10 Powerful Ideas	Bruce Maggs
Solutions to Final Review Exercises	May 2, 1998

Quickies

1.

$$\sum_{i=0}^{n} 2^i = \frac{2^{n+1}-1}{2-1} = 2^{n+1}-1$$

2.

$$\sum_{i=0}^{n} x^i = \frac{x^{n+1}-1}{x-1}$$

3.

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2} \text{ (Little Gauss's formula)}$$

4.

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n$$

5.

$$\binom{n}{i-1} + \binom{n}{i} = \binom{n+1}{i} \text{ (Pascal's triangle)}$$

6. What is the coefficient of $a^2b^3c^5$ in $(a+b+c)^{10}$?

$$\binom{10}{2;3;5} = \frac{10!}{2!3!5!}$$

Induction

7. *Solve the following recurrences:*

(a)

$$\begin{aligned} T(n) &= 6T(n-1) - 8T(n-2) \\ T(0) &= 0 \\ T(1) &= 1 \end{aligned}$$

This problem is a linear recurrence (like the Fibonacci recurrence), so we can solve it by assuming that all solutions have the form $T(n) = \lambda^n$, and substituting to solve for λ:

$$\begin{aligned} \lambda^n &= 6\lambda^{n-1} - 8\lambda n - 2 \\ \lambda^n - 6\lambda^{n-1} + 8\lambda n - 2 &= 0 \\ \lambda^{n-2}(\lambda^2 - 6\lambda + 8) &= 0 \\ \lambda^{n-2}(\lambda - 4)(\lambda - 2) &= 0 \end{aligned}$$

The values of λ that satisfy this equation are $\lambda = 0, 2, 4$. Thus $T(n)$ is a linear combination of 2^n and 4^n (since 0^n contributes nothing). Let $T(n) = a2^n + b4^n$, and solve for a and b with the base cases:

$$\begin{aligned} T(0) = a2^0 + b4^0 &= 0 \\ T(1) = a2^1 + b4^1 &= 1 \end{aligned}$$

$$\begin{aligned} a + b &= 0 \\ 2a + 4b &= 1 \end{aligned}$$

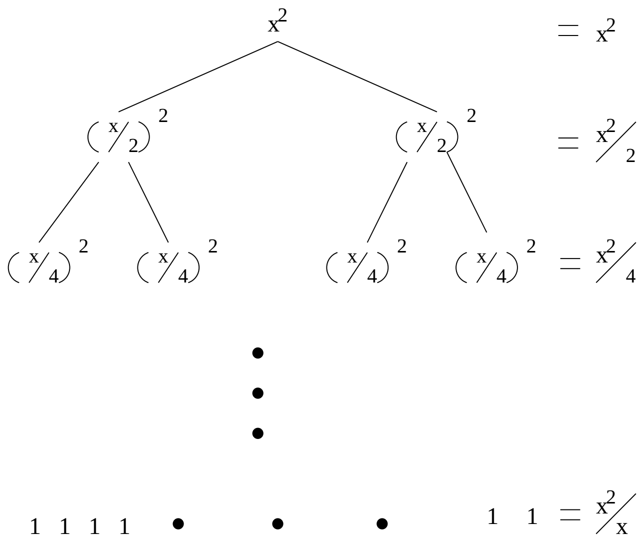
$$\begin{aligned} a &= -\frac{1}{2} \\ b &= \frac{1}{2} \end{aligned}$$

So the answer is

$$T(n) = -\frac{1}{2}2^n + \frac{1}{2}4^n$$

(b)

$$\begin{aligned} T(n) &= 2T(n/2) + n^2 \\ T(1) &= 1 \end{aligned}$$



The sum of the line sums is:

$$\sum_{i=0}^{\lg x} \frac{x^2}{2^i} = x^2 \sum_{i=0}^{\lg x} 2^{-i} = x^2 \frac{1 - 2^{-(\lg x+1)}}{1 - 2^{-1}} = x^2 \frac{1 - \frac{1}{2x}}{\frac{1}{2}} = 2x^2 - x$$

8. *Prove by induction that $\phi^n = F_n\phi + F_{n-1}$ for $n \geq 1$.*

Base case. $n = 1$. $\phi = F_1\phi + F_0 = 1\phi + 0 = \phi$.

