Notation: for a fixed n, let $\overline{a}$ be the least residue of $a \pmod{n}$, i.e. the unique number between 0 and $n-1$ congruent to a.

Last time: Method of successive squaring

Given x, k, and big n, compute $x^k \pmod{n}$ as follows.

1. If $\gcd(x,n) = 1$, first reduce $k \equiv \bar{k} \pmod{\phi(n)}$, so that by Euler's formula
$$x^k \equiv x^{\bar{k}} \pmod{n}.$$
(since $x^k = x^{m\phi(n)+\overline{k}} = (x^{\phi(n)})^m x^{\overline{k}} \equiv_n 1^m \cdot x^{\overline{k}}$).
2. Decompose $\bar{k}$ (or k if $\gcd(x,n) \neq 1$) into powers of 2:
$$\bar{k} = 2^{a_1} + 2^{a_2} + \cdots + 2^{a_\ell}.$$
3. Use successive squaring (*square, reduce, square, reduce, ...*) to compile a table of data for $x^{2^a} \pmod{n}$, for as many a as you need.
($x = \boxed{x^1}, (x^1)^2 = \boxed{x^2}, (x^2)^2 = \boxed{x^4}, (x^4)^2 = \boxed{x^8}, (x^8)^2 = \boxed{x^{16}} \ldots$)
4. Use your table and your decomposition to compute $x^k \pmod{n}$:
$$x^k \equiv \overline{x^{2^{a_1}}} \cdot \overline{x^{2^{a_2}}} \cdots \overline{x^{2^{a_\ell}}} \pmod{n}.$$

Goal: Reverse the process. Namely, given k, b, and big n, solve $x^k \equiv b \pmod{n}$ for x.

Goal: Reverse the process. Namely, given k, b, and big n, solve $x^k \equiv b \pmod{n}$ for x.

Process: Assume $\gcd(b, n) = 1 = \gcd(k, \phi(n))$.

Goal: Reverse the process. Namely, given k, b, and big n, solve $x^k \equiv b \pmod{n}$ for x.

Process: Assume $\gcd(b, n) = 1 = \gcd(k, \phi(n))$.

1. Compute $\phi(n)$: If $n = p_1^{r_1} \cdots p_\ell^{r_\ell}$, then

$$\phi(n) = p_1^{r_1 - 1}(p_1 - 1) \cdots p_\ell^{r_\ell - 1}(p_\ell - 1).$$

Goal: Reverse the process. Namely, given k, b, and big n, solve $x^k \equiv b \pmod{n}$ for x.

Process: Assume $\gcd(b, n) = 1 = \gcd(k, \phi(n))$.

1. Compute $\phi(n)$: If $n = p_1^{r_1} \cdots p_\ell^{r_\ell}$, then
$$\phi(n) = p_1^{r_1 - 1}(p_1 - 1) \cdots p_\ell^{r_\ell - 1}(p_\ell - 1).$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that
$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}.$$

Goal: Reverse the process. Namely, given k, b, and big n, solve $x^k \equiv b \pmod{n}$ for x.

Process: Assume $\gcd(b, n) = 1 = \gcd(k, \phi(n))$.

1. Compute $\phi(n)$: If $n = p_1^{r_1} \cdots p_\ell^{r_\ell}$, then
$$\phi(n) = p_1^{r_1 - 1}(p_1 - 1) \cdots p_\ell^{r_\ell - 1}(p_\ell - 1).$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that
$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}.$$

3. Compute $b^u \pmod{n}$ by the method of successive squaring.

Goal: Reverse the process. Namely, given k, b, and big n, solve $x^k \equiv b \pmod{n}$ for x.

Process: Assume $\gcd(b, n) = 1 = \gcd(k, \phi(n))$.

1. Compute $\phi(n)$: If $n = p_1^{r_1} \cdots p_\ell^{r_\ell}$, then
$$\phi(n) = p_1^{r_1-1}(p_1 - 1) \cdots p_\ell^{r_\ell-1}(p_\ell - 1).$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that
$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}.$$

3. Compute $b^u \pmod{n}$ by the method of successive squaring.

Then setting $x = \overline{b^u}$, we have
$$x^k = (\overline{b^u})^k$$

Goal: Reverse the process. Namely, given k, b, and big n, solve $x^k \equiv b \pmod{n}$ for x.

