```
In[4]:= << NumberTheory`NumberTheoryFunctions`
```

Choose a six digit prime ...

```
In[19]:= p = 100981

Out[19]= 100981
```

... such that p - 1 has small factors :

```
In[21]:= FactorInteger[p - 1]

Out[21]= {{2, 2}, {3, 3}, {5, 1}, {11, 1}, {17, 1}}
```

7 is a primitive root mod p :

```
In[56]:= alpha = 7

Out[56]= 7

In[57]:= PowerMod[alpha, (p - 1) / 2, p]

Out[57]= 100980

In[58]:= PowerMod[alpha, (p - 1) / 3, p]

Out[58]= 39995

In[59]:= PowerMod[alpha, (p - 1) / 5, p]

Out[59]= 45195

In[60]:= PowerMod[alpha, (p - 1) / 11, p]

Out[60]= 62356

In[61]:= PowerMod[alpha, (p - 1) / 17, p]

Out[61]= 84576
```

Compute alpha inverse for later use :

```
In[76]:= alpha ' = PowerMod[alpha, -1, p]

Out[76]= 14426
```

What ' s the discrete log of b to the base 2 ? Call it a.

```
In[77]:= b = 54321

Out[77]= 54321
```

```
In[78]:= PowerMod[b, (p - 1) / 2, p]

Out[78]= 100980
```

So a is congruent to 1 mod 2.

```
In[79]:= b1 = Mod[b * alpha ', p]

Out[79]= 22186

In[80]:= PowerMod[b1, (p - 1) / 4, p]

Out[80]= 1
```

Thus a is congruent to 1 mod 4.

Now look at a mod powers of 3.

```
In[97]:= Do[Print[PowerMod[7, i * (p - 1) / 3, p]], {i, 0, 2}]

1

39995

60985

In[82]:= PowerMod[b, (p - 1) / 3, p]

Out[82]= 1

In[83]:= PowerMod[b, (p - 1) / 9, p]

Out[83]= 39995

In[84]:= b1 = Mod[b * alpha ' ^3, p]

Out[84]= 35487

In[85]:= PowerMod[b1, (p - 1) / 27, p]

Out[85]= 60985
```

So a is congruent to 21 = 0 + 1 * 3 + 2 * 9 modulo 27

```
In[89]:= t = Table[PowerMod[7, i * (p - 1) / 5, p], {i, 1, 5}]

Out[89]= {45195, 45338, 45439, 65989, 1}

In[90]:= Do[If[PowerMod[b, (p - 1) / 5, p] == t[[i]], Print[i]], {i, 1, 5}]

4
```

So a is congruent to 4 mod 5

```
In[91]:= t = Table[PowerMod[7, i * (p - 1) / 11, p], {i, 1, 11}]

Out[91]= {62356, 98312, 89505, 54891, 32201, 19352, 91343, 51784, 74648, 31493, 1}
```

```
In[92]:= Do[If[PowerMod[b, (p - 1) / 11, p] == t[[i]], Print[i]], {i, 1, 11}]

7
```

So a is congruent to 7 mod 11

```
In[93]:= t = Table[PowerMod[7, i * (p - 1) / 17, p], {i, 1, 17}]

Out[93]= {84576, 9660, 67870, 9156, 55548, 88585, 81627,
  18106, 57172, 4868, 16431, 68715, 82309, 38787, 81527, 42910, 1}

In[94]:= Do[If[PowerMod[b, (p - 1) / 17, p] == t[[i]], Print[i]], {i, 1, 17}]

5
```

And a is congruent to 5 mod 17.

```
In[100]:=
ChineseRemainderTheorem[{1, 21, 4, 7, 5}, {4, 27, 5, 11, 17}]

Out[100]=
35229
```

Check :

```
In[101]:=
PowerMod[7, 35229, p]

Out[101]=
54321
```