

```
In[194]:= 1 + 1
```

```
Out[194]= 2
```

**We will give examples of solving  $x^2 = a \pmod{p}$   
when we know  $(a/p) = 1$ .**

**The easiest case is when  $p = 3 \pmod{4}$ .**

**Then  $a^{(p+1)/4} \pmod{p}$  is a solution, as is shown in Ex. 25.6**

```
In[195]:=
```

```
p = 36718527505391
```

```
Out[195]= 36718527505391
```

```
In[196]:=
```

```
Mod[p, 4]
```

```
Out[196]= 3
```

**It is easy to get a value of a with  $(a/p) =$**

**1. You can try a random a and check if  $(a/p) = 1$  OR you can take a random b  
and let  $a = b^2 \pmod{p}$   
(which is what I did to get the values of a below).**

```
In[197]:=
```

```
a = 25362520310473
```

```
Out[197]= 25362520310473
```

```
In[198]:=
```

```
JacobiSymbol[a, p]
```

```
Out[198]= 1
```

```
In[199]:=
```

```
PowerMod[a, (p + 1) / 4, p]
```

```
Out[199]= 32387464229719
```

**This should be a solution. We check it.**

```
In[200]:=
```

```
a
```

```
Out[200]= 25362520310473
```

```
In[201]:=
      PowerMod[32387464229719, 2, p]
```

```
Out[201]= 25362520310473
```

**So it is indeed a solution.**

**If  $p$  is congruent to 1 (mod 4),  
then it is congruent to 1 or 5 (mod 8). The next easiest case is  $p = 5$  (mod 8).**

**Ex. 25.7 has you show that one of two possible values will be a solution. More precisely,  
if  $a^{(p-1)/4} = 1 \pmod{p}$  then  $a^{(p+3)/8} \pmod{p}$  will be a solution, and if  
 $a^{(p-1)/4} = -1 \pmod{p}$   
then  $(2a) \pmod{p}$  will be a solution.**

```
In[202]:=
```

```
      p = 2237245427968095333757
```

```
Out[202]= 2237245427968095333757
```

```
In[203]:=
```

```
      Mod[p, 8]
```

```
Out[203]= 5
```

```
In[204]:=
```

```
      a = 495695650312953922152
```

```
Out[204]= 495695650312953922152
```

```
In[205]:=
```

```
      JacobiSymbol[a, p]
```

```
Out[205]= 1
```

```
In[206]:=
```

```
      PowerMod[a, (p - 1) / 4, p]
```

```
Out[206]= 1
```

**So in this case  $a^{(p+3)/8} \pmod{p}$  should be a solution.**

```
In[207]:=
```

```
      PowerMod[a, (p + 3) / 8, p]
```

```
Out[207]= 3583756933101838268
```

**Let ' s check it.**

In[208]:=

**a**

Out[208]= 495695650312953922152

In[209]:=

**PowerMod[3583756933101838268, 2, p]**

Out[209]= 495695650312953922152

**So this is indeed a solution. Let ' s try a different value of a (mod p) with  $p = 5 \pmod{8}$ .**

In[210]:=

**a = 884707196773969056497**

Out[210]= 884707196773969056497

In[211]:=

**JacobiSymbol[a, p]**

Out[211]= 1

In[212]:=

**PowerMod[a, (p - 1) / 4, p]**

Out[212]= 2237245427968095333756

In[213]:=

**p - 1**

Out[213]= 2237245427968095333756

**Since  $a^{(p-1)/4} = -1 \pmod{p}$  the formula :**

**$(2a)(4a)^{(p-5)/8} \pmod{p}$**

**Should be a solution**

In[214]:=

**PowerMod[4 \* a, (p - 5) / 8, p]**

Out[214]= 1199639413493961479180

In[215]:=

**Mod[2 \* a \* 1199639413493961479180, p]**

Out[215]= 2200547322010256055690

**This should be a solution. Let ' s check.**

In[217]:=

**a**

Out[217]= 884707196773969056497

```
In[218]:= PowerMod[2200547322010256055690, 2, p]
```

```
Out[218]= 884707196773969056497
```