Process: Assume $\gcd(b,n) = 1 = \gcd(k,\phi(n))$.

1. Compute $\phi(n)$: If $n = p_1^{r_1} \cdots p_\ell^{r_\ell}$, then
$$\phi(n) = p_1^{r_1-1}(p_1-1)\cdots p_\ell^{r_\ell-1}(p_\ell-1).$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that
$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}.$$

3. Compute $b^u \pmod{n}$ by the method of successive squaring.

Then setting $x = \overline{b^u}$, we have
$$x^k = (\overline{b^u})^k \equiv_n b^{uk}$$

Goal: Reverse the process. Namely, given k, b, and big n, solve $x^k \equiv b \pmod{n}$ for x.

Process: Assume $\gcd(b, n) = 1 = \gcd(k, \phi(n))$.

1. Compute $\phi(n)$: If $n = p_1^{r_1} \cdots p_\ell^{r_\ell}$, then
$$\phi(n) = p_1^{r_1 - 1}(p_1 - 1) \cdots p_\ell^{r_\ell - 1}(p_\ell - 1).$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that
$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}.$$

3. Compute $b^u \pmod{n}$ by the method of successive squaring.

Then setting $x = \overline{b^u}$, we have
$$x^k = (\overline{b^u})^k \equiv_n b^{uk} \equiv_n b^{1 + v\phi(n)}$$

Goal: Reverse the process. Namely, given k, b, and big n, solve $x^k \equiv b \pmod{n}$ for x.

Process: Assume $\gcd(b, n) = 1 = \gcd(k, \phi(n))$.

1. Compute $\phi(n)$: If $n = p_1^{r_1} \cdots p_\ell^{r_\ell}$, then
$$\phi(n) = p_1^{r_1 - 1}(p_1 - 1) \cdots p_\ell^{r_\ell - 1}(p_\ell - 1).$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that
$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}.$$

3. Compute $b^u \pmod{n}$ by the method of successive squaring.

Then setting $x = \overline{b^u}$, we have
$$x^k = (\overline{b^u})^k \equiv_n b^{uk} \equiv_n b^{1+v\phi(n)} = b \cdot (b^{\phi(n)})^v$$

Goal: Reverse the process. Namely, given k, b, and big n, solve $x^k \equiv b \pmod{n}$ for x.

Process: Assume $\gcd(b, n) = 1 = \gcd(k, \phi(n))$.

1. Compute $\phi(n)$: If $n = p_1^{r_1} \cdots p_\ell^{r_\ell}$, then
$$\phi(n) = p_1^{r_1 - 1}(p_1 - 1) \cdots p_\ell^{r_\ell - 1}(p_\ell - 1).$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that
$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}.$$

3. Compute $b^u \pmod{n}$ by the method of successive squaring.

Then setting $x = \overline{b^u}$, we have
$$x^k = (\overline{b^u})^k \equiv_n b^{uk} \equiv_n b^{1+v\phi(n)} = b \cdot (b^{\phi(n)})^v \equiv_n b,$$
as desired.

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.

We have $\gcd(x, 1073) | \gcd(758, 1073) = 1$ ✓

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.
We have $\gcd(x, 1073) | \gcd(758, 1073) = 1$ ✓

1. Compute $\phi(n)$:

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.
We have $\gcd(x, 1073) \mid \gcd(758, 1073) = 1$ ✓

1. Compute $\phi(n)$: Factor n to get $1073 = 29 \cdot 37$.

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.
We have $\gcd(x, 1073) \mid \gcd(758, 1073) = 1$ ✓

1. Compute $\phi(n)$: Factor n to get $1073 = 29 \cdot 37$. So

$$\boxed{\phi(1073) = (29-1)(37-1) = 1008.}$$

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.

