Recall: we compute

$$2^{2016} \equiv 2^{360} \pmod{1739}$$

Approach 3 (Successive squaring):

Write 360 as a sum of powers of 2:

$$360 = \underset{256}{2^8} + \underset{64}{2^6} + \underset{32}{2^5} + \underset{8}{2^3}$$

Then compute the sequence $a_n \equiv 2^{2^n} \pmod{1739}$

Notice $a_{n+1} \equiv a_n^2 \pmod{1739}$.

n	0	1	2	3	4	5	6	7	8
2^{2^n} mod 1739	2	4	16	256	1193	747	1529	625	1089

Compute

$$2^{360} = 2^{2^8} \cdot 2^{2^6} \cdot 2^{2^5} \cdot 2^{2^3} \equiv 1089 \cdot 1529 \cdot 747 \cdot 256$$

$$\equiv 852 \cdot 1681 \equiv 667 \pmod{1739}.$$

In total this method requires $8+3=11$ (heavy) multiplications.

Approach 4: We work with residues modulo 37 and 47 separately and then use CRT.

By FLT, $2^{36} \equiv 1 \pmod{37} \Rightarrow 2^{360} = (2^{36})^{10} \equiv 1 \pmod{37}$

$2^{46} \equiv 1 \pmod{47} \Rightarrow 2^{360} = 2^{7 \cdot 46 + 38} \equiv 2^{38} \pmod{47}$

We can use successive squarings. That will use $5+2=7$ (light) multiplications.

$2^{38} \equiv 9 \pmod{47}$ (Check!)

Now we solve the system

$$\begin{cases} x \equiv 1 \pmod{37} \\ x \equiv 9 \pmod{47} \end{cases}$$

Use EEA:

$47 = 1 \cdot 37 + 10$

$37 = 3 \cdot 10 + 7$

$10 = 1 \cdot 7 + 3$

$7 = 2 \cdot 3 + 1$

47	37	10	7	3	1
-	-	1	3	1	2
0	1	1	4	5	14
1	0	1	3	4	11

Finally, $1 = -11 \cdot 47 + 14 \cdot 37$.

The answer then is $2^{360} \equiv 1 \cdot (-11) \cdot 47 + 9 \cdot 14 \cdot 37$

$\equiv 4145 \equiv 667 \pmod{1739}$

§9 Computation of k'th roots modulo a number.

Task: Given $a \in \mathbb{Z}$, $k, m \in \mathbb{Z}^+$, find an integer x such that $x^k \equiv a \pmod{m}$.

Important restrictions:

(a) $\gcd(k, \varphi(m)) = 1$.

(b) $\gcd(a, m) = 1$

(In some cases we can drop this restriction, in particular for $m=p$ or $m=pq$ where $p \neq q$ are prime, see "RSA Theorem").

Example: Find cubic root of $18 \pmod{11}$.

$$x^3 \equiv 18 \pmod{11} \equiv 7 \pmod{11}$$

Compose a table of cubes mod 11:

x	0	1	2	3	4	5	6	7	8	9	10
x^3 (mod 11)	0	1	8	5	9	4	7	2	6	3	10

(note that $(-x)^3 \equiv -x^3$).

From the table we see that there is the unique solution $x \equiv 6 \pmod{11}$.

Much more efficient method for computing k'th roots:

(1) Compute $\varphi(m)$

(2) Find integer s,t, $s>0$ such that
$1 = s\cdot k + t\cdot\varphi(m)$ (EEA)

(3) Compute
$x \equiv a^s \pmod{m}$ (successive squaring)

(Indeed $a^1 = a^{sk+t\varphi(m)} = (a^s)^k \cdot (a^{\varphi(m)})^t$
$\equiv [E\text{-}FT] \equiv (a^s)^k \pmod{m}$

In other words $x \equiv a^s \pmod{m}$ satisfies
$x^k \equiv a \pmod{m}$)

Remark: We just provide one solution, we do not show that it is unique. In fact, it is unique, but we will not show that.

Example: $x^{101} \equiv 262 \pmod{667}$.

(1) One can find that $667 = 23\cdot 29$
Then $\varphi(667) = 22\cdot 28 = 616$

(2) Apply EEA,

$616 = 6\cdot 101 + 10$
$101 = 10\cdot 10 + 1$

We can write $1 = 101 - 10\cdot 10 = 101 - 10(616 - 6\cdot 101)$
$= 61\cdot 101 - 10\cdot 616$

(3) Compute $x \equiv 262^{61} \pmod{667}$.

We apply successive squarings (or approach 4) to get

$x \equiv 262^{61} \equiv 233 \pmod{667}$. (Check!)