Extended Euclidean Algorithm

$\overset{15}{a} x \equiv \underline{1} \mod \overset{79}{n}$

$\gcd(a,n)=1$, x is unknown

$x = a^{-1} \mod n$ ("a inverse mod n")

Euclidean Alg $\gcd(15,79)$

$79 = 5\times\underline{15} + \underline{4}$
$15 = 3\times\underline{4} + \underline{3}$
$* \quad 4 = 1\times\underline{3} + \boxed{1}$
$3 = 3\times 1 + 0$

79 divided by 15
(a) unique quotient (q)
(b) unique remainder (r)
$0 \le r < 15$
If dividing a by b 1 soln to
$a = bq + r$ int q, r
$0 \le r < b$.

Determine $15^{-1} \mod 79$

$\underline{4} - 1\times\underline{3} = \underline{1}$ (linear combo of 4,3 that is equal to 1.)

$4 - 1\times(15 - 3\times 4) = 1$

$4 - 1\times\underline{15} + 3\times\underline{4} = 1$

$4\times\underline{4} - 1\times\underline{15} = 1$ (linear combo of 15,4 equal to 1)

$4\times(79 - 5\times 15) - 1\times 15 = 1$

$4\times 79 - 20\times\underline{15} - 1\times\underline{15} = 1$

$4\times\underline{79} - 21\times\underline{15} = 1$ (linear combo of 79,15 equal to 1)

if $a = b$
$a \equiv b \mod n$
for all pos int n.

$4\times 79 - 21\times 15 \equiv 1 \pmod{79}$

$4\times 0 - 21\times 15 \equiv 1 \pmod{79}$

$-21\times 15 \equiv 1 \pmod{79}$

$15^{-1}_{79} \equiv -21 \mod 79$

$\equiv \boxed{58 \mod 79}$

$\gcd(231, 102)$

$$231 = 2\times102 + 27$$
$$102 = 3\times27 + 21$$
$$27 = 1\times21 + 6$$
$$21 = 3\times6 + \boxed{3}$$
$$6 = 2\times3 + 0$$

$102^{-1} \bmod 231$
DOES NOT
EXIST

$$79^{-1} \bmod \underline{\underline{15}}$$
$$\equiv 4^{-1} \bmod 15 \quad \text{since} \quad 79 \equiv 4 \bmod 15$$

Find $103^{-1} \bmod 231$

$$231 = 2\times103 + 25$$
$$103 = 4\times25 + 3$$
$$25 = 8\times3 + 1$$

$$\underline{25} - 8\times\underline{3} = 1$$
$$25 - 8(103 - 4\times25) = 1$$
$$25 - 8\times103 + 32\times25 = 1$$
$$33\times\underline{25} - 8\times103 = 1 \ \cancel{\bmod 103}$$
$$33(231 - 2\times103) - 8\times103 = 1$$
$$33\times231 - 66\times103 - 8\times103 = 1$$
$$33\times231 - 74\times103 \equiv 1 \bmod 231$$
$$-74\times103 \equiv 1 \bmod 231$$
$$103^{-1} \equiv \overset{231}{-74}$$
$$\equiv 157 \bmod 231$$