MATHS 255

## Collaborative Tutorial 19/5/03

- 1. Suppose  $x^n = x^{n+k}$ . Then  $x^n x^k = x^n$ , so multiplying by  $x^{-n}$  gives  $x^k = e$ . Conversely, suppose  $x^k = e$ . Then  $x^{n+k} = x^n x^k = x^n e = x^n$ .
- **2.** Suppose G is finite. Let  $x \in G$ . Then the elements  $x^n$  for  $n \in \mathbb{N}$  cannot all be different, so there exist  $n, m \in \mathbb{N}$  with n < m and  $x^n = x^m$ . Since n < m, there is some k with n + k = m. Then  $x^n + k = x^n$ , so  $x^k = e$  by the previous question.
- **3.** We must check that  $e \in \langle x \rangle$ , that if  $g, h \in \langle x \rangle$  then  $gh \in \langle x \rangle$ , and that if  $g \in \langle x \rangle$  then  $g^{-1} \in \langle x \rangle$ .
  - $e = x^0 \in \langle x \rangle$ .
  - if  $g, h \in \langle x \rangle$  then  $g = x^n$ ,  $h = x^m$  for some  $n, m \in \mathbb{Z}$ . But then  $gh = x^{m+n} \in \langle x \rangle$ .
  - if  $g \in \langle x \rangle$  then  $g = x^n$  for some  $n \in \mathbb{Z}$ , so  $g^{-1} = (x^n)^{-1} = x^{-n} \in \langle x \rangle$ .
- **4.** Suppose that  $x^n = e$ . Put k = o(x). Divide k into n, to get n = qk + r where  $0 \le r < k$ . Now, we have

$$e = x^n = x^{qk+r} = x^{qk}x^r = (x^k)^q x^r = e^q x^r = x^r,$$

so  $x^r = e$ . Since k was the least natural number with  $x^k = e$ , and r < k, we must have r = 0, so n = qk, so  $k \mid n$ .

5. We wish to know how many distinct values  $x^n$  can take. Well, we have

$$\begin{aligned} x^n &= x^m \iff x^{n-m} = e \\ &\iff o(x) \mid n-m \\ &\iff n \equiv m \pmod{o(x)}. \end{aligned}$$

Thus the number of distinct values is the same as the number of congruence classes modulo o(x), which is precisely o(x).

From Qustion 3, we know that  $\langle x \rangle$  is a subgroup of G, so by Lagrang's Theorem  $|\langle x \rangle| | o(G)$ , so since  $|\langle x \rangle| = o(x)$  we have o(x) | o(G).