Inductive step. Assume $\phi^n = F_n\phi + F_{n-1}$. Consider ϕ^{n+1}:

$$\begin{aligned} \phi^{n+1} &= \phi^n \phi \\ &= (F_n\phi + F_{n-1})\phi \\ &= F_n\phi^2 + F_{n-1}\phi \\ &= F_n(\phi + 1) + F_{n-1}\phi \text{ because } \phi^2 = \phi + 1 \\ &= (F_n + F_{n-1})\phi + F_n \\ &= F_{n+1}\phi + F_n \text{ by definition of Fibonacci numbers} \end{aligned}$$

A number of students worked not in terms of ϕ for these two induction problems, but in terms of $\frac{1+\sqrt{(5)}}{2}$. This expansion was unnecessary and often led to arithmetic problems.

Groups and Fields

9. *State the four properties that define a group.*

The properties that define a group $(G, \cdot)$ are:

Closure: for all $a, b \in G$, $a \cdot b \in G$.

Associativity: for all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Identity: there exists an element $e \in G$ such that for all $a \in G$, $a \cdot e = e \cdot a = a$.

Inverses: for all $a \in G$, there exists an element a^{-1} such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

A common error is to confuse associativity with commutativity (for all $a, b \in G$, $a \cdot b = b \cdot a$). Associativity is required of a group; commutativity is not. Can you name a non-commutative group?

10. *List all the subgroups of $(\mathcal{Z}_p, +)$, where p is prime.*

The only subgroups are the trivial subgroups, $\{0\}$ and $\mathcal{Z}_p$ itself. Why are there no others? By Lagrange's Theorem, the size of a subgroup must divide the size of the group. Since $\mathcal{Z}_p = \{0, \ldots, p\}$, the size of $\mathcal{Z}_p$ is p, whose only factors are 1 and p itself. Thus the only possible subgroup sizes are 1 and p. Every subgroup must contain the identity element 0, so $\{0\}$ is the only subgroup of size 1, and $\mathcal{Z}_p$ is the only subset of size p. Thus no other subgroups are possible.

11. *Prove that the set of n-bit bitstrings is a group under the operation bitwise XOR.*

Let's represent n-bit bitstrings as $a_1 a_2 \cdots a_n$, and the XOR operation as $\oplus$. We shall prove the four group properties:

Closure: Take any two bitstrings $a = a_1 a_2 \cdots a_n$ and $b = b_1 b_2 \cdots b_n$. Then $a \oplus b = (a_1 \oplus b_1)(a_2 \oplus b_2) \cdots (a_n \oplus b_n)$ is also an n-bit bitstring.

Associativity: For any n-bit bitstrings a, b, c, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ if and only if for all bits i, $(a_i \oplus b_i) \oplus c_i = a_i \oplus (b_i \oplus c_i)$, which is true if and only if the XOR operation on single bits is associative. Here are two ways to prove this. We know that XORing several bits together computes the parity of the bits (the XOR is 1 if there are an odd number of 1s, or 0 if there are an even number of 1s). The parity of the bits is independent of the way you parenthesize the XOR, so XOR is associative. (It's even independent of the order, so XOR is commutative, too.)

If this argument is too fuzzy (or you forgot about this meaning of XOR), you can also check associativity by writing out a truth table:

a_i	b_i	c_i	$(a_i \oplus b_i) \oplus c_i$	$a_i \oplus (b_i \oplus c_i)$
0	0	0	0	0
0	0	1	1	1
0	1	0	1	1
0	1	1	0	0
1	0	0	1	1
1	0	1	0	0
1	1	0	0	0
1	1	1	1	1

Identity: The identity element is an n-bit string consisting of zeros, $00\cdots0$, because $a_i \oplus 0 = a_i$.

Inverses: The inverse of every element is itself, because $a_i \oplus a_i = 0$.

