Groups and Group Actions, Sheet 4, HT2020

Pudding

I would really appreciate feedback on ways in which these comments and solutions could be improved and made more helpful, so please let me know about typos (however trivial), mistakes, alternative solutions, or additional comments that might be useful.

I'm not going to give full details/proofs for every question, but hopefully I'll give something useful against which you can compare your thinking.

Vicky Neale (vicky.neale@maths)

P1. Let $F = 2^{32} + 1$. Let p be a prime dividing F. What is the order of 2 in $\mathbb{Z}_p^*$? Deduce that $p \equiv 1 \pmod{64}$. Use this to show that F is not prime.

If $p \mid F$, then $F \equiv 0 \pmod{p}$, so $2^{32} \equiv -1 \pmod{p}$. Squaring both sides gives $2^{64} \equiv 1 \pmod{p}$, which means that the order of 2 in $\mathbb{Z}_p^*$ divides 64. But since 2^{32} is not 1 in $\mathbb{Z}_p^*$, the order does not divide 32, so in fact the order of 2 in $\mathbb{Z}_p^*$ is exactly 64.

Now Fermat's Little Theorem (since p is prime and 2 is certainly coprime to p) tells us that $2^{p-1} \equiv 1 \pmod{p}$, and hence the order of 2 in $\mathbb{Z}_p^*$ divides $p - 1$, so $p \equiv 1 \pmod{64}$.

This significantly shrinks the pool of potential prime factors of F, so we can just go through and check. We find that $F = 4294967297$, and if we check numbers of the form $1 + 64k$ for $k \geqslant 1$ (even without worrying whether these numbers are prime), we find that 641 is a factor of F, and so F is not prime.

The number F in this question is a Fermat number: it is of the form $2^{2^n}+1$. In fact it is the smallest Fermat number not to be a prime. This has an interesting history, and you can read more about it at `http://mathshistory.st-andrews.ac.uk/HistTopics/Prime_numbers.html` and `https://www.mathpages.c`

P2. We say that $n \geqslant 2$ is a *Carmichael number* if n is not prime and $a^{n-1} \equiv 1 \pmod{n}$ for all a coprime to n. Show that if $n = (6k+1)(12k+1)(18k+1)$ where k is a positive integer such that $6k+1$, $12k+1$ and $18k+1$ are all prime, then n is a Carmichael number. Use this construction to find two Carmichael numbers.

Take $n = (6k+1)(12k+1)(18k+1)$ where $6k+1$, $12k+1$ and $18k+1$ are all prime. Take a coprime to n.

Then certainly a is coprime to $6k+1$, to $12k+1$ and to $18k+1$, and so by Fermat's Little Theorem we have

$$\begin{aligned} a^{6k} &\equiv 1 \pmod{6k+1} \\ a^{12k} &\equiv 1 \pmod{12k+1} \\ a^{18k} &\equiv 1 \pmod{18k+1}. \end{aligned}$$

Thus $a^{36k} \equiv 1 \pmod{p}$ where p is each of the primes $6k+1$, $12k+1$ and $18k+1$.

A quick piece of algebra shows that $36k$ divides $n-1$, and so $a^{n-1} \equiv 1 \pmod{p}$ where p is each of the three primes.

Now $6k+1$, $12k+1$ and $18k+1$ are pairwise coprime and each divide $a^{n-1}-1$, so their product divides $a^{n-1}-1$, so $a^{n-1} \equiv 1 \pmod{n}$.

This shows that n is a Carmichael number.

Taking $k = 1, 6$ (where happily the factors all turn out to be prime) gives the Carmichael numbers $7 \times 13 \times 19 = 1729$ and $37 \times 73 \times 109 = 291708$.

There are many interesting things to say about Carmichael numbers. A very readable place to start would be this article by Andrew Granville (one of the three mathematicians who, in 1992, proved that there are infinitely many Carmichael numbers) `https://dms.umontreal.ca/~andrew/PDF/Notices1.pdf`.

P3. Let G be a group of order n with a subgroup H of order $n-1$. What can you say about n?

By Lagrange's Theorem, we see that $n-1 \mid n$. But then $n-1$ divides both $n-1$ and n, so it divides their difference $n-(n-1) = 1$. Since $n-1 \geqslant 1$, we see that in fact $n-1 = 1$, so $n = 2$.

This tells us that G is isomorphic to C_2, which is (up to isomorphism) the only group of order 2.