

We will use these earlier facts extensively:

- For prime p , Z_p^* always has a generator (never mind how you get it, but you can always say *pick a generator of Z_p^**).
- For prime p ,
 - For every a in Z_p^* , $a^{p-1} = 1 \pmod p$
 - For generator g , of course $g^{p-1} = 1 \pmod p$ but actually $g^k = 1 \pmod p$ for any $1 \leq k < p-1$ i.e. generator does not reach 1 before $p-1$.
 - For odd p , $g^{\frac{p-1}{2}} = -1 \pmod p$.
- Remember you can write *every number* in Z_p^* as $g^{\text{something}} \pmod p$
- If $g^a = g^b \pmod p$, then $a = b \pmod{p-1}$
- For a in Z_p^* , a can be written in terms of g i.e. $a = g^i \pmod p$ for some i . Then, a is a square iff i is even (i.e. if a is square, then i is even and vice versa and if a is not a square then i is odd and vice versa).

1. Case: If $p = 1 \pmod 4$, then -1 is a square. Since $p = 1 \pmod 4$, $(p-1)/4$ is an integer, so consider $g^{(p-1)/4}$. Since $(g^{(p-1)/4})^2 = g^{(p-1)/2} = -1 \pmod p$, so $g^{(p-1)/4}$ is a square root of -1 .

Case: If -1 is a square, then $p = 1 \pmod 4$. Since -1 is a square, there is some i such that $(g^i)^2 = g^{2i} = -1 \pmod p$. Since $g^{(p-1)/2} = -1 \pmod p$, so $2i = (p-1)/2 \pmod{p-1}$. Since $p-1$ is even, $2i$ is even so $(p-1)/2$ must be even i.e. $4|p-1$ or $p = 1 \pmod 4$.

2.1 Assume $p = 1 \pmod 4$.

Case: If a is a square, then $-a$ is a square. Since a is a square, so $a = g^{2i} \pmod p$ for some i (a is of the form g^{even}). Then $-a = -1 \cdot a = g^{(p-1)/2} g^{2i} \pmod p$. Since $p = 1 \pmod 4$, $(p-1)/2 = 2j$ (even). So, $-a = g^{2j} g^{2i} = g^{2(i+j)} \pmod p$. $2(i+j)$ is even, so $-a$ is a square.

Case: If $-a$ is a square, then a is a square. Same proof, multiply $-a$ by $-1 = g^{(p-1)/2} = g^{\text{even}} \pmod p$.

2.2 Assume $p = 3 \pmod{4}$.

Case: If a is a square, then $-a$ is not a square. As before, $a = g^{2i} \pmod{p}$ and $-a = g^{(p-1)/2} g^{2i} \pmod{p}$. Since $p = 3 \pmod{4}$, $(p-1)/2 = 2j+1$ (odd). Then, $-a = g^{2j+1} g^{2i} = g^{2(i+j)+1} \pmod{p}$. Since $2(i+j)+1$ is odd, so $-a$ is not a square.

Case: If $-a$ is a square, then a is not a square. Similar to above, multiply $-a$ by $g^{(p-1)/2} = g^{\text{odd}} \pmod{p}$.

3 Let a be a square mod p i.e. $a = g^{2i} \pmod{p}$ for some i . Since p is odd, $g^i \pmod{p}$ and $-g^i \pmod{p}$ are distinct and give 1 when squared. So, g^i and $-g^i$ are the two square roots of a . Since $p = 3 \pmod{4}$, so $(p-1)/2 = 2j+1$ (odd). $-g^i = (-1)g^i = g^{(p-1)/2} g^i = g^{2j+1+i} \pmod{p}$. Since i is odd iff $2j+1+i$ is even, so exactly one of i and $2j+1+i$ is even. Thus exactly one of the two square roots of a is a square.

4 Choose any non-square a except -1 . We know that $a = g^{2i+1} \pmod{p}$ for some i (odd exponent). We will use an earlier homework result that *if a and $p-1$ are co-prime and g is a generator for Z_p^* , then g^a is also a generator*. So, we will have to show that $(2i+1)$ is co-prime to $p-1 = 2q$.

Note that $2i+1$ is odd, so not divisible by 2. Also, $1 \leq 2i+1 < p-1 = 2q$, so $q|2i+1$ implies $q = 2i+1$, in which case $g^{2i+1} = g^q = g^{(p-1)/2} = -1 \pmod{p}$. Since we chose $a \neq -1 \pmod{p}$, so this case is not possible either. Hence there is no common factor between $2q$ and $2i+1$, so by the earlier result $a = g^{2i+1}$ is also a generator.