

MATH 113 FALL 2000, HOMEWORK 5

ALLEN KNUTSON

p115 #9. $(12)(478)(21)(72815) = \dots$ let's just follow 1 to get the idea;

$$(12)(478)(21)(72815) \cdot 1 = (12)(478)(21) \cdot 5 = (12)(478) \cdot 5 = (12) \cdot 5 = 5$$

and where does 5 go?

$$(12)(478)(21)(72815) \cdot 5 = (12)(478)(21) \cdot 7 = (12)(478) \cdot 7 = (12) \cdot 8 = 8$$

etc. In all, $(158)(247)$, with 3, 5, 6 not moved by anything.

#10. If π 's values on 12345678 are 82637451, then in cycles, $\pi = (18)(2)(364)(57)$. Writing this out in transpositions, all we need to break up is $(364) = (36)(64)$. So $\pi = (18)(36)(64)(57)$.

#14-18. The order of an element of S_n is the least common multiple of the cycle lengths; we studied this way back when first thinking about the orders of graph automorphisms.

So these questions are about writing a number n as a sum of smaller numbers so as to maximize the LCM. Obviously it doesn't help to use two summands that have a GCD more than 1 – we can divide one of them by the GCD and not change the overall LCM.

Also, we can replace any number by the prime powers (like 16 or 27) dividing it (and pad out what's left over with 1s), so it's enough to think about writing n as a sum of prime powers.

Let's see 15 in detail. The largest prime we could use is 13, leaving 2 over, for $\text{lcm} = 26$. If we use 11, then there's 4 left over, getting 44. If we use 7, there's 8 left over, and the best way to use those is as $3+5$ for $3 \cdot 5 \cdot 7 = 105$ in all.

If the largest prime we use is 5, there's $15-5=10$ left over to use on 2s and 3s. The best use is $1+1+1+3+4$, but obviously this isn't as good as putting the $1+1+1+4$ together into a 7 as we did above.

Coming down to the wire, if the largest prime we use is 3, we could either look at $15 = 3+8+1+1+1+1$ or $15 = 9+4+1+1$. And if we only use powers of 2, the best we can do is $15=8$ plus seven 1s. So 105 is the winner.

In total, the best are

- $5 = 2 + 3$ with LCM 6
- $6 = 2 + 3 + 1$ with LCM 6 (or $6 = 6$ is just as good)
- $7 = 3 + 4$ with LCM 12
- $10 = 2 + 3 + 5$ with LCM 30
- $15 = 3 + 5 + 7$ with LCM 105

(A much more serious challenge: if $f(n)$ = the maximal order of an element in S_n , show $\log f(n) / \sqrt{n \log n}$ goes to 1 as n goes to infinity.)

#26,30. We'll do both of these as one. Let H be a subgroup of S_n containing an odd permutation σ . Let $E = H \cap A_n$ be the even permutations in H . Then we claim

1. $H = E \cup E\sigma$
2. E and $E\sigma$ have the same size.

The first is because if $\tau \in H$ but $\tau \notin E$, then τ is odd, so $\tau\sigma^{-1}$ is even, so $\tau\sigma^{-1} \in E$. Therefore $\tau \in E\sigma$.

The second is because $E\sigma$ is a left coset of E , so they have the same size. (We proved this before; the proof consisted of showing “multiply by σ ” was a 1:1 correspondence of E and $E\sigma$.)

#30. This is the case $H = S_n (n > 1)$.

#26. Either H has all even permutations, or it doesn't, in which case we apply the above.

Q. Let p be prime, $G = \{1, \dots, p-1\}$ under multiplication mod p . Show G is a group.

We need to know that multiplication is well-defined on here (if it is, it's certainly associative), has an identity (yes: 1), and inverses. The well-definedness is because $p \nmid a, p \nmid b$ implies $p \nmid ab$.

Inverses are trickier. Consider the map $\hat{n} : G \rightarrow G$ that multiplies by $n \pmod p$, for $n \in G$. We claim this map is 1 : 1. If $na \equiv nb \pmod p$, $n(a-b) \equiv 0 \pmod p$, so $p \mid n(a-b)$. But $p \nmid n$, so $p \mid a-b$. In particular $a \equiv b \pmod p$, i.e. $a = b$ as elements of G .

Since it's 1:1, it's onto, because G is finite. (This wouldn't have worked on \mathbb{Z} – doubling is 1:1 but not onto.) So it hits 1. Therefore for any $n \in G$, there exists an m such that $nm \equiv 1$; so inverses exist and G is therefore a group.

Q. If p prime, $p \nmid n$, show $n^p \equiv n \pmod p$.

We'll show $n^{p-1} \equiv 1 \pmod p$ (and then multiply both sides by n). Regarding this as an equation in G , this says that the order of the group element n divides $p-1$, the order of the group G . But we know this is true for any element of any finite group.

(Here's another proof avoiding explicit mention of groups, just for your cultural benefit. String together p beads of n colors; there are n^p different such strings of beads. If you close them up to form necklaces, not all the necklaces are different, because some will be rotations of others. Each necklace is either monochromatic, or can be rotated to exactly $p-1$ other necklaces, *since p is prime*. So n^p equals the number of monochromatic necklaces plus p times the number of polychromatic necklaces. Hence mod p , $n^p \equiv n$.)

#30. Look back up at #26.