More on RSA.

Recall: we write

$$a \equiv b \pmod{m}$$

if $m \mid (a-b)$, meaning $a-b = mq$ for some $q \in \mathbb{Z}$.

[Relevance to RSA: we encode a message n as a message r by writing

$$n^k = mq + r \quad (0 \le r < m) \qquad (*)$$

for given $k, m \in \mathbb{N}$. Note that $(*)$ says

$$n^k - r = mq,$$

so $m \mid (n^k - r)$, so $n^k \equiv r \pmod{m}$.]

Properties of "mod m:"

<u>Proposition.</u>
Let $a, b, c, d, m \in \mathbb{Z}$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
(i) $a + c \equiv b + d \pmod{m}$,
(ii) $a - c \equiv b - d \pmod{m}$,
(iii) $ac \equiv bd \pmod{m}$.

<u>Proof</u> of (i) only (see HW 1 for (ii) and (iii)).
Suppose $a, b, c, d, m \in \mathbb{Z}$, $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$.
Then $m \mid (a-b)$ and $m \mid (c-d)$, so $a - b = mq$ and $c - d = ms$ for some $q, s \in \mathbb{Z}$.
But then

$$(a+c)-(b+d) = (a-b)+(c-d)$$
$$= mq+ms$$
$$= m(q+s),$$

so $m \mid ((a+c)-(b+d))$, so $a+c \equiv b+d \pmod{m}$.

So, for $a,b,c,d,m \in \mathbb{Z}$, $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m} \Rightarrow a+b \equiv c+d \pmod{m}$. $\square$

"implies"

Example: Since $12 \equiv 5 \pmod{7}$, $21 \equiv 14 \pmod{7}$, $7 \equiv 0 \pmod{7}$, and $776 \equiv 6 \pmod{7}$, we can conclude that

$$12(21-7)+776 \equiv 5(14-0)+6 \pmod{7}.$$

(DIY: check this.)

Back to RSA: AGAIN, to encode a numerized message n, given $k, m \in \mathbb{N}$, we write

$$n^k = m \cdot q + r \quad (0 \le r < m).$$

Then r <u>is</u> the coded message.

SO: we need to find an r with $0 \le r < m$ <u>and</u> with $n^k \equiv r \pmod{m}$. This is called "reducing $n^k \pmod{m}$."

Q: How do we do this?
A: "Successive squaring."

<u>Example:</u> reduce $12^7 \pmod{35}$.

Solution:

Step 1: first, we find the binary expansion of the exponent 7 (express 7 as a sum of powers of 2). We have

$$7 = 4 + 2 + 1.$$

Step 2: Raise the base 12 to successive powers of 2, reducing (mod 35) along the way, and using each computation to help with the next one. Like this:

$$\begin{aligned} 12^1 &\equiv 12 \pmod{35} \\ 12^2 &= 144 = 35\cdot 4 + 4 \equiv 4 \pmod{35} \\ 12^4 &= (12^2)^2 \equiv 4^2 \equiv 16 \pmod{35}. \end{aligned}$$

[Stop at the highest power of 2 from Step 1.]

Step 3. Combine Steps 1 and 2, reducing along the way, to compute $12^7 \pmod{35}$.

Like this:

$$\begin{aligned} 12^7 &= 12^{4+2+1} \\ &= 12^4 \cdot 12^2 \cdot 12^1 \\ &= 16\cdot 4\cdot 12 \\ &= 16\cdot 48 \\ &= 16\cdot(35\cdot 1 + 13) \\ &\equiv 16\cdot 13 \\ &\equiv 208 \\ &\equiv 35\cdot 5 + 33 \\ &\equiv 33 \pmod{35}. \end{aligned}$$

So $12^7 \equiv 33 \pmod{35}$.