

We illustrate the method of successive squaring to compute $a^k \pmod{m}$ when k is large. First we'll practice with the example $7^{327} \pmod{853}$, which is also done in the book.

First find the base 2 expansion of k .

```
BaseForm[327, 2]
```

```
1010001112
```

This tells us $327 = 2^8 + 2^6 + 2^2 + 2^1 + 2^0$.

Since the base two expansion has 9 digits, we start with our value a and successively square it \pmod{m} a total of 9 times. We print $\{i - 1, a^{(2^i)} \pmod{m}\}$ for $i = 1$ to $i = 9$.

```
a = 7; Do[Print[{i - 1, a}]; a = Mod[a2, 853], {i, 1, 9}]
```

```
{0, 7}
```

```
{1, 49}
```

```
{2, 695}
```

```
{3, 227}
```

```
{4, 349}
```

```
{5, 675}
```

```
{6, 123}
```

```
{7, 628}
```

```
{8, 298}
```

Now using the base 2 expansion we see we want

$a^{(2^8)} * a^{(2^6)} * a^{(2^2)} * a^{(2^1)} * a^{(2^0)}$

\pmod{m} . So we multiply the numbers corresponding to 8, 6, 2, 1, 0.

```
Mod[298 * 123 * 695 * 49 * 7, 853]
```

```
286
```

So our answer is 286 $\pmod{853}$, which does agree with the book's answer.

We'll do the harder example of $2^{2378} \pmod{2379}$.

```
BaseForm[2378, 2]
```

```
1001010010102
```

```
a = 2; Do[Print[{i - 1, a}]; a = Mod[a2, 2379], {i, 1, 12}]
```

```
{0, 2}
```

```
{1, 4}
```

```
{2, 16}
```

```
{3, 256}
```

```
{4, 1303}
```

```
{5, 1582}
```

```
{6, 16}
```

```
{7, 256}
```

```
{8, 1303}
```

```
{9, 1582}
```

```
{10, 16}
```

```
{11, 256}
```

From the base 2 expansion we compute :

```
Mod[256 * 1303 * 16 * 256 * 4, 2379]
```

```
1330
```

Note that since this is not congruent to 1 (mod 2379) we have that 2379 is not prime.

```
PrimeQ[2379]
```

```
False
```

```
<< NumberTheory`PrimeQ`
```

```
PrimeQCertificate[2379]
```

```
{2, 2378, 2379}
```

The above shows that Mathematica used the same calculation we did, i.e. $2^{2378} \pmod{2379}$ to show that 2379 was not prime.