We have $\gcd(x, 1073) \mid \gcd(758, 1073) = 1$ ✓

1. Compute $\phi(n)$: Factor n to get $1073 = 29 \cdot 37$. So

$$\boxed{\phi(1073) = (29-1)(37-1) = 1008.}$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that

$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}:$$

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.
We have $\gcd(x, 1073) | \gcd(758, 1073) = 1$ ✓

1. Compute $\phi(n)$: Factor n to get $1073 = 29 \cdot 37$. So

$$\boxed{\phi(1073) = (29-1)(37-1) = 1008.}$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that

$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}:$$

   Using the Eulidean algorithm, we get

$$\begin{aligned}
1008 &= 131 * 7 + 91 \\
131 &= 91 * 1 + 40 \\
91 &= 40 * 2 + 11 \\
40 &= 11 * 3 + 7 \\
11 &= 7 * 1 + 4 \\
7 &= 4 * 1 + 3 \\
4 &= 3 * 1 + 1
\end{aligned}$$

so that

$$\begin{aligned}
1 &= 4 + (-1)3 = 4 + (-1)(7 + (-1)4) \\
&= 2 * 4 + (-1)7 \\
&= 2(11 + (-1)7) + (-1)7 \\
&= \cdots = (-277) * 131 + 36 * 1008.
\end{aligned}$$

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.

We have $\gcd(x, 1073) | \gcd(758, 1073) = 1$ ✓

1. Compute $\phi(n)$: Factor n to get $1073 = 29 \cdot 37$. So

$$\boxed{\phi(1073) = (29-1)(37-1) = 1008.}$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that

$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}:$$

Using the Eulidean algorithm, we get

$$\begin{aligned} 1008 &= 131 * 7 + 91 \\ 131 &= 91 * 1 + 40 \\ 91 &= 40 * 2 + 11 \\ 40 &= 11 * 3 + 7 \\ 11 &= 7 * 1 + 4 \\ 7 &= 4 * 1 + 3 \\ 4 &= 3 * 1 + 1 \end{aligned}$$

so that

$$\begin{aligned} 1 &= 4 + (-1)3 = 4 + (-1)(7 + (-1)4) \\ &= 2 * 4 + (-1)7 \\ &= 2(11 + (-1)7) + (-1)7 \\ &= \cdots = (-277) * 131 + 36 * 1008. \end{aligned}$$

Another solution:

$$1 = (-277 + 1008) * 131 + (36 - 131) * 1008 = 731 * 131 - 95 * 1008.$$

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.

We have $\gcd(x, 1073) | \gcd(758, 1073) = 1$ ✓

1. Compute $\phi(n)$: Factor n to get $1073 = 29 \cdot 37$. So

$$\boxed{\phi(1073) = (29-1)(37-1) = 1008.}$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that

$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}:$$

$$\boxed{1 = 731 * 131 - 95 * 1008}$$

3. Compute $b^u \pmod{n}$ by the method of successive squaring:

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.

We have $\gcd(x, 1073) | \gcd(758, 1073) = 1$ ✓

1. Compute $\phi(n)$: Factor n to get $1073 = 29 \cdot 37$. So

$$\boxed{\phi(1073) = (29 - 1)(37 - 1) = 1008.}$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that

$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}:$$

$$\boxed{1 = 731 * 131 - 95 * 1008}$$

3. Compute $b^u \pmod{n}$ by the method of successive squaring:
   We have $731 = 2^9 + 2^7 + 2^6 + 2^4 + 2^3 + 2^1 + 1$.

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.
We have $\gcd(x, 1073) | \gcd(758, 1073) = 1$ ✓

1. Compute $\phi(n)$: Factor n to get $1073 = 29 \cdot 37$. So
$$\boxed{\phi(1073) = (29-1)(37-1) = 1008.}$$
2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that
$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}:$$
$$\boxed{1 = 731 * 131 - 95 * 1008}$$
3. Compute $b^u \pmod{n}$ by the method of successive squaring:
We have $731 = 2^9 + 2^7 + 2^6 + 2^4 + 2^3 + 2^1 + 1$. So using

a	$\overline{758^{2^{a-1}}}^2$	$\overline{758^{2^a}}$
1	574564	509
2	259081	488
3	238144	1011
4	1022121	625
5	390625	53
6	2809	663
7	439569	712
8	506944	488
9	238144	1011

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.

