Math 561/661 **Fall 2023**
Homework 5 **Drew Armstrong**

1. First Isomorphism Theorem. Let $\varphi : (G, *, \varepsilon_G) \to (H, \bullet, \varepsilon_H)$ be a group homomorphism. Consider the kernel and image:

$$\ker \varphi = \{a \in G : \varphi(a) = \varepsilon_H\},$$
$$\operatorname{im} \varphi = \{\varphi(a) : a \in G\}.$$

(a) Prove that φ is injective if and only if $\ker \varphi = \{\varepsilon_G\}$. In this case, prove that $G \cong \operatorname{im} \varphi$.
(b) Prove that $\ker \varphi$ is a normal subgroup of G, so the set of cosets $G/\ker \varphi$ is a group. Prove that the function $\Phi : G/\ker \varphi \to \operatorname{im} \varphi$ defined by $\Phi([a]) := \varphi(a)$ is a well-defined group isomorphism.

(a): First suppose that φ is injective, so that $\varphi(a) = \varphi(b)$ implies $a = b$ for all $a, b \in G$. In order to show that $\ker \varphi = \{\varepsilon_G\}$, consider any element $a \in \ker \varphi$, so that $\varphi(a) = \varepsilon_H$. Then since $\varphi(\varepsilon_G) = \varphi_H$ we conclude that $a = \varepsilon_G$. Conversely, suppose that $\ker \varphi = \{\varepsilon_G\}$. In order to show that φ is injective, consider any $a, b \in G$ satisfying $\varphi(a) = \varphi(b)$. Then we have

$$\varphi(a^{-1} * b) = \varphi(a)^{-1} \bullet \varphi(b) = \varphi(b)^{-1} \bullet (b) = \varepsilon_H,$$

so that $a^{-1} * b \in \ker \varphi$. Since $\ker \varphi = \{\varepsilon_G\}$ this implies that $a^{-1} * b = \varepsilon_G$, and hence $a = b$.

(b): The assignment $\Phi([a]) := \varphi(a)$ is surjective by definition. We must show that Φ is well-defined, injective, and that it satisfies the property of group homomorphism. First we observe that Φ is well-defined and injective since for all $a, b \in G$ we have

$$\begin{aligned}
[a] = [b] &\iff a * \ker \varphi = b * \ker \varphi \\
&\iff a^{-1} * b \in \ker \varphi \\
&\iff \varphi(a^{-1} * b) = \varepsilon_H \\
&\iff \varphi(a)^{-1} \bullet \varphi(b) = \varepsilon_H \\
&\iff \varphi(a) = \varphi(b) \\
&\iff \Phi([a]) = \Phi([b]).
\end{aligned}$$

Then to see that Φ is a group homomorphism, we observe for all $a, b \in G$ that

$$\begin{aligned}
\Phi([a] * [b]) &= \Phi([a * b]) \\
&= \varphi(a * b) \\
&= \varphi(a) \bullet \varphi(b) \\
&= \Phi([a]) \bullet \Phi([b]).
\end{aligned}$$

Remark. This is a good example of of a proof that "writes itself", since it only uses the definitions and the basic properties of group homomorphisms. It does not involve any "thinking". I call this style of math "theory building", as opposed to "problem solving". Still, the First Isomorphism Theorem can be useful. For example, it gives a better point of view on the order of a group element. For any group element $a \in G$ recall that there exists a group homomorphism $\varphi_a : \mathbb{Z} \to G$ defined by $\varphi_a(k) := a^k$. The image of φ_a is the set of powers of a, which we know is the smallest subgroup of G that contains a. In other words, we have $\operatorname{im} \varphi_a = \langle a \rangle$. The kernel of φ_a, being a subgroup of $\mathbb{Z}$, must have the form $n\mathbb{Z}$ for some integer

$n \geq 0$. Now the First Isomorphism Theorem says that the map $\Phi : \mathbb{Z}/n\mathbb{Z} \to G$ defined by $\Phi([k]) = a^k$ is an isomorphism. In other words, we have

$$a^k = a^\ell \quad \iff \quad \Phi([k]) = \Phi([\ell]) \quad \iff \quad [k] = [\ell] \quad \iff \quad k \equiv \ell \bmod n.$$

This n is called the *order* of the element $a \in G$. In summary: The order of $a \in G$ is the unique integer $n \geq 0$ such that $\ker \varphi_a = n\mathbb{Z}$. [Here $n = 0$ corresponds to "infinite order".]

