EXAMPLES: Let's compute orders in $(\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$:

$\underset{\{\bar 1, \bar 2\}}{\|}$ $\underset{\{\bar 1, \bar 2, \bar 3, \bar 4\}}{\|}$

$(\bar a, \bar b)$	$\text{ord}(\bar a, \bar b)$
$(\bar 1, \bar 1)$	1
$(\bar 1, \bar 2)$	4
$(\bar 1, \bar 3)$	4
$(\bar 1, \bar 4)$	2
$(\bar 2, \bar 1)$	2
$(\bar 2, \bar 2)$	4
$(\bar 2, \bar 3)$	4
$(-\bar 1, -\bar 1) = (\bar 2, \bar 4)$	2

Looks similar to $(\mathbb{Z}/15\mathbb{Z})^\times$! Not a coincidence...

3rd century AD.?

Sun Ze's Theorem ("Chinese Remainder Thm") (PROP 2.11.3 + more)

Given m, n $\boxed{\text{with } \gcd(m,n)=1,}$ the map

$$\begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \bar a & \longmapsto & (\bar a, \bar a) \\ (\text{mod } mn) & & (\text{mod } m) \quad (\text{mod } n) \end{array}$$

is well-defined, a bijection, and respects both $+$ and $\times$, so that it gives group isomorphisms

$$(\mathbb{Z}/mn\mathbb{Z})^+ \cong (\mathbb{Z}/m\mathbb{Z})^+ \times (\mathbb{Z}/n\mathbb{Z})^+$$

$$\text{and } (\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

10/12/2018 > proof: Well-defined-ness of f comes from $\bar a = \bar a'$ in $\mathbb{Z}/mn\mathbb{Z}$

$$\Rightarrow a - a' \in mn\mathbb{Z}$$
$$\Rightarrow a - a' \in m\mathbb{Z}, n\mathbb{Z}$$
$$\Rightarrow \bar a = \bar a' \text{ in } \mathbb{Z}/m\mathbb{Z}, \quad \bar a = \bar a' \text{ in } \mathbb{Z}/n\mathbb{Z}$$

Respecting $+, \times$ comes from their componentwise defn on right.
Bijectivity of f comes from an explicit inverse map g, that comes from picking any $x, y \in \mathbb{Z}$ with $xm + yn = 1$ (since $\gcd(m,n)=1$).

This let's one define

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \xrightarrow{g} \mathbb{Z}/mn\mathbb{Z}$$
$$(\bar{c}, \bar{d}) \longmapsto \overline{ync + xmd}$$

and check $(g\circ f)(\bar{a}) = g((\bar{a},\bar{a})) = \overline{yna + xma} = \overline{(yn+xm)\cdot a} = \bar{1}\cdot\bar{a} = \bar{a}$

and $(f\circ g)(\bar{c},\bar{d}) = f(\overline{ync+xmd}) = (\overline{ync+xmd}, \overline{ync+xmd})$
$= (\overline{ync}, \overline{xmd})$ in $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$
$\stackrel{\vee}{=} (\bar{1}\cdot\bar{c}, \bar{1}\cdot\bar{d}) = (\bar{c},\bar{d})$ ∎

since $xm+yn=1$
$\Rightarrow \overline{xm} = \bar{1}$ in $\mathbb{Z}/n\mathbb{Z}$
$\overline{yn} = \bar{1}$ in $\mathbb{Z}/m\mathbb{Z}$

There's an alternate way we might recognize $(\mathbb{Z}/mn\mathbb{Z})^+ \cong (\mathbb{Z}/m\mathbb{Z})^+ \times (\mathbb{Z}/n\mathbb{Z})^+$, via a general product recognition result.

$G = G_1 \times G_2$ has 2 subgroups $H = G_1 \times \{1\}$
$K = \{1\} \times G_2$

that (a) intersect in $\{\overset{(1,1)}{1}\} (= H\cap K)$
(b) commute with each other : $hk = kh$ $\forall h\in H, k\in K$ $\left(\text{since } (g_1,1)\cdot(1,g_2) = (g_1,g_2) = (1,g_2)\cdot(g_1,1)\right)$
and (c) $G = H\cdot K$ since $(g_1,g_2) = (g_1,1)\cdot(1,g_2)$
$:= \{hk : h\in H, k\in K\}$

That's all you need...

PROPOSITION: If a group G has two subgroups $H,K < G$, then the
(PROP 2.11.4)
multiplication map

$$H\times K \xrightarrow{\mu} G$$
$$(h,k) \longmapsto hk$$

is an isomorphism of groups $\iff \begin{cases} \text{(a) } H\cap K = \{1\} \\ \text{(b) } H,K \text{ commute, i.e. } hk=kh\ \forall h\in H, k\in K \\ \text{(c) } HK = G \end{cases}$

proof: Check μ is injective $\iff$ (a) $H\cap K = \{1\}$: If μ is injective then any $g\in H\cap K$ has $\mu(g, g^{-1}) = g\cdot g^{-1} = 1 = \mu(1,1)$
forcing $g=1$, i.e. $H\cap K = \{1\}$
If $H\cap K = \{1\}$ and $\mu(h,k)=1$ then $hk=1$
$\Rightarrow h = k^{-1}\in K$
$\Rightarrow h\in H\cap K \Rightarrow h=1.$