12. *Prove that the set of n-bit bitstrings with even parity is a subgroup of the group in the previous problem.*

Clearly n-bit bitstrings with even parity are a subset of n-bit bitstrings. So it remains to show that the group properties hold for this subset:

Closure: In this case, closure is the hardest to prove. Take any a, b which are n-bit bitstrings with even parity. Even parity means that $a_1 \oplus a_2 \oplus \cdots \oplus a_n = 0$ and $b_1 \oplus b_2 \oplus \cdots \oplus b_n = 0$. We know from above that XOR is associative and commutative, so the parity of $a \oplus b$ is:

$$\begin{aligned}(a_1 \oplus b_1) \oplus (a_2 \oplus b_2) \oplus \cdots \oplus (a_n \oplus b_n) &= (a_1 \oplus a_2 \oplus \cdots \oplus a_n) \oplus (b_1 \oplus b_2 \oplus \cdots \oplus b_n) \\ &= 0 \oplus 0 \\ &= 0\end{aligned}$$

Thus $a \oplus b$ is an n-bit bitstring with even parity.

Associativity: The bitwise XOR operation is associative, as we showed in the previous problem.

Identity: the identity element $00\cdots0$ has even parity, so it's present in the subset.

Inverses: every element is its own inverse, so all elements in the subset have inverses.

13. *Show that the set of complex numbers $a + bi$ is a field.*

Recall that a field $(S, +, \cdot)$ consists of two groups $(S, +)$ and $(S - \{0\}, \cdot)$ with the distributive property $x \cdot (y + z) = x \cdot y + x \cdot y$. It's straightforward to check that the complex numbers are a group under addition:

Closure: $(a + bi) + (a' + b'i) = (a + a') + (b + b')i$
Associativity: by the associativity of $+$.
Identity: $(0 + 0i) + (a + bi) = (a + bi) + (0 + 0i) = a + bi$.
Inverses: $(a + bi) + (-a - bi) = 0 + 0i$.

We can also check that the complex numbers omitting $0+0i$ are a group under multiplication:

Closure: $(a + bi) \cdot (a' + b'i) = (aa' - bb') + (a'b + ab')i$
Associativity: by the associativity of $\cdot$.
Identity: $(1 + 0i) \cdot (a + bi) = (a + bi) \cdot (1 + 0i) = a + bi$.
Inverses: The multiplicative inverse of $(a+bi)$ is $\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$, which exists as long as $a+bi \neq 0+0i$.

The distributive property also holds for $+$ and $\cdot$, so the complex numbers are a field.

Counting and Probability

14. *The numbers 1447, 1005, and 1231 have something in common: each is a 4-digit number beginning with 1 that has exactly two identical digits. How many such numbers are there?*

Consider first the case where the duplicated digit is 1. The second 1 may be in one of 3 places in the number. The remaining two digits can be chosen in $9 \cdot 8$ ways, for a total of $3 \cdot 9 \cdot 8$ numbers.

Now consider the cases where the duplicated digit is other than 1. There are 9 choices for the duplicated digit, and $\binom{3}{2} = 3$ ways to arrange them in the last 3 places of the number. The remaining digit in the word can neither be 1 nor the same as the duplicated digit, for 8 possible choices. Thus

Combining these cases gives

$$3 \cdot 9 \cdot 8 + 9 \cdot 3 \cdot 8 = 432$$

15. *What is the largest 2-digit prime factor of the integer $n = \binom{200}{100}$?*

The answer is 61. Consider reducing n to

$$\binom{200}{100} = \frac{200 \cdot 199 \cdot 198 \cdot \dots \cdot 101}{100 \cdot 99 \cdot 98 \cdot \dots \cdot 1}$$

In the denominator, 61 occurs once, as itself. In the numerator, 61 occurs as a prime factor twice, in the integers $2 \cdot 61 = 122$ and $3 \cdot 61 = 183$. Thus the denominator cancels out only one factor of 61, leaving $\binom{200}{100}$ divisible by 61. Now consider any two-digit prime number larger than 61. The next largest is 67, which occurs once in the denominator (as itself), but only once in the numerator, as $2 \cdot 67 = 134$. Thus 67 and all higher two-digit primes cancel out.

16. *Letters in Morse code are formed by a succession of dots and dashes with repetitions allowed. How many different letters could be represented by 10 or fewer dots and dashes?*

Using exactly i symbols, 2^i. So the answer is $\sum_{i=1}^{10} 2^i = 2^{11} - 1$.

