Compute $a^{-1} \bmod m$? Run Extended Euclid's Algorithm

Euclid's algorithm: given x, y, output $\gcd(x, y)$.

Extended Euclid's Algorithm: During each step of Euclid's algorithm, do more stuff. Thus, by running almost the same algorithm, you get $\gcd(x, y)$ as a integer linear combination of x and y. i.e. $\gcd(x, y) = ax + by$ for some $a, b \in \mathbb{Z}$.

(a) What is $\gcd(2328, 440)$?

On the side, write down the newly introduced value as an integer combination of the previous two inputs.

Sol:

$$\gcd(2328, 440) = \gcd(440, 128) \quad (\equiv 2328 \pmod{440})$$
$$= \gcd(128, 56) \quad \text{new input!}$$
$$= \gcd(56, 16)$$
$$= \gcd(16, 8)$$
$$= \gcd(8, 0)$$
$$= 8$$

$$128 = 1 \times 2328 + (-5) \times 440$$
$$56 = 1 \times 440 + (-3) \times 128$$
$$16 = 1 \times 128 + (-2) \times 56$$
$$\Rightarrow \quad 8 = 1 \times 56 + (-3) \times 16$$
$$0 = 1 \times 16 + (-2) \times 8$$

(b) What is $\gcd(2328, 440)$ as an integer linear combination of 2328 and 440?

On the right side above, we have a set a equations, "describing" 8, 2328, and 440. Keep substituting to get the answer.

Sol:

$$8 = 1 \times 8 + 0 \times 0$$
$$= 1 \times 8 + (1 \times 16 + (-2) \times 8)$$
$$= 1 \times 16 - 1 \times 8$$
$$= 1 \times 16 - 1 \times (1 \times 56 + (-3) \times 16)$$
$$= -1 \times 56 + 4 \times 16$$
$$= -1 \times 56 + 4 \times (1 \times 128 + (-2) \times 56)$$
$$= 4 \times 128 - 9 \times 56$$
$$= 4 \times 128 - 9 \times (1 \times 440 + (-3) \times 128)$$
$$= -9 \times 440 + 31 \times 128$$
$$= -9 \times 440 + 31 \times (1 \times 2328 + (-5) \times 440)$$
$$= 31 \times 2328 - 164 \times 440$$

Or, start from yellow arrow, substitute one number at a time, in backwards order

$$8 = 1 \times 56 + (-3) \times 16$$
$$= 1 \times 56 + (-3) \times (1 \times 128 + (-2) \times 56)$$
$$= 1 \times 56 + (-3) \times 128 + 6 \times 56$$
$$= 7 \times 56 + (-3) \times 128$$
$$= 7 \times (1 \times 440 + (-3) \times 128) + (-3) \times 128$$
$$= 7 \times 440 + (-21) \times 128 + (-3) \times 128$$
$$= 7 \times 440 + (-24) \times 128$$
$$= 7 \times 440 + (-24) \times (1 \times 2328 + (-5) \times 440)$$
$$= 7 \times 440 + (-24) \times 2328 + 120 \times 440$$
$$= 127 \times 440 - 24 \times 2328$$

(c) Express $\gcd(17, 38)$ as a "combination" of 17 and 38.

Sol:

$$4 = 1 \times 38 + (-2) \times 17$$
$$\Rightarrow \quad 1 = 1 \times 17 + (-4) \times 4$$
$$0 = 1 \times 4 + (-4) \times 1$$

$\gcd(17, 38) = \gcd(38, 17) = \gcd(17, 4)$
$= \gcd(4, 1)$
$= \gcd(1, 0)$
$= 1$

$$\gcd(17, 38) = 1 = 1 \times 17 + (-4) \times 4$$
$$= 1 \times 17 + (-4) \times (1 \times 38 + (-2) \times 17)$$
$$= 1 \times 17 + (-4) \times 38 + 8 \times 17$$
$$= -4 \times 38 + 9 \times 17$$

(d) What is 17^{-1} in mod 38?

Sol: 9.

$$1 = 9 \times 17 + 4 \times 38$$
$$\Rightarrow \quad 9 \times 17 \equiv 1 \pmod{38}$$
$$\Rightarrow \quad 17^{-1} \equiv 9 \pmod{38}$$

Concept: $1 = y = x + km$ (9×17, 4×38) $\Rightarrow x \equiv y \pmod{m}$

Fast way of computing exponents? Try repeated square / FLT.

e.g. Compute $14^9 \pmod{55}$

$$
\begin{aligned}
14^9 &\equiv 14 \cdot 14^8 \\
&\equiv 14 \cdot (14^2)^4 \\
&\equiv 14\,(196)^4 \\
&\equiv 14\,(31)^4 \\
&\equiv 14\,(31^2)^2 \\
&\equiv 14\,(961)^2 \\
&\equiv 14\,(26)^2 \\
&\equiv 14\,(676) \\
&\equiv 14\,(16) \\
&\equiv 4 \pmod{55}
\end{aligned}
$$

idea: multiplying out 14^9 then take mod is hard, so we want to keep the number during each step relatively small (compare to 14^9).

We "make the number smaller" step by step, instead of multiplying out 14^9 first and then "reduce" it at once.

e.g. Compute $4^{25} \pmod 7$.

If you see a mod p where p is a prime, try using FLT.
It gives you a congruence relation involving 1.

According to FLT, $4^6 \equiv 1 \pmod 7$

$$\Rightarrow (4^6)^4 \equiv 1^4 \pmod 7$$

$$\Rightarrow (4)^{24} \cdot 4 \equiv 4 \pmod 7$$

Thus, $4^{25} \equiv 4 \pmod 7$