We have $\gcd(x, 1073) | \gcd(758, 1073) = 1$ ✓

1. Compute $\phi(n)$: Factor n to get $1073 = 29 \cdot 37$. So

$$\boxed{\phi(1073) = (29-1)(37-1) = 1008.}$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that

$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}:$$

$$\boxed{1 = 731 * 131 - 95 * 1008}$$

3. Compute $b^u \pmod{n}$ by the method of successive squaring: We have $731 = 2^9 + 2^7 + 2^6 + 2^4 + 2^3 + 2^1 + 1$. So using

a	$\overline{758^{2^{a-1}}}^2$	$\overline{758^{2^a}}$
1	574564	509
2	259081	488
3	238144	1011
4	1022121	625
5	390625	53
6	2809	663
7	439569	712
8	506944	488
9	238144	1011

we have

$$\begin{aligned} 758^{731} &\equiv_{1073} 758^{2^9} * 758^{2^7} * 758^{2^6} \\ &\qquad * 758^{2^4} * 758^{2^3} * 758^2 * 758 \\ &\equiv_{1073} (1011 * 712 * 663) \\ &\qquad * (625 * 1011) * (509 * 758) \\ &\equiv_{1073} 749 * 951 * 615 \\ &\equiv_{1073} 905. \end{aligned}$$

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.
We have $\gcd(x, 1073) | \gcd(758, 1073) = 1$ ✓

1. Compute $\phi(n)$: Factor n to get $1073 = 29 \cdot 37$. So
$$\boxed{\phi(1073) = (29-1)(37-1) = 1008.}$$
2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that
$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}:$$
$$\boxed{1 = 731 * 131 - 95 * 1008}$$
3. Compute $b^u \pmod{n}$ by the method of successive squaring:
$$\boxed{758^{731} \equiv_{1073} 905.}$$

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.
We have $\gcd(x, 1073) | \gcd(758, 1073) = 1$ ✓

1. Compute $\phi(n)$: Factor n to get $1073 = 29 \cdot 37$. So
$$\boxed{\phi(1073) = (29-1)(37-1) = 1008.}$$
2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that
$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}:$$
$$\boxed{1 = 731 * 131 - 95 * 1008}$$
3. Compute $b^u \pmod{n}$ by the method of successive squaring:
$$\boxed{758^{731} \equiv_{1073} 905.}$$

Then setting $x = 905$, we have
$$905^{131} \equiv_{1073} (758^{731})^{131}$$

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.
We have $\gcd(x, 1073) | \gcd(758, 1073) = 1$ ✓

1. Compute $\phi(n)$: Factor n to get $1073 = 29 \cdot 37$. So
$$\boxed{\phi(1073) = (29-1)(37-1) = 1008.}$$
2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that
$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}:$$
$$\boxed{1 = 731 * 131 - 95 * 1008}$$
3. Compute $b^u \pmod{n}$ by the method of successive squaring:
$$\boxed{758^{731} \equiv_{1073} 905.}$$

Then setting $x = 905$, we have
$$905^{131} \equiv_{1073} (758^{731})^{131} = 758^{731*131}$$

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.
We have $\gcd(x, 1073) | \gcd(758, 1073) = 1$ ✓

1. Compute $\phi(n)$: Factor n to get $1073 = 29 \cdot 37$. So

$$\boxed{\phi(1073) = (29-1)(37-1) = 1008.}$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that

$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}:$$

$$\boxed{1 = 731 * 131 - 95 * 1008}$$

3. Compute $b^u \pmod{n}$ by the method of successive squaring:

$$\boxed{758^{731} \equiv_{1073} 905.}$$

Then setting $x = 905$, we have

$$905^{131} \equiv_{1073} (758^{731})^{131} = 758^{731*131} = 758^{1+95*1008}$$

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.
We have $\gcd(x, 1073) | \gcd(758, 1073) = 1$ ✓

1. Compute $\phi(n)$: Factor n to get $1073 = 29 \cdot 37$. So

$$\boxed{\phi(1073) = (29-1)(37-1) = 1008.}$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that