17. *n balls are placed randomly into n cells. What's the probability that exactly one cell remains empty?*

This problem was a little vague, and left some things unspecified (like whether balls are distinguishable or identical, and whether you can put more than one ball in a cell). On the bright side, though, you can look at it as several different counting problems rolled into one:

Interpretation 1: Suppose the balls are labeled so you can tell them apart, and the cells can hold more than one ball. Then the only way to put n balls in n cells leaving exactly one cell empty is to put two balls in one cell, one ball into each of $n-2$ other cells, and leave the last cell empty. The number of ways to do this is:

$$\begin{aligned} n \text{ (choices for empty cell)} \\ \times(n-1) \text{ (choices for the double-occupancy cell)} \\ \times(nchoose2) \text{ (choices for the balls in the doubled cell)} \\ \times(n-2)! \text{ (ways to place the other n-2 balls in the other cells)} \end{aligned}$$

Since the total number of ways to place labeled balls in labeled cells is n^n, the probability of exactly one cell empty is:

$$\frac{n(n-1)\binom{n}{2}(n-2)!}{n^n}$$

This is equivalent to

$$\frac{n!\binom{n}{2}}{n^n}$$

Interpretation 2. Suppose the balls are identical, *in the sense that the random process placing balls into cells makes no distinction between them.* (This isn't physically realistic if your random process is throwing ping pong balls into cells, because in the physical world, all balls are *different.* In quantum theory, however, it turns out that electrons behave as if they were identical – as bizarre as that sounds – so you could think about assigning n electrons to n energy levels leaving exactly one energy level empty.)

Anyway, if the balls are identical, then the number of ways to arrange the balls depends only on which cells you choose, not on the balls you decide to use for each cell, so the number of ways to leave one cell empty is just $n(n-1)$. The total size of the sample space is computed as if you were distributing n gold bars among n pirates; in other words, $\binom{2n-1}{n-1}$. So the probability would be:

$$\binom{n(n-1)}{\binom{2n-1}{n-1}}$$

Interpretation 3. What if a cell can't hold more than one ball? (This is a reasonable interpretation of the word "cell".) Then there's *no* way to leave a cell empty, because you'd have to double up in some other cell (by the pigeonhole principle). Thus the probability would be 0.

18. *A fair coin is flipped n times. What's the probability that all the heads occur at the end of the sequence?*

$$\frac{n+1}{2^n}$$

19. *A box contains 90 good and 10 defective screws. What's the probability that if 10 screws are used, none will be defective?*

$$\frac{\binom{90}{10}}{\binom{100}{10}}$$

20. *What is*

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} \cdots$$

and why?

Recall that

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

Now let $a = -1$ and $b = 1$. Clearly $(a+b)^n = 0$ for all $n > 0$, so

$$0 = \sum_{i=0}^{n} \binom{n}{i} (-1)^i$$

Since $\binom{n}{i} = 0$ for all $i > n$, we can let the sum go to infinity:

$$0 = \sum_{i=0}^{\infty} \binom{n}{i} (-1)^i$$

Finally, note that $(-1)^i$ alternates between $+1$ and -1, so this sum expands to:

$$0 = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} \cdots$$

21. *What is $(x+y+z)^m$ as a sum of terms?*

This is the multinomial formula,

$$\sum_{a,b,c:a+b+c=m} \frac{m!}{a!b!c!} x^a y^b z^c$$

22. *True or false:*

(a) *$E[AB] = E[A]E[B]$ if and only if A and B are independent.*

True. We proved this in recitation, and discussed it in the solutions to homework 8.

(b) *$E[A+B] = E[A] + E[B]$ if and only if A and B are independent.*

False! Linearity of expectation does not require that the random variables be independent. See the proof of linearity of expectation in lecture 19 if you don't believe this.

We've used this fact over and over to compute apparently difficult expectations. On Quiz 3, for example, we found the expected number of k-cliques by summing the expected value of each individual k-clique's indicator random variable. This works despite the fact that the k-cliques may share edges (making their indicator random variables dependent).

(c) *$E[\log A] = \log E[A]$ for all random variables A.*

False! Here's a simple counterexample. Let A be the random variable where $A = 1$ with probability 0.5, and $A = 2$ with probability 0.5. Then $E[A] = 0.5 \cdot 1 + 0.5 \cdot 2 = 1.5$, so $\log E[A] \approx 0.585$. But $E[\log A] = 0.5 \cdot 0 + 0.5 \cdot 1 = 0.5$. So $E[\log A] \neq \log E[A]$.

In general, it's dangerous to assume that expectation "distributes" through arbitrary computations.

