More decoding.

(A) Recall: to decode a coded message $b \equiv n^k \pmod{m}$, with $m = pq$ and $\varphi(m) = (p-1)(q-1)$ (and all conditions as before), we:

(1) Find $x, y \in \mathbb{N}$ with
$$kx - \varphi(m)y = 1,$$

(2) Compute $b^x \pmod{m}$. That's it!

Example 1.
Decode $b = 21$, with $k = 37$ and $m = 143 = 11 \cdot 13$.

Solution.
We have $\varphi(m) = 10 \cdot 12 = 120$. We find that
$$37 \cdot 13 - 120 \cdot 4 = 1.$$

So we compute $21^{13} \pmod{143}$:

$$13 = 8 + 4 + 1$$

$$21 \equiv 21 \pmod{143}$$
$$21^2 = 441 = 143 \cdot 3 + 12 \equiv 12 \pmod{143}$$
$$21^4 = (21^2)^2 \equiv 12^2 = 144 \equiv 1 \pmod{143}$$
$$21^8 = (21^4)^2 \equiv 1^2 \equiv 1 \pmod{143}$$

So
$$\begin{aligned} 21^{13} &\equiv 21^{8+4+1} \\ &\equiv 21^8 \cdot 21^4 \cdot 21^1 \\ &\equiv 1 \cdot 1 \cdot 21 \equiv 21 \pmod{143}. \end{aligned}$$

(B) **The Euclidean algorithm.**

This method lets us, given $a, b \in \mathbb{N}$,

(i) Find $\gcd(a,b)$,

(ii) Find $x, y \in \mathbb{N}$ such that
$$ax - by = \gcd(a,b).$$

(iii) In particular, if $\gcd(k, \varphi(m)) = 1$, we can find $x, y \in \mathbb{N}$ with
$$kx - \varphi(m)y = 1.$$

Example 2a.
Find $\gcd(582, 165)$.

Solution.

Step 1: Divide the smaller number into the larger one:

dividend   divisor

$$582 = 165 \cdot 3 + 87 \qquad \text{(a)}$$

quotient   remainder

Step 2: Divide the previous remainder into the previous divisor:

$$165 = 87 \cdot 1 + 78 \qquad \text{(b)}$$

Step 3: repeat Step 2 until you get a remainder of zero:

$$87 = 78 \cdot 1 + 9 \qquad \text{(c)}$$

$$78 = 9\cdot 8 + 6 \qquad (d)$$
$$9 = 6\cdot 1 + \boxed{3} \qquad (e)$$
$$6 = 3\cdot 2 + 0 \qquad (f)$$

Step 4 Your next-to-last remainder (just before the remainder 0) is your gcd.

SO: $\gcd(582, 165) = 3$.

Example 2b.

Express $\gcd(582, 165)$ in the form $582x - 165y$ $(x, y \in \mathbb{N})$.

Solution. We work backwards from the next-to-last equation in Step 3 above:

$$
\begin{aligned}
3 &= 9 - 6\cdot 1 && \text{(by equation (e))}\\
&= 9 - (78 - 9\cdot 8)\cdot 1 && \text{(by equation (d))}\\
&= 9\cdot 9 - 78\cdot 1 && \text{(simplify)}\\
&= 9\cdot(87 - 78\cdot 1) - 78\cdot 1 && \text{(by equation (c))}\\
&= 87\cdot 9 - 78\cdot 10 && \text{(simplify)}\\
&= 87\cdot 9 - (165 - 87\cdot 1)\cdot 10 && \text{(by equation (b))}\\
&= 87\cdot 19 - 165\cdot 10 && \text{(simplify)}\\
&= (582 - 165\cdot 3)\cdot 19 - 165\cdot 10 && \text{(by equation (a))}\\
&= 582\cdot 19 - 165\cdot 67. && \text{(simplify)}
\end{aligned}
$$

Conclusion:

$$\gcd(582, 165) = 582\cdot 19 - 165\cdot 67.$$