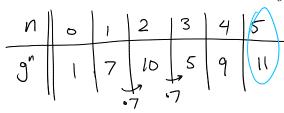
**Directions:** Show all work. No credit for answers without work.

1. [2 points] Let p = 13 and g = 7. Find  $\log_q(11)$  in  $\mathbb{F}_p$ .



2. [2 points] Let p=3167 and g=7; note that p is prime. Given that in  $\mathbb{F}_p$ , we have  $\log_q(2)=786$  and  $\log_q(3)=953$ , find  $\log_q(12)$ .

Grien: 
$$g^{786} = 2$$
 and  $g^{963} = 3$ , we have that
$$12 = 2^{2} \cdot 3 = (g^{786})^{2} \cdot g^{953} = g^{(2.786) + 953}$$

- 3. [2 parts, 3 points each] Alice and Bob use the Diffie-Hellman key exchange protocol with p = 179 and g = 2.
  - (a) Alice picks a = 33 as her private number. What should she send to Bob?

New 
$$A = g^{\alpha} = 2^{33}$$
 $2^{2} = 4$ 
 $2^{4} = 4 \cdot 4 = 16$ 
 $2^{8} = 16 \cdot 16 = 256 = 77$ 
 $2^{16} = 77 \cdot 77 = 22$ 
 $2^{32} = 92 \cdot 22 = 126$ 

S. 
$$A = 2^{33} = 2^{32} \cdot 2$$
  
=  $(26) \cdot 2 = 252 = 73$ 

(b) Alice receives B=145 from Bob. What is their shared secret?

The shared secret is  $B^q = (145)^{33}$ 

$$(145)^2 = 82$$
  
 $(145)^4 = 82.82 = 10$   
 $(145)^8 = (0|-10| = 177$   
 $(145)^{16} = 177.177 = 4$   
 $(145)^{32} = 4.4 = 16$ 

So 
$$B^{9} = (145)^{33}$$

$$= (145)^{32} \cdot 145$$

$$= 16 \cdot 145$$

$$= 172$$