23. *What is the probability of rolling two pair (such as 5 5 3 3 6) on the first roll in Yahtzee?*

Let's count the number of two-pair rolls. First choose the two dice that make up the high pair ($\binom{5}{2}$), the two dice that show the low pair ($\binom{3}{2}$), and the unpaired die (1 way). Next pick the two numbers that are paired ($\binom{6}{2}$ ways). Finally pick the unpaired number (4 ways). Since the total number of rolls is $1/6^5$, the probability of two pair is:

$$\frac{\binom{5}{2}\binom{3}{2}\binom{6}{2}4}{6^5}$$

24. *What is the probability of getting two pair (such as Q Q A A 3) in poker?*

$$\frac{13 \cdot \binom{4}{2} \cdot 12 \cdot \binom{4}{2} \cdot 11 \cdot \binom{4}{1}}{\binom{52}{5}}$$

25. *If you choose a k-bit number by randomly picking bits, what is the probability of getting a power of 2?*

A k-bit number is a power of 2 if exactly one of its bits is 1 and the rest are 0. So the probability is

$$\frac{k}{2^k}$$

An equivalent way to look at this problem is that there are k powers of 2 in the sample space: $2^0, 2^1, \ldots, 2^{k-1}$.

26. *If you pick a k-bit number at random, what is the probability of picking a prime?*

From the Prime Density Theorem, there are about $n/\ln n$ primes less than or equal to n. So the probability of picking a prime in $\{0, \ldots, 2^k - 1\}$ is approximately

$$\frac{2^k/\ln 2^k}{2^k} = \frac{1}{k \ln 2}$$

27. *What is $90^{1584} \pmod{11}$? (Hint: use Fermat's Little Theorem)*

Fermat's Little Theorem states that, for any prime p, $a^{p-1} = 1 \pmod{p}$. In other words, when working modulo p, we can reduce a^x to $a^{x \pmod{p-1}}$. Here $p = 11$, so we can say:

$$\begin{aligned} 90^{1584} &= 90^4 \pmod{11} \\ &= 2^4 \pmod{11} \\ &= 16 \pmod{11} \\ &= 5 \pmod{11} \end{aligned}$$

28. *Give two proofs for the identity*

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$$

One proof should be algebraic (manipulating symbols), the other combinatoric (showing a correspondence between two sets).

The algebraic proof is a straightforward application of the binomial theorem:

$$\begin{aligned}\sum_{i=0}^{n} \binom{n}{i} &= (1+1)^n \\ &= 2^n\end{aligned}$$

For the combinatoric proof, we will show that both sides of the identity count the subsets of an n-element set. One way to count the subsets of an n-element set is to represent each subset by an n-bit string where bit i is set if and only if element i appears in the set. There are 2^n such bit vectors, so the number of subsets is 2^n. Alternatively, we could count the subsets of an n-element set by counting the subsets of size i and summing for $i = 0 \ldots n$. There are $\binom{n}{i}$ subsets of size i, so the total number of subsets is $\sum_{i=0}^{n} \binom{n}{i}$.

29. If you pick two socks at random from a drawer with 5 gray socks and 4 black socks, what is the probability that the two socks match?

There are two disjoint cases: either you draw two gray socks (probability $\frac{5}{9}\frac{4}{8}$), or two black socks (probability $\frac{4}{9}\frac{3}{8}$), so the answer is:

$$\frac{5}{9}\frac{4}{8} + \frac{4}{9}\frac{3}{8} = \frac{4}{9}$$

Alternatively, you could look at the number of ways to choose two gray socks ($\binom{5}{2}$) or two black socks ($\binom{4}{2}$) and divide by the total number of ways to choose two socks ($\binom{9}{2}$) to get the same answer:

$$\frac{\binom{5}{2} + \binom{4}{2}}{\binom{9}{2}} = \frac{4}{9}$$

30. What is the probability that, out of n people chosen at random, at least two have the same birthday?

It's easier to compute the complement of this event: the probability that all n people have different birthdays:

$$1 \cdot \frac{364}{365} \cdot \frac{363}{365} \cdots \frac{365-n+1}{365}$$

So the probability that at least two have the same birthday is:

$$1 - \frac{365 \cdot 364 \cdot 363 \cdots (365-n+1)}{365^n}$$

31. How many people must you choose at random in order to ensure that at least *ten* people have the same birthday (ignore leap years)?

