. Then $P(n) = q^{n-1}p$, where $q = 1-p$ as before. The function $n \mapsto n$ is the one whose expected value we want. This expected value is

$$\sum_{n=1}^{\infty} nq^{n-1}p = p\sum_n nq^{n-1}.$$

Since $\dfrac{1}{1-x} = \sum x^n$, we learn in Math 1B that $\dfrac{1}{(1-x)^2} = \sum nx^{n-1}$. Hence the expected value is

$$\frac{p}{(1-q)^2} = \frac{1}{p}.$$

Cute!

The final topic for today has to do with independence of random variables. We've already learned about independence of events. We say that f and g are independent if $P(f = r_1 \text{ and } g = r_2)$ is the product

$$P(f = r_1)P(g = r_2).$$

Say f corresponds to the event A and g to the event B. The particular equality

$$P(f = 1 \text{ and } g = 1) = P(f = 1)P(g = 1)$$

amounts to the definition of A and B being independent:

$$P(A \cap B) = P(A)P(B).$$

Hence if f and g are independent, so are A and B.

How about the converse? Suppose that A and B are independent. We have to check, e.g., that

$$P(f = 1 \text{ and } g = 0) = P(f = 1)P(g = 0).$$

This means

$$P(A \cap (S \setminus B)) = P(A)P(S \setminus B).$$

The right-hand side is $P(A) - P(A)P(B) = P(A) - P(A \cap B) = P(A \setminus B)$. Same for the left-hand side.