$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}:$$

$$\boxed{1 = 731 * 131 - 95 * 1008}$$

3. Compute $b^u \pmod{n}$ by the method of successive squaring:

$$\boxed{758^{731} \equiv_{1073} 905.}$$

Then setting $x = 905$, we have

$$905^{131} \equiv_{1073} (758^{731})^{131} = 758^{731*131} = 758^{1+95*1008}$$
$$= 758 \cdot (758^{1008})^{95}$$

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.
We have $\gcd(x, 1073) | \gcd(758, 1073) = 1$ ✓

1. Compute $\phi(n)$: Factor n to get $1073 = 29 \cdot 37$. So

$$\boxed{\phi(1073) = (29-1)(37-1) = 1008.}$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that

$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}:$$

$$\boxed{1 = 731 * 131 - 95 * 1008}$$

3. Compute $b^u \pmod{n}$ by the method of successive squaring:

$$\boxed{758^{731} \equiv_{1073} 905.}$$

Then setting $x = 905$, we have

$$905^{131} \equiv_{1073} (758^{731})^{131} = 758^{731*131} = 758^{1+95*1008}$$
$$= 758 \cdot (758^{1008})^{95} \equiv_{1073} 758,$$

as desired.

Example: Find a solution to $x^{131} \equiv 758 \pmod{1073}$.
We have $\gcd(x, 1073) | \gcd(758, 1073) = 1$ ✓

1. Compute $\phi(n)$: Factor n to get $1073 = 29 \cdot 37$. So

$$\boxed{\phi(1073) = (29 - 1)(37 - 1) = 1008.}$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that

$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}:$$

$$\boxed{1 = 731 * 131 - 95 * 1008}$$

3. Compute $b^u \pmod{n}$ by the method of successive squaring:

$$\boxed{758^{731} \equiv_{1073} 905.}$$

Then setting $x = 905$, we have

$$905^{131} \equiv_{1073} (758^{731})^{131} = 758^{731*131} = 758^{1+95*1008}$$
$$= 758 \cdot (758^{1008})^{95} \equiv_{1073} 758,$$

as desired. So $x = 905$ is a solution to $x^{131} \equiv 758 \pmod{1073}$.

Goal: Reverse the process. Namely, given k, b, and big n, solve $x^k \equiv b \pmod{n}$ for x.

Process: Assume $\gcd(b, n) = 1 = \gcd(k, \phi(n))$.

1. Compute $\phi(n)$: If $n = p_1^{r_1} \cdots p_\ell^{r_\ell}$, then
$$\phi(n) = p_1^{r_1 - 1}(p_1 - 1) \cdots p_\ell^{r_\ell - 1}(p_\ell - 1).$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that
$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}.$$

3. Compute $b^u \pmod{n}$ by the method of successive squaring.

Then setting $x = \overline{b^u}$, we have
$$x^k = (\overline{b^u})^k \equiv_n b^{uk} \equiv_n b^{1+v\phi(n)} = b \cdot (b^{\phi(n)})^v \equiv_n b,$$
as desired.

Goal: Reverse the process. Namely, given k, b, and big n, solve $x^k \equiv b \pmod{n}$ for x.

Process: Assume $\gcd(b, n) = 1 = \gcd(k, \phi(n))$.

1. Compute $\phi(n)$: If $n = p_1^{r_1} \cdots p_\ell^{r_\ell}$, then
$$\phi(n) = p_1^{r_1 - 1}(p_1 - 1) \cdots p_\ell^{r_\ell - 1}(p_\ell - 1).$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that
$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}.$$

3. Compute $b^u \pmod{n}$ by the method of successive squaring.

Then setting $x = \overline{b^u}$, we have
$$x^k = (\overline{b^u})^k \equiv_n b^{uk} \equiv_n b^{1+v\phi(n)} = b \cdot (b^{\phi(n)})^v \equiv_n b,$$
as desired.

How computationally difficult for large n?

Goal: Reverse the process. Namely, given k, b, and big n, solve $x^k \equiv b \pmod{n}$ for x.

Process: Assume $\gcd(b, n) = 1 = \gcd(k, \phi(n))$.

