1. How many subgroups does $\mathbf{Z}_{30}$ have? $\mathbf{Z}_{32}$?

There is a 1-1 correspondence between subgroups of a cyclic group and divisors of its order. Thus, $\mathbb{Z}_{30}$ has 8 subgroups and $\mathbb{Z}_{32}$ has 6.

```
> map(numtheory[divisors],[30,32]);
                [{1, 2, 3, 5, 6, 10, 15, 30}, {1, 2, 4, 8, 16, 32}]
```

2. Are there elements of order 20 in the symmetric group S_{10}? Exhibit one or explain why there aren't any. How about elements of order 21? 23? 25? 30?

Since disjoint cycles commute, the order of a product of disjoint cycles is the l.c.m. of the orders of the cycles (= their lengths).

20: $(12345)(6789)$

21: $(1234567)(8\,9\,10)$

23: None. The largest cycles have length 10.

25: None. You'd need a 25-cycle for this.

30: $(12345)(678)(9\,10)$

3. Suppose G is a multiplicative group, $a \in G$. Prove that $a^n = e \Leftrightarrow |a|$ divides n.

$\Leftarrow$ Suppose $|a|$ divides n. Then $n = |a|q$ for some q, so $a^n = a^{|a|q} = (a^{|a|})^q = e^q = e$ ☺

$\Rightarrow$ By the division algorithm $\exists\, q, r$ with

$n = |a|q + r \qquad 0 \le r < |a|$

then $e = a^n = a^{|a|q+r} = (a^{|a|})^q a^r = e^q a^r = a^r$

If r were positive, then by definition of $|a|$ we'd have $|a| \le r$. ☹ Thus $r = 0$ ☺

4. Suppose G is a multiplicative group, $a \in G$. Prove that $a^{|G|} = e$. What conclusion can you draw about $|a|$, if $a \neq e$ and $|G|$ is prime? Explain.

By Lagrange's theorem $|a| = |\langle a \rangle|$ divides $|G|$ so by #3 $a^{|G|} = e$.

If $|G|$ is prime and $|a| \neq 1$ we must have $|a| = |G|$. By the way, this means $G = \langle a \rangle$.

5. Prove that $H = \{1, i, -1, -i\}$ is a multiplicative subgroup of the unit circle in the complex plane. Find two nontrivial cosets of H in the multiplicative group of all nonzero complex numbers $\mathbf{C}^*$ — one coset that is a subset of the unit circle and one not. Sketch H and the two cosets you found. How many distinct cosets does H have in $\mathbf{C}^*$?

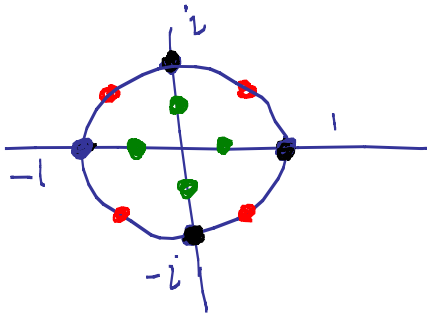
Let $z_1 = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}$, $z_2 = \frac{1}{2}$

$z_1 H = \left\{ \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}} \right\}$

$z_2 H = \left\{ \frac{1}{2}, i\frac{1}{2}, -\frac{1}{2}, -i\frac{1}{2} \right\}$.

By inspection all points in $z_1 H$ lie on the unit circle.

Sketch



H has infinitely many cosets in $\mathbf{C}^*$

```
> pcp:=z->[Re(z),Im(z)];
```

$$pcp := z \to [\Re(z), \Im(z)]$$

```
> H:=[1,I,-1,-I];
```

$$H := [1, I, -1, -I]$$

```
> z1:=(1+I)/sqrt(2); z2:=1/2;
```

$$z1 := \left(\frac{1}{2} + \frac{1}{2}I\right)\sqrt{2}$$

$$z2 := \frac{1}{2}$$

```
> H1:=map(t->z1*t,H);
  H2:=map(t->z2*t,H);
```

$$H1 := \left[\left(\frac{1}{2} + \frac{1}{2}I\right)\sqrt{2}, \left(\frac{-1}{2} + \frac{1}{2}I\right)\sqrt{2}, \left(\frac{-1}{2} - \frac{1}{2}I\right)\sqrt{2}, \left(\frac{1}{2} - \frac{1}{2}I\right)\sqrt{2}\right]$$

$$H2 := \left[\frac{1}{2}, \frac{1}{2}I, \frac{-1}{2}, \frac{-1}{2}I\right]$$

```
> po:=style=point,symbol=circle,symbolsize=12:
  pH:=plot(map(pcp,H),po,color=blue):
  pH1:=plot(map(pcp,H1),po,color=red):
  pH2:=plot(map(pcp,H2),po,color=green):
  plots[display]({pH,pH1,pH2});
```