By the generalized Pigeonhole Principle, you need at least $365 \cdot 9 + 1 = 3286$ people to *ensure* that at least ten people have the same birthday.

Infinities, Undecidability, Intractability, Languages

32. *Give an example of each of the following, or explain why it don't exist.*

    (a) *a countably infinite field:* the rationals. (Possible wrong answers include: the integers, which are countably infinite but not a field; the reals, which are a field but uncountable; and GF_p, which is a field but finite.)

    (b) *a finite group:* $(\mathcal{Z}_n, +)$, $(\mathcal{Z}_n^*, \cdot)$.

    (c) *an uncountable regular language:* no such thing exists. A language is a set of finite strings over some finite alphabet Σ. Any language can be placed in one-to-one onto correspondence with the natural numbers by interpreting the strings as numbers in base $|\Sigma|$, so all languages are countable. Thus all regular languages (sets of strings accepted by a finite state machine) are also countable.

    (d) *a one-to-one onto function from $\mathcal{N}$ to $\mathcal{R}$:* no such thing exists. Cantor's diagonalization argument shows that it is impossible to place the natural numbers in one-to-one onto correspondence with the reals.

Graph Theory

33. *How many different Hamiltonian cycles are possible in a labeled complete graph on n vertices?*

    A Hamiltonian cycle visits every node exactly once. Since a complete graph includes all possible edges, every possible arrangement of the nodes is a Hamiltonian cycle. Thus the answer is

    $$n!$$

34. *How many trees can be made with 10 labeled nodes and 10 edges?*

    None. A tree with n nodes has $n-1$ edges.

A Moment's Thought

35. *For $\{1, 2, 3, \ldots, n\}$ and each of its nonempty subsets a unique* alternating sum *is defined as follows: Arrange the numbers in the subset in decreasing order and then, beginning with the largest, alternately add and subtract successive numbers. (For example, the alternating sum for $\{1, 2, 4, 6, 9\}$ is $9 - 6 + 4 - 2 + 1 = 6$ and for $\{5\}$ it is simply 5.) Find the sum of all such alternating sums for $n = 7$.*

    Let's start with a small example: $n = 2$. The set $\{1, 2\}$ has three nonempty subsets: itself (alternating sum 2-1) and the singleton sets $\{1\}$ and $\{2\}$ (alternating sum 1 and 2 respectively). Summing the alternating sums gives $(2-1)+1+2$. Observe that the 1 appears with both positive and negative weight, so it cancels, whereas the 2 appears only with positive weight, so we get $2 + 2 = 4$.

    So consider a different representation: instead of computing alternating sums, consider counting the ways each integer can appear in an alternating sum with positive or negative weight, and sum up the contributions of each integer to make the final sum. For the integer n itself, this calculation is easy: any subset containing n will always list n first in the alternating sum, so n will always be added to the final sum, never subtracted. Thus the contribution of n to the sum is n times the number of subsets in which it appears, 2^{n-1}.

For the remaining integers (1 to $n-1$), we claim that their contribution will always be zero. Take any i from 1 to $n-1$, and consider the subsets containing i. The subsets containing an even number of integers larger than i cause i to have a positive weight in their alternating sums. The subsets containing an odd number of integers larger than i cause i to have a negative weight. But the same number of subsets satisfy the even criterion as satsify the odd criterion. (Think about using a bit-string representation to pick the integers larger than i: the number of bit strings with an odd number of 1s is equal to the number with an even number of 1s.) Thus the additions of i are exactly cancelled by subtractions of i.

This leaves only the contribution from the integer n, so the sum of alternating sums is

$$n2^{n-1}$$

36. *Imagine constructing a graph as follows. Draw 10 nodes. Then for each pair of nodes, draw an edge between them with probability p. What is the expected number of nodes with degree exactly two?*

Every node has 9 possible edges leaving it, each chosen independently with probability p. Thus the probability that a particular node has exactly two edges leaving it is $\binom{9}{2}p^2(1-p)^7$. So if we define an indicator random variable X_i (which is 1 if node i has degree exactly two, and 0 otherwise), then $E[X_i] = \binom{9}{2}p^2(1-p)^7$. Summing $E[X_i]$ over all the nodes in the graph gives the expected number of degree-2 nodes:

$$10\binom{9}{2}p^2(1-p)^7$$