1. Compute $\phi(n)$: If $n = p_1^{r_1} \cdots p_\ell^{r_\ell}$, then
$$\phi(n) = p_1^{r_1 - 1}(p_1 - 1) \cdots p_\ell^{r_\ell - 1}(p_\ell - 1).$$
2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that
$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}.$$
3. Compute $b^u \pmod{n}$ by the method of successive squaring.

(By method of successive squaring, which is "fast".)

Then setting $x = \overline{b^u}$, we have
$$x^k = (\overline{b^u})^k \equiv_n b^{uk} \equiv_n b^{1+v\phi(n)} = b \cdot (b^{\phi(n)})^v \equiv_n b,$$
as desired.

How computationally difficult for large n?

Goal: Reverse the process. Namely, given k, b, and big n, solve $x^k \equiv b \pmod{n}$ for x.

Process: Assume $\gcd(b, n) = 1 = \gcd(k, \phi(n))$.

1. Compute $\phi(n)$: If $n = p_1^{r_1} \cdots p_\ell^{r_\ell}$, then
$$\phi(n) = p_1^{r_1-1}(p_1 - 1) \cdots p_\ell^{r_\ell - 1}(p_\ell - 1).$$

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that
$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}.$$
(By Euclidean algorithm, which is "fast".)

3. Compute $b^u \pmod{n}$ by the method of successive squaring.
(By method of successive squaring, which is "fast".)

Then setting $x = \overline{b^u}$, we have
$$x^k = (\overline{b^u})^k \equiv_n b^{uk} \equiv_n b^{1+v\phi(n)} = b \cdot (b^{\phi(n)})^v \equiv_n b,$$
as desired.

How computationally difficult for large n?

Goal: Reverse the process. Namely, given k, b, and big n, solve $x^k \equiv b \pmod{n}$ for x.

Process: Assume $\gcd(b, n) = 1 = \gcd(k, \phi(n))$.

1. Compute $\phi(n)$: If $n = p_1^{r_1} \cdots p_\ell^{r_\ell}$, then
$$\phi(n) = p_1^{r_1-1}(p_1 - 1) \cdots p_\ell^{r_\ell-1}(p_\ell - 1).$$
(By prime factorization, which is "slow"!!)

2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that
$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}.$$
(By Euclidean algorithm, which is "fast".)

3. Compute $b^u \pmod{n}$ by the method of successive squaring.
(By method of successive squaring, which is "fast".)

Then setting $x = \overline{b^u}$, we have
$$x^k = (\overline{b^u})^k \equiv_n b^{uk} \equiv_n b^{1+v\phi(n)} = b \cdot (b^{\phi(n)})^v \equiv_n b,$$
as desired.

How computationally difficult for large n?

Goal: Reverse the process. Namely, given k, b, and big n, solve $x^k \equiv b \pmod{n}$ for x.

Process: Assume $\gcd(b, n) = 1 = \gcd(k, \phi(n))$.

1. Compute $\phi(n)$: If $n = p_1^{r_1} \cdots p_\ell^{r_\ell}$, then
$$\phi(n) = p_1^{r_1 - 1}(p_1 - 1) \cdots p_\ell^{r_\ell - 1}(p_\ell - 1).$$
(By prime factorization, which is "slow"!!)
2. Find pos. integers u and v satisfying $ku - \phi(n)v = 1$, so that
$$ku \equiv 1 \pmod{\phi(n)}, \qquad \text{i.e. } u = k^{-1} \pmod{\phi(n)}.$$
(By Euclidean algorithm, which is "fast".)
3. Compute $b^u \pmod{n}$ by the method of successive squaring.
(By method of successive squaring, which is "fast".)

Then setting $x = \overline{b^u}$, we have
$$x^k = (\overline{b^u})^k \equiv_n b^{uk} \equiv_n b^{1+v\phi(n)} = b \cdot (b^{\phi(n)})^v \equiv_n b,$$
as desired.

How computationally difficult for large n?

Punchline: If you know the prime factorization of n, this computation is fast ("polynomial time"); if you don't, this computation is slow (for now–see "P versus NP").