1. (a) $n! = n(n-1)(n-2)\dots 2\cdot 1$ so $5! = 5\cdot 4\cdot 3\cdot 2\cdot 1 = 120$. What are the prime factors of 12!.
   (b) Show $2|(n^2-n)$.
   (c) Show the numbers $6k+5$ and $7k+6$ are co-prime for every $k\geq 1$.

   Answer: a: So

$$\begin{aligned} 12! &= 12\cdot 11\cdot 10\cdot 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2 \\ &= 3\cdot 2^2\cdot 11\cdot 2\cdot 5\cdot 3^2\cdot 2^3\cdot 7\cdot 2\cdot 3\cdot 5\cdot 2^2\cdot 3\cdot 2 \\ &= 3^5\cdot 2^8\cdot 5^2\cdot 7\cdot 11 \end{aligned} \tag{1}$$

   b: Well $n^2-n = n(n-1)$ and one of those has to be even. c: Say $a|6k+5$ so $6k+5 = ra$ for some r and hence

$$7k+6 = k+1+ra \tag{2}$$

   So $a|7k+6$ only if $a|k+1$, now $a|6k+5$ and $a|k+1$ means $a|k$ which in turn means $a|1$. There might be a more elegant way of doing this, but this way is one way.

2. Let p be an odd prime. Find the values of x so that it is its own inverse modulo p.

   Answer: If x is its own inverse $x^2\equiv 1$ or $x^2-1\equiv 0$. Hence $p|x^2-1$ or $p|(x+1)(x-1)$, since p is prime that means $p|(x+1)$ or $p|(x-1)$ giving $x=1$ or $x=p-1$.

3. Use Euler's theorem to compute
   (a) $3^{340} \pmod{341}$
   (b) $7^{8^9} \pmod{100}$
   (c) $2^{10000} \pmod{121}$

   Answer: Now

$$341 = 11\cdot 31 \tag{3}$$

   so $\phi(341) = 300$ and hence

$$3^{340}\equiv 3^{40} \tag{4}$$

   which is still a little too big for a calculator and so we need to beat it down a bit further. $3^6 = 729\equiv 47$ so

$$3^{40} = (3^6)^6 3^4 \equiv 47^6 3^4 \tag{5}$$

   Now $47^2 =\equiv 163$ so we get

$$29^6 3^4 \equiv 163^3 3^4 = 3(3*163)^3 = 3(148)^3 = 56 \tag{6}$$

   Next, $\phi(100) = 40$ so we actually need to find $8^9 \pmod{40}$ first, since $8^3\equiv 32 \pmod{40}$ this gives

$$32^3 = 2^{15} = 2^6 2^9 \equiv 2^{11} = 2^2 2^9 \equiv 2^2 2^5 \equiv 8 \tag{7}$$

all mod 40, so now we want $7^8 \pmod{100}$ and this is one. Finally $\phi(121) = 110$ so we want 10000 mod 110 which is 100. Now $2^7 \equiv 7$ mod 121. hence

$$2^{100} = (2^7)^{14}4 \equiv 7^{14}2^2 \equiv 101^4 14^2 \equiv 67. \tag{8}$$

4. A subgroup of a group is a subset of the group that is a group, the main thing to check is that the subset is closed. Now, using the notation in the lecture notes $\{e, a\}$ in the Z_4 group is not a subgroup since $a^2 = c$ so it isn't closed. Can you find a Z_2 subgroup of Z_4? What about V_4? It has three Z_2 subgroups.

   Answer: Unlike a, the element $c^2 = e$ so $\{e, c\}$ is a Z_2 subgroup. In V_4 all the elements square to the identity, so $\{e, a\}$, $\{e, b\}$ and $\{e, c\}$ are all Z_2 subgroups.