Euclidean Algorithm.

Suppose a and b are positive integers with no nontrivial common factor. Then there are integers x, y, R, Q such that

$$xa = Rb + 1$$
$$yb = Qa + 1.$$

For small values of $a+b$ one can find these by inspection:

$$a = 5,\ b = 7 : \quad 3 \cdot 5 = 2 \cdot 7 + 1$$
$$3 \cdot 7 = 4 \cdot 5 + 1$$

Not always $x = y$. Let $a = 6$, $b = 7$:

$$6 \cdot 6 = 5 \cdot 7 + 1$$
$$7 \cdot 7 = 8 \cdot 6 + 1$$

General case Suppose $a = 77$, $b = 52$.

Use Euclidean long division algorithm.

$$77 = 1 \cdot 52 + 25$$
$$52 = 2 \cdot 25 + 2$$
$$25 = 2 \cdot 12 + 1$$

if there are no common factor, eventually you get remainder of 1.

Write the remainders successively as linear combinations $N \cdot 77 + M \cdot 52$ where N & M are integers.

$$25 = 77 \cdot 1 - 52 \cdot 1.$$

$$\begin{aligned} 2 &= 52 \cdot 1 - 2 \cdot 25 = \\ &\quad 52 \cdot 1 - 2(77 \cdot 1 - 52 \cdot 1) = \\ &\quad 52 \cdot 3 - 77 \cdot 2 \end{aligned}$$

$$\begin{aligned} 1 &= 25 - 2 \cdot 12 = \\ &\quad 25 \cdot 1 - (52 \cdot 3 - 77 \cdot 2) \cdot 12 = \\ &\quad (77 \cdot 1 - 52 \cdot 1) - 12(52 \cdot 3 - 77 \cdot 2) = \\ &\quad 77 \cdot 25 - 52 \cdot 37. \end{aligned}$$

<u>Check this</u>: $1925 - 1924 = 1$

So $77 \cdot 25 = 52 \cdot 37 + 1$

<u>Other one?</u> Here is one method.

~~both~~ sides

If $77x = 52R + 1$, then
$-52R = -77x + 1$. Choose k so large that $77k - R,\ 52k - x \geq 0$ (here we can take $k = 1$). Then we ~~have~~ can add $77 \cdot 52 \cdot k$ to both sides and attain

$$\underbrace{52(77 - R)}_{y} = 77 \cdot \underbrace{(52 - x)}_{Q} + 1.$$

So $y = \cancel{77-25=52}\ 77 - 37 = 40$.
$Q = 52 - 25 = 27$. Check

$$52 \cdot 40 \stackrel{??}{=} 77 \cdot 27 + 1$$
$$2080 \qquad 2079$$

Application to Chinese Remainder Problems.

Suppose $n = ? \times 3 + 2$
$= ?? \times 5 + 3$.

What are the possible values of n?

Write $n = 3p + 2$. Find possible p values

~~Find x so that $3x = 5k + 1$~~ $x = 2$, $k = 1$.

Want to choose p so that

$$3p + 2 = 5z + 3 \text{ for some } z.$$

choose x so $3x = 5w + 1$ some w.

Easy to do, let $3 \cdot 2 = 5 + 1$ Then

$$6p + 4 = 10z + 1.$$

So $p + 5p + 4 = 2 \cdot 5z + 1$.

$$p + 3 = 5(2z - p)$$

So we want to choose p such that $p+3$ is divisible by 5. But this means $p = 5t + 2$ some t, and hence we get

$$n = 3(5t+2) + 2 = 15t + 8.$$

Check that these values work.

$$n = 3 \cdot (5t+2) + 2 = 5(3t+1) + 3.$$

General Procedure

Solve $n = Ku + a = Lv + b$

u & v relatively prime.

Want to find x, y, Q, R so that

$$xu = Rv + 1 \qquad \text{(as before)}$$
$$yv = Qu + 1$$

Now take product of $Ku + a = Lv + b$ with x: $Kux + xa = Lvx + xb$

$$K + KRv + xa = Lvx + xb.$$

$$\text{So} \quad K + xa - xb = v\underbrace{(Lx - KR)}_{\text{something}}.$$

This means we should have

$$K = tv + xb - xa \quad \text{for some } t.$$

so that

$$n = Ku + a = tvu + uxb - uxa + a$$
$$= tvu + (Rv+1)(b-a) + a.$$

The equations show that n leaves the right remainders when divided by u or v.

(Much easier with use of integers mod m for various integers m).

Problems with 3 conditions

Find n such that the remainder is $\left\{\begin{matrix}2\\3\\4\end{matrix}\right\}$ when div. by $\left\{\begin{matrix}3\\5\\7\end{matrix}\right\}$.

The first two conditions imply n has the form $15s+8$ for some s. We want to see what conditions on s are needed so that $n = 7t+4$ for some t.

Now $15 = 2\cdot 7+1$, so $15s+8 = s+14s+8 = 7t+4$, so that $s+4 = 7M$, some M. This is equivalent to saying that $s = 7M'+3$ for some M' and hence we obtain $n = 15s+8 = 15\cdot(7M'+3)+8 = 105M'+53$.

Check the answer:

$$
\begin{aligned}
105M'+53 &= 3(35M'+17)+2 \qquad & 53 &= 3\cdot 17+2 \\
&= 5(21M'+10)+3 & &= 5\cdot 10+3 \\
&= 7(15M'+7)+4. & &= 7\cdot 7+4
\end{aligned}
$$