Check μ is a group homomorphism $\Leftrightarrow$ (b) H, K commute

$$\mu((h_1,k_1)(h_2,k_2)) = \mu((h_1,k_1))\,\mu((h_2,k_2)) \quad \forall\, h_i \in H,\ k_i \in K,\ i=1,2$$

$$\mu((h_1,k_1)(h_2,k_2)) = \mu((h_1h_2, k_1k_2)) = h_1h_2k_1k_2 \qquad \mu((h_1,k_1))\,\mu((h_2,k_2)) = h_1k_1 \cdot h_2k_2$$

$\Leftrightarrow \quad h_1h_2k_1k_2 = h_1k_1h_2k_2$) mult. on left by h_1^{-1}, on right by k_2^{-1}

$\Leftrightarrow \quad h_2k_1 = k_1h_2 \quad \forall k_1 \in K, h_2 \in H$ i.e. H, K commute.

Lastly μ is surjective $\Leftrightarrow$ (c) $G = HK$ since $HK = \mathrm{im}(\mu)$. ∎

This proposition almost applies to $(\mathbb{Z}/mn\mathbb{Z})^+ = G$ if $\gcd(m,n)=1$

with subgroups $H = (\mathbb{Z}/m\mathbb{Z})^+ \cong$ multiples of $\bar{n}$ inside $(\mathbb{Z}/mn\mathbb{Z})^+$

$K = (\mathbb{Z}/n\mathbb{Z})^+ \cong$ multiples of $\bar{m}$ inside $(\mathbb{Z}/mn\mathbb{Z})^+$

Q: Why is $H \cap K = \{1\}$ $(= \{\bar{0}\})$?

Why do H, K commute?

($G = H + K$ is less obvious, but can note both $G = (\mathbb{Z}/mn\mathbb{Z})^+$, and $H \times K$ have same cardinality mn, so the injective homomorphism μ must also surject).

~~REMARK~~:

Note that one can use Sun Ze's Thm. and induction on k to prove

if $(m_1, m_2, \ldots, m_k)$ have $\gcd(m_i, m_j) = 1$ $\forall i \neq j$ then

$$\begin{aligned} \mathbb{Z}/m_1m_2\cdots m_k\mathbb{Z} &\longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \\ \bar{a} &\longmapsto (\bar{a}, \ldots, \bar{a}) \end{aligned}$$

is a bijection respecting $+, \times$

COROLLARY: $(\mathbb{Z}/m_1m_2\cdots m_k\mathbb{Z})^\times \cong (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})^\times$ if $\gcd(m_i, m_j) = 1$

so if $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ for distinct primes p_i, then $\varphi(n) = \varphi(p_1^{e_1}) \cdots \varphi(p_r^{e_r}) = \prod_{i=1}^{r} (p_i^{e_i} - p_i^{e_i - 1})$.

A digression to describe RSA encryption

Alice wants to be able to have Bob send her secret messages (as some $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$), while Eve is eavesdropping (!?)

STEP 1:

Alice picks two huge ($\sim 10^{1000}$) random primes p, q keeping them secret,

but then computes $n = p \cdot q$ and publishes n.

She also picks a randomly chosen encryption exponent $\bar{e} \in (\mathbb{Z}/(p-1)(q-1))^\times$,

and publishes e as an integer in range $1, 2, \ldots, (p-1)(q-1)$,

keeping $(p-1)(q-1)$ secret.

She lastly computes the decryption exponent $\bar{d} = \bar{e}^{-1}$ in $(\mathbb{Z}/(p-1)(q-1))^\times$,

but keeps it secret.

STEP 2: When Bob wants to send Alice $\bar{x}$ in $\mathbb{Z}/pq\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$,

he computes $\bar{y} := \bar{x}^e$ and sends $\bar{y}$ to Alice publicly instead.

STEP 3: Alice decrypts $\bar{y}$ by computing

$$\bar{y}^d = (\bar{x}^e)^d = \bar{x}^{de} = \bar{x}^{1+k(p-1)(q-1)} = \bar{x}^1 \left(\bar{x}^{(p-1)(q-1)}\right)^k = \bar{x} \cdot \bar{1} = \bar{x}$$

for some $k \in \mathbb{Z}$, since $\bar{d} = \bar{e}^{-1}$ in $(\mathbb{Z}/(p-1)(q-1)\mathbb{Z})^\times$

by Euler's Thm, since $\varphi(n) = \varphi(pq) = (p-1)(q-1)$

10/15/18 >

Crucial points

- Every computation Alice or Bob must do need to be achievable quickly, meaning at worst in # of steps at most a polynomial in # of digits of p or q ($= \log(p), \log(q)$)
  (Math 5248 discusses these computational issues)
- Eve would need to either factor n into $p \cdot q$ (only slow, exponential algorithms known !)
  or compute $\sqrt[e]{\bar{y}} = \bar{x}$ in $\mathbb{Z}/n\mathbb{Z}$ (same story !)