Example illustrating an application of Corollary 3:

Find the multiplicative inverse of 10 (mod 29).

By the Euclidean algorithm

$$29 = 10 \times 2 + 9$$

$$10 = 9 \times 1 + 1$$

$$9 = 1 \times 9 + 0$$

$\therefore \gcd(29, 10) = \gcd(9, 1) = 1$

This confirms that 10 is relatively prime to 29.

To find the multiplicative inverse of 10 (mod 29) we now proceed as follows:

$$1 = 10 - 9 = (1)10 + (-1)9$$

$$= 10 - (29 - 10 \times 2) = (-1)29 + (3)10.$$

Therefore $1 = (-1)29 + (3)10$,

and so $1 \equiv 3 \times 10 \pmod{29}$

and therefore 3 is the multiplicative inverse of 10 (mod 29).

If m is <u>not</u> prime, then $(\mathbb{Z}_m - \{0\}, \cdot)$ is <u>not</u> a group, for not all elements have multiplicative inverses. In fact, given $a \in \mathbb{Z}_m - \{0\}$, we may use the Euclidean algorithm to determine whether $\gcd(m,a) = 1$, and if $\gcd(m,a) = 1$, then by "working backwards", we can find the multiplicative inverse of a (mod m).

We state, without further proof ...

<u>Theorem 4</u> $a \in \mathbb{Z}_m$ has a multiplicative inverse (mod m) if and only if $\gcd(m,a) = 1$.

Example Find the multiplicative inverses of 11 and 12 (mod 26), if they exist.

By the Euclidean algorithm,

$$26 = 11 \times 2 + 4$$
$$11 = 4 \times 2 + 3$$
$$4 = 3 \times 1 + 1$$
$$3 = 1 \times 3 + 0$$

Therefore $\gcd(26,11) = \gcd(3,1) = 1$.

"Working backwards"...

$$1 = 4 - 3 = (1)4 + (-1)3$$
$$= 4 - (11 - 4\times 2) = (-1)11 + (3)4$$
$$= -11 + 3(26 - 11\times 2) = (3)26 + (-7)11.$$

Therefore $1 = (3)26 + (-7)11$,

so $1 \equiv (-7) \times 11 \pmod{26}$

and therefore 19 is the multiplicative inverse of 11 (mod 26).