Q: How to find a modular inverse?

Extended Euclidean Algorithm (EEA): It calculates GCD of two integers, say a and n; and in the case for which $\text{GCD}(a, n) = 1$, it can be used to find a^{-1}.

Let's start with Euclidean Algorithm (EA), and how it can be used to calculate GCD(a,b):

Let $r_0 = a$, and $r_1 = b$ be integers such that $a \geq b > 0$. If we use successive division to obtain $r_i = r_{j+1}q_{j+1} + r_{j+2}$ with $0 < r_{j+2} < r_{j+1}$ for $j = 1, 2, \ldots, n-2$ and $r_{n+1} = 0$, then $\text{GCD}(a, b) = r_0$. (the least non-zero remainder)

e.g. Suppose we want to find GCD(252,198).

$$\begin{aligned}
252 &= 1 \cdot 198 + 54 \\
198 &= 3 \cdot 54 + 36 \\
54 &= 1 \cdot 36 + 18 \longrightarrow \text{GCD}(252, 198) = 18 \\
36 &= 2 \cdot 18 + 0
\end{aligned}$$

0	r_j	r_{j+1}	q_{j+1}	r_{j+2}
0	252	198	1	54
1	198	54	3	36
2	54	36	1	18
3	36	18	2	0

- Extremely fast! $\mathcal{O}((\log_2 a)^3)$ bit operations.

It turns out that you can always write the GCD of two numbers as a linear combination of the two. For example $18 = 4 \cdot 252 - 5 \cdot 198$.

Now, if GCD$(a, n) = 1$, then there exists integers x and y such that $ax + ny = 1$. This implies that $ax - 1 = ny$ or $n|(ax - 1)$, or $ax \equiv 1 \mod n$ (i.e. $x = a^{-1}$).

One can use this fact to work backward in the Euclidean Algorithm described above to find the the required linear relationship (i.e. If GCD(a,n) = 1, work backward from last equation in our EC algorithm to find the corresponding coefficients).

However, finding this linear combination can be easier and more systematic, if we use the following theorem.

Theorem: Suppose a, b are two positive integers. Then

$$GCD(a, b) = s_n a + t_n b \quad \text{for } n = 0, 1, 2, \ldots$$

where s_n, t_n are the n^{th}term of the sequence defined recursively by $s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$ and $s_j = s_{j-2} - q_{j-1}s_{j-1},\ t_j = t_{j-2} - q_{j-1}t_{j-1}$.

Example: Write GCD(252,198)=18 as a linear combination of 252 and 198.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	-1
3	36	18	2	0	-3	4
					4	-5

$s_0 = 1$ $\qquad$ $t_0 = 0$

$s_1 = 0$ $\qquad$ $t_1 = 1$

$s_2 = s_0 - s_1 q_1 = 1 - 0 \cdot 1 = 1$ $\qquad$ $t_2 = t_0 - t_1 q_1 = 0 - 1 \cdot 1 = -1$

$s_3 = s_1 - s_2 q_2 = 0 - 1 \cdot 3 = -3$ $\qquad$ $t_3 = t_1 - t_2 q_2 = 1 - (-1) \cdot 3 = 4$

$s_4 = s_2 - s_3 q_3 = 1 - (-3) \cdot 1 = 4$ $\qquad$ $t_4 = t_2 - t_3 q_3 = -1 - 4 \cdot 1 = -5$

$$\therefore 18 = s_4 \cdot 252 + t_4 \cdot 198 = 4 \cdot 252 - 5 \cdot 198.$$

Example 2: How to find $(101)^{-1} \mod 840$

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	840	101	8	32	1	0
1	101	32	3	5	0	1
2	32	5	6	2	+1	-8
3	5	2	2	1	-3	25
4	2	1	2	0	19	-158
					-41	341

$s_j = s_{j-2} - q_{j-1}s_{j-1}$ | $t_j = t_{j-2} - q_{j-1}t_{j-1}$

$s_0 = 1$ | $t_0 = 0$

$s_1 = 0$ | $t_1 = 1$

$s_2 = s_0 - q_1 s_1 = 1 - (8)(0) = 1$ | $t_2 = t_0 - q_1 t_1 = 0 - (8)(1) = -8$

$s_3 = s_1 - q_2 s_2 = 0 - (3)(1) = -3$ | $t_3 = t_1 - q_2 t_2 = 1 - (3)(-8) = 25$

$s_4 = s_2 - q_3 s_3 = 1 - (6)(-3) = 19$ | $t_4 = t_2 - q_3 t_3 = (-8) - (6)(25) = -158$

$s_5 = (-3) - (2)(19) = -41$ | $t_5 = 25 - (2)(158) = 341$