The Euclidean Algorithm and RSA decoding.

Recall:

(a) To find $\gcd(a,b)$ $(a,b \in \mathbb{N})$:

(i) Divide the smaller number into the larger to get a "remainder equation."

(ii) Divide the remainder from the previous remainder equation into the divisor from that equation.

(iii) Repeat (ii) above until your remainder is zero.

(iv) The previous remainder is $\gcd(a,b)$.

Example 1(a).

Find $\gcd(35,24)=1$.

Solution

We divide 24 into 35:

$35 = 24 \cdot 1 + 11.$ (IR)

Continue:

$24 = 11 \cdot 2 + 2$ (S)

$11 = 2 \cdot 5 + \boxed{1}$ ← $\gcd(35,24)$ (A)

$2 = 2 \cdot 1 + 0$

So $\gcd(35,24)=1$.

(b) Linear combinations.

Once you've found gcd(a,b) as above, find $x, y \in \mathbb{N}$ with

a "linear combination" of a and b

$$ax - by = \gcd(a,b)$$

as follows:

(i) Take the next-to-last remainder equation from part (a) and solve for the remainder (which *is* gcd(a,b)).

(ii) Solve the previous remainder equation for the remainder there, and plug this result into your previous result. Simplify by collecting like terms.

(iii) Repeat step (ii) until you're done.

Example 1(b).

Find $x, y \in \mathbb{N}$ with

$$35x - 24y = 1.$$

Solution.

We have

$$\begin{aligned}
1 &= 11 - 2\cdot 5 && \text{(by (A))}\\
&= 11 - (24 - 11\cdot 2)\cdot 5 && \text{(by (\$))}\\
&= 11\cdot 11 - 24\cdot 5 && \text{(simplify)}\\
& (35 - 24\cdot 1)\cdot 11 - 24\cdot 5 && \text{(by (R))}\\
&= 35\cdot 11 - 24\cdot 16 && \text{(simplify).}
\end{aligned}$$

So

$$35\cdot 11 - 24\cdot 16 = 1.$$

Parts (a) and (b) above constitute th
Euclidean algorithm.

(c) Decoding.

Example 1(c).
Decode the message $b=31$ using $k=35$ and $m=39$.

Solution

We have $m=3\cdot 13$, so $\varphi(m)=2\cdot 12=24$.
We have $\gcd(k,\varphi(m))=\gcd(35,24)=1$ by part (a) above, and

$$35\cdot 11-24\cdot 16=1$$

by part (b).

So we compute $31^{11} \pmod{39}$:

$$11=8+2+1$$

$$31^1 \equiv 31 \pmod{39}$$
$$31^2 \equiv 961 \equiv 39\cdot 24+25\equiv 25 \pmod{39}$$
$$31^4 \equiv (31^2)^2 \equiv 25^2 \equiv 625 \equiv 39\cdot 16+1 \equiv 1 \pmod{39}$$
$$31^8 \equiv (31^4)^2 \equiv 1^2 \equiv 1 \pmod{39}.$$

So
$$\begin{aligned} 31^{11} &\equiv 31^{8+2+1} \\ &\equiv 31^8\, 31^2\, 31^1 \\ &\equiv 1\cdot 25\cdot 31 \\ &\equiv 775 \\ &\equiv 39\cdot 19+34 \equiv 34 \pmod{39}. \end{aligned}$$

The decoded message is X.