5\. Let $\bar{a}$ be the inverse of a modulo m

a) $a=4$, $m=9$. Then by Euclidean Algorithm, we have

$\gcd(4,9) = \gcd(4, \underline{9 \bmod 4})$ | $9 = 2\times 4 + 1$

$= \gcd(4,1) = 1$ (it means $\bar{a}$ exists) | $\Rightarrow 1 = 9 \underbrace{-2}_{\bar{a}} \times 4$

Thus, $\boxed{\bar{a} \equiv -2 \bmod 9} = -2$, or 7 or 16 ...

b) $a=19$, $m=141$. Then by Euclidean Algorithm, we have

$\gcd(19,141) = \gcd(19, \underline{141 \bmod 19})$ | $141 = 7\times 19 + 8 \Rightarrow 8 = 141 - 7\times 19$ — ④

$= \gcd(19,8) = \gcd(\underline{19 \bmod 8}, 8)$ | $19 = 2\times 8 + 3 \Rightarrow 3 = 19 - 2\times 8$ — ③

$= \gcd(3,8) = \gcd(3, \underline{8 \bmod 3})$ | $8 = 2\times 3 + 2 \Rightarrow 2 = 8 - 2\times 3$ — ②

$= \gcd(3,2) = \gcd(\underline{3 \bmod 2}, 2)$ | $3 = 1\times 2 + 1 \Rightarrow 1 = 3 - 1\times 2$ — ①

$= \gcd(1,2) = 1$

From ①: $1 = 3 - 1\times 2 \overset{\text{From ②}}{=} 3 - 1\times(8 - 2\times 3) = 3\times 3 - 1\times 8$

$\boxed{\text{From ③}}$ $= 3\times(19 - 2\times 8) - 1\times 8 = -7\times 8 + 3\times 19$

$\boxed{\text{From ④}}$ $= -7\times(141 - 7\times 19) + 3\times 19 = -7\times 141 + \underbrace{52}_{\bar{a}}\times 19$

$\boxed{\text{Thus, } \bar{a} \equiv 52 \pmod{141}}$

c) $a=55$, $m=89$. Then by Euclidean Algorithm, we have

$\gcd(55,89) = \gcd(55, \underline{89 \bmod 55})$ | $89 = 1\times 55 + 34 \rightarrow 34 = 89 - 1\times 55$ — ⑧

$= \gcd(55,34) = \gcd(\underline{55 \bmod 34}, 34)$ | $55 = 1\times 34 + 21 \rightarrow 21 = 55 - 1\times 34$ — ⑦

$= \gcd(21,34) = \gcd(21, \underline{34 \bmod 21})$ | $34 = 1\times 21 + 13 \rightarrow 13 = 34 - 1\times 21$ — ⑥

$= \gcd(21,13) = \gcd(\underline{21 \bmod 13}, 13)$ | $21 = 1\times 13 + 8 \rightarrow 8 = 21 - 1\times 13$ — ⑤

$= \gcd(8,13) = \gcd(8, \underline{13 \bmod 8})$ | $13 = 1\times 8 + 5 \rightarrow 5 = 13 - 1\times 8$ — ④

$= \gcd(8,5) = \gcd(\underline{8 \bmod 5}, 5)$ | $8 = 1\times 5 + 3 \rightarrow 3 = 8 - 1\times 5$ — ③

$= \gcd(3,5) = \gcd(3, \underline{5 \bmod 3})$ → $5 = 1\times 3 + 2 \rightarrow 2 = 5 - 1\times 3$ — ②

$= \gcd(3,2) = \gcd(\underline{3 \bmod 2}, 2)$ → $3 = 1\times 2 + 1 \rightarrow 1 = 3 - 1\times 2$ — ①

$= \gcd(1,2) = 1$

From ①: $1 = 3 - 1\times 2 \underset{\boxed{\text{From ②}}}{=} 3 - 1\times(5 - 1\times 3) = 2\times 3 - 1\times 5$

$\boxed{\text{From ③}}$ $\equiv 2\times(8 - 1\times 5) - 1\times 5 = 2\times 8 - 3\times 5$

$\boxed{\text{From ④}}$ $\equiv 2\times 8 - 3\times(13 - 1\times 8) = 5\times 8 - 3\times 13$

$\boxed{\text{From ⑤}}$ $\equiv 5\times(21 - 1\times 13) - 3\times 13 = 5\times 21 - 8\times 13$