**So indeed it works.**

**Now we consider a prime congruent to 1 (mod 8) and apply the algorithm I gave on handout (which is called Tonelli ' s algorithm) to solve  $x^2 = a \pmod{p}$ .**

```
In[219]:=
```

```
    p = 63018038201
```

```
Out[219]= 63018038201
```

```
In[220]:=
```

```
    Mod[63018038201, 8]
```

```
Out[220]= 1
```

```
In[221]:=
```

```
    a = 15598430872
```

```
Out[221]= 15598430872
```

```
In[222]:=
```

```
    JacobiSymbol[a, p]
```

```
Out[222]= 1
```

**First find an integer h with  $(h/p) = -1$ .**

```
In[223]:=
```

```
    JacobiSymbol[3, p]
```

```
Out[223]= -1
```

**h = 3 will work. Of course I could have tried a random h as well.**

```
In[224]:=
```

```
    h = 3
```

```
Out[224]= 3
```

**At the start I set  $e1 = (p - 1) / 2$  and  $e2 = p - 1$ .**

```
In[225]:=
```

```
    e1 = (p - 1) / 2
```

```
Out[225]= 31509019100
```

```
In[226]:=
      e2 = p - 1
```

```
Out[226]= 63018038200
```

**Now compute  $a^{(e1/2)} * h^{(e2/2)} \pmod{p}$**

```
In[227]:=
      PowerMod[a, e1 / 2, p]
```

```
Out[227]= 1
```

```
In[228]:=
      PowerMod[h, e2 / 2, p]
```

```
Out[228]= 63018038200
```

**So  $a^{(e1/2)} * h^{(e2/2)} = -1 \pmod{p}$ .  
Hence my new  $e1 = e1 / 2$  while my new  
 $e2 = e2 / 2 + (p - 1) / 2 \pmod{p - 1}$**

```
In[229]:=
      e1 = e1 / 2
```

```
Out[229]= 15754509550
```

```
In[230]:=
      e2 = Mod[e2 / 2 + (p - 1) / 2, p - 1]
```

```
Out[230]= 0
```

**Note  $e1$  is still even so we continue the algorithm.**

```
In[231]:=
      PowerMod[a, e1 / 2, p]
```

```
Out[231]= 63018038200
```

```
In[232]:=
      PowerMod[a, e2 / 2, p]
```

```
Out[232]= 1
```

**So  $a^{(e1/2)} * h^{(e2/2)} = -1 \pmod{p}$   
once again so my new  
 $e1 = e1 / 2$  while my new  $e2 = e2 / 2 + (p - 1) / 2$ .**

```
In[233]:=
      e1 = e1 / 2
```

```
Out[233]= 7877254775
```

```
In[234]:=  
e2 = Mod[e2 / 2 + (p - 1) / 2, p - 1]
```

```
Out[234]= 31509019100
```

**My solution should now be  $a^{(m+1)} * h^{(e2/2)} \pmod{p}$  where  $e1 = 2 * m + 1$ .**

```
In[235]:=  
m = (e1 - 1) / 2
```

```
Out[235]= 3938627387
```

```
In[236]:=  
PowerMod[a, m + 1, p]
```

```
Out[236]= 16086169165
```

```
In[237]:=  
PowerMod[h, e2 / 2, p]
```

```
Out[237]= 52523332947
```

**Their product is :**

```
In[238]:=  
Mod[16086169165 * 52523332947, p]
```

```
Out[238]= 14457125918
```

**This should be our answer. Recall**

```
In[239]:=  
a
```

```
Out[239]= 15598430872
```

```
In[240]:=  
PowerMod[14457125918, 2, p]
```

```
Out[240]= 15598430872
```

**Indeed it works.**