

## If $p$ is prime, how do we find $\alpha \in \mathbb{F}_p^*$ of large prime order?

Exercise 1.33 gives a reliable way to find such an  $\alpha$  in general. This problem looks at a specific case.

1. Use Mathematica to verify that  $p = 415643$  is prime.
2. Verify that  $q = 207821$  is prime and that  $q \mid (p - 1)$ . What is  $\frac{p-1}{q}$ ?
3. What are all of the possible orders of elements in  $\mathbb{F}_p^*$ ?
4. Let  $a = 6$ , and compute  $a^2 \pmod p$  and  $a^q \pmod p$ .  
Use your answers to determine  $\text{ord}(a)$  in  $\mathbb{F}_p^*$ .
5. Repeat (d) with  $a = 9$  and  $a = 415642$ .
6. Find  $\text{ord}(a^2)$  in  $\mathbb{F}_p^*$  for the following values of  $a$ :

$$a = 6, \quad a = 9, \quad a = 100000, \quad a = 415642$$

Pick a few more random values of  $a$  and find  $\text{ord}(a^2)$  in  $\mathbb{F}_p^*$ .