$\boxed{\text{From ⑥}}$ $\equiv 5\times 21 - 8\times(34 - 1\times 21) = 13\times 21 - 8\times 34$

$\boxed{\text{From ⑦}}$ $\equiv 13\times(55 - 1\times 34) - 8\times 34 = 13\times 55 - 21\times 34$

$\boxed{\text{From ⑧}}$ $\equiv 13\times 55 - 21\times(89 - 1\times 55) = \underbrace{34}_{\bar{a}}\times 55 - 21\times 89$

$\boxed{\text{Thus, } \bar{a} \equiv 34 \pmod{89}}$

d) $a = 89$, $m = 232$. Then by Euclidean Algorithm, we have

$\gcd(89, 232) = \gcd(89, \underline{232 \bmod 89})$ → $232 = 2\times 89 + 54 \rightarrow 54 = 232 - 2\times 89$ — ⑥

$= \gcd(89, 54) = \gcd(\underline{89 \bmod 54}, 54)$ → $89 = 1\times 54 + 35 \rightarrow 35 = 89 - 1\times 54$ — ⑤

$= \gcd(35, 54) = \gcd(35, \underline{54 \bmod 35})$ → $54 = 1\times 35 + 19 \rightarrow 19 = 54 - 1\times 35$ — ④

$= \gcd(35, 19) = \gcd(\underline{35 \bmod 19}, 19)$ → $35 = 1\times 19 + 16 \rightarrow 16 = 35 - 1\times 19$ — ③

$= \gcd(16, 19) = \gcd(16, \underline{19 \bmod 16})$ → $19 = 1\times 16 + 3 \rightarrow 3 = 19 - 1\times 16$ — ②

$= \gcd(16, 3) = \gcd(\underline{16 \bmod 3}, 3)$ → $16 = 5\times 3 + 1 \rightarrow 1 = 16 - 5\times 3$ — ①

$= \gcd(1, 3) = \underline{1}$

From ①: $1 = 16 - 5\times 3 \overset{\text{From ②}}{=} 16 - 5\times(19 - 1\times 16) = 6\times 16 - 5\times 19$

$\boxed{\text{From } ③} \Rightarrow \; = 6\times(35 - 1\times 19) - 5\times 19 = -11\times 19 + 6\times 35$

$\boxed{\text{From } ④} \Rightarrow \; = -11\times(54 - 1\times 35) + 6\times 35 = 17\times 35 - 11\times 54$

$\boxed{\text{From } ⑤} \Rightarrow \; = 17\times(89 - 1\times 54) - 11\times 54 = 17\times 89 - 28\times 54$

$\boxed{\text{From } ⑥} \Rightarrow \; = 17\times 89 - 28\times(232 - 2\times 89) = 73\times 89 - 28\times 232$

$\Rightarrow \; 1 = \underbrace{73}_{\bar{a}}\times 89 - 28\times 232$

$\boxed{\text{Then } \bar{a} \equiv 73 \bmod 232}$

11. (a) Solve $19x \equiv 4 \pmod{141}$

<u>Sol</u>: By 5(b), the inverse of 19 modulo 141 is 52.

Thus, we have $\underbrace{52\cdot 19}_{52\cdot 19 \equiv 1 \pmod{141}} x \equiv 52\cdot 4 \pmod{141}$

$\Rightarrow \; 1\cdot x \equiv 208 \pmod{141} = 67 \pmod{141}$

$\Rightarrow \; x \equiv 67 \pmod{141}$

(b) Solve $55x \equiv 34 \pmod{89}$

By 5(c), the inverse of 55 modulo 89 is 34.

Thus, we have $\underbrace{34\cdot 55}_{\equiv 1 \pmod{89}} x \equiv 34\cdot 34 \pmod{89}$

$\Rightarrow \; x \equiv 1156 \pmod{89} = 88 \pmod{89}$

$\Rightarrow \; x \equiv 88 \pmod{89}$

$34 \times 34 = 136 + 1020 = 1156$

$1156 = 89 \times 12 + 88$ ($1156 - 890 = 266$, $266 - 178 = 88$)

(c) Solve $89x \equiv 2 \pmod{232}$

By 5(d), the inverse of 89 modulo 232 is 73.

Thus, we have $\underbrace{73\cdot 89}_{73\cdot 89 \equiv 1 \pmod{232}} x \equiv 73\cdot 2 \pmod{232}$

$$\Rightarrow \qquad x \equiv 146 \pmod{232}$$