

18.781: Ideas for solutions to problem set 2

1.4 (4) (a) Let us first count the number of ways to choose n pairs (a_i, b_i) in $\{1, \dots, 2n\}$ with the order of a_i and b_i being specified (that is, a_i is the "first element" and b_i is the "second"). Well, there are $\binom{2n}{n}$ choices for the a_i , and once we fix the a_i , the choice of the b_i amounts to ordering the n remaining unchosen elements. There are $n!$ ways of doing this, so we find that the number of ways to choose ordered pairs (a_i, b_i) in $\{1, \dots, 2n\}$ is equal to

$$\binom{2n}{n}(n!) = \frac{(2n)!}{n!}.$$

Now to answer the question, note that if we are interested in unordered subsets (a_i, b_i) we just have to see how much we are "double counting" in the above. Well the answer is 2^n , for given any collection (α_i, β_i) of n disjoint unordered pairs in $\{1, \dots, 2n\}$, there are 2 ways of ordering each pair (α_i, β_i) , and with n pairs this gives 2^n possible orderings. Thus the answer to the question is

$$\frac{(2n)!}{2^n n!}.$$

To see the identity

$$(2n-1)(2n-3)\cdots 5\cdot 3\cdot 1 = \frac{(2n)!}{2^n n!},$$

note that

$$2^n n! = 2^n \prod_{j=1}^n j = \prod_{j=1}^n (2j).$$

That is, the product over the even numbers in the interval $[1, 2n]$. Therefore, when we divide $(2n)!$ by $2^n n!$ we are just left with the product over the odd numbers in the interval $[1, 2n]$.

(b) Well, $(n+1)\cdots(2n)$ is equal to $\frac{(2n)!}{n!}$, and by the discussion in (a) this is an integer (equal to the number of possible ways to choose ordered pairs). On the other hand, since by (a) the number $\frac{(2n)!}{2^n n!}$ is an *odd* integer, the power of 2 in $\frac{(2n)!}{n!}$ must be exactly n .

1.4 (8) (a) If $M = 0$ the result is clear. So we assume true for M and prove it for $M + 1$. A consequence of theorem 1.20 which we discussed in class is that

$$\binom{k+M+2}{k+1} = \binom{k+M+1}{k+1} + \binom{k+M+1}{k}.$$

By induction, the right hand side is equal to

$$\left(\sum_{m=0}^M \binom{m+k}{k}\right) + \binom{k+M+1}{k} = \sum_{m=0}^{M+1} \binom{m+k}{k}.$$

(b) Each subset of \mathcal{S} with $k+1$ elements contains a unique maximal element in the interval $[k+1, k+M+1]$. Therefore, the possible maximal elements of such subsets are $k+1+m$, where m runs between 0 and M . Now if we fix a number $k+1+m$, then the number of subsets of \mathcal{S} with $k+1+m$ as its maximal element is equal to the number of subset of $\{1, \dots, k+m\}$ with k elements. This number is equal to

$$\binom{m+k}{k}.$$

As we sum of the m , we therefore obtain that

$$\sum_{m=0}^M \binom{m+k}{k}$$

is equal to the number of subset of \mathcal{S} with $k+1$ elements which is

$$\binom{k+M+1}{k+1}.$$

(c) Let $f_k(z)$ be the function $1/(1-z)^{k+1}$. Then Taylor's theorem implies that for $|z| < 1$,

$$f_k(z) = \sum_{n=0}^{\infty} f_k^{(n)}(0) \frac{z^n}{n!}.$$

On the other hand, an induction shows that

$$f_k^{(n)}(z) = \frac{(k+1)(k+1)\cdots(k+n)}{(1-z)^{k+1+n}}.$$

Therefore, Taylor's theorem shows that

$$1/(1-z)^{k+1} = \sum_{n=0}^{\infty} \binom{k+n}{n} z^n.$$

Now multiplying out the expression

$$(1+z+z^2+\cdots)\left(\sum_{n=0}^{\infty} \binom{k+n}{n} z^n\right)$$

we see that the coefficient of z^M is equal to $\sum_{m=0}^M \binom{m+k}{k}$. On the other hand, the coefficient of z^M in the Taylor series of $f_{k+1}(z)$ is by the above discussion equal to

$$\binom{k+M+1}{k+1}.$$

The equality follows.

2.1 (5) We claim that the congruence $x \equiv 5 \pmod{12}$ is equivalent to the two stated congruences. Certainly, if $x = 5 + 12y$ for some y , then $x \equiv 1 \pmod{4}$ and $x \equiv 2 \pmod{3}$. On the other hand, if x satisfies these two congruences, then we can write $x = 1 + 4a$ for some a . Hence $1 + 4a \equiv 2 \pmod{3}$, and hence $a \equiv 1 \pmod{3}$. Therefore, $a = 1 + 3b$ for some b . We therefore find that $x = 1 + 4(1 + 3b) = 5 + 12b$, and so $x \equiv 5 \pmod{12}$.

2.1 (6) If $a^2 \equiv b^2 \pmod{p}$, then $p|(a^2 - b^2)$ and so p divides $(a-b)(a+b)$. Since p is prime, this implies that p divides either $a+b$ or $a-b$.

2.1 (10) 1,1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4.

2.1 (12) By contradiction. If $19|4n^2+4$, then $4(n^2+1) \equiv 0 \pmod{19}$. Since $(4, 19) = 1$, this implies that $n^2+1 \equiv 0 \pmod{19}$. This implies that -1 is a square mod 19 which contradicts 2.12.