2. Orbit-Stabilizer Theorem. Let $(G, *, \varepsilon)$ be a group and let X be a set. An *action of G on X* is a function $G \times X \to X$, which we can denote by $(g, x) \mapsto g(x)$, satisfying two rules:

(A1) For all $x \in X$ we have $\varepsilon(x) = x$.

(A2) For all $a, b \in G$ and $x \in X$ we have $(a * b)(x) = a(b(x))$.

(a) Consider the relation $\sim$ on X defined by

$$x \sim y \quad \iff \quad \exists g \in G, y = g(x).$$

Prove that this is an equivalence relation. The equivalence classes are called *orbits*:

$$\mathrm{Orb}(x) := \{y \in X : x \sim y\} \subseteq X.$$

(b) For any $x \in X$ we define the *stabilizer subgroup*:

$$\mathrm{Stab}(x) := \{g \in G : g(x) = x\} \subseteq G.$$

Prove that $\mathrm{Stab}(x)$ is indeed a subgroup of G. [It need not be a normal subgroup.]

(c) Consider any element $x \in X$. From part (b) we may consider the set of cosets $G/\mathrm{Stab}(x)$. Prove that the function $\Phi : G/\mathrm{Stab}(x) \to \mathrm{Orb}(x)$ defined by $\Phi([a]) = a(x)$ is a well-defined bijection.

(a): *Reflexive.* Axiom (A1) says that $x = \varepsilon(x)$ for all $x \in X$. Since $\varepsilon \in G$ this implies that $x \sim x$ for all $x \in X$. *Symmetric.* Suppose that $x \sim y$ so that $y = g(x)$ for some $g \in G$. Then

$$\begin{aligned} y &= g(x) \\ g^{-1}(y) &= g^{-1}(g(x)) \\ g^{-1}(y) &= (g^{-1} * g)(x) && \text{(A2)} \\ g^{-1}(y) &= \varepsilon(x) \\ g^{-1}(y) &= x. && \text{(A1)} \end{aligned}$$

Since $g^{-1} \in G$ this implies that $y \sim x$. *Transitive.* Suppose that $x \sim y$ and $z \sim y$ so that $y = g(x)$ and $z = h(y)$ for some $g, h \in G$. Then we have

$$\begin{aligned} z &= h(y) \\ &= h(g(x)) \\ &= (h * g)(x). && \text{(A2)} \end{aligned}$$

Since $h * g \in G$ this implies that $x \sim z$.

(b): To show that $\mathrm{Stab}(x) \subseteq G$ is a subgroup, we consider any $a, b \in \mathrm{Stab}(x)$, so that $a(x) = x$ and $b(x) = x$. Observe that $a(x) = x$ implies $a^{-1}(x) = x$:

$$\begin{aligned} a(x) &= x \\ a^{-1}(a(x)) &= a^{-1}(x) \\ (a^{-1} * a)(x) &= a^{-1}(x) && \text{(A2)} \\ \varepsilon(x) &= a^{-1}(x) \end{aligned}$$

$$x = a^{-1}(x). \tag{A1}$$

Then we have

$$(a^{-1} * b)(x) = a^{-1}(b(x)) = a^{-1}(x) = x,$$

which says that $a^{-1} * b \in \mathrm{Stab}(x)$.

(c): Fix any point $x \in X$. I claim that the rule $\Phi([a]) := a(x)$ defines a bijection from the set of cosets $G/\mathrm{Stab}(x)$ to the set of points $\mathrm{Orb}(x)$. It is clearly surjective, so we only need to check that Φ is well-defined and injective. To see this, note for all $a, b \in G$ that

$$\begin{aligned}
[a] = [b] &\iff a * \mathrm{Stab}(x) = b * \mathrm{Stab}(x) \\
&\iff a^{-1} * b \in \mathrm{Stab}(x) \\
&\iff (a^{-1} * b)(x) = x \\
&\iff a^{-1}(b(x)) = x \\
&\iff b(x) = a(x) \\
&\iff \Phi([a]) = \Phi([b]).
\end{aligned}$$

Remark. Note that this is almost identical to the proof of the First Isomorphism Theorem. The main difference is that $\mathrm{Orb}(x)$ and $G/\mathrm{Stab}(x)$ are not groups (the subgroup $\mathrm{Stab}(x)$ need not be normal), so the Orbit-Stabilizer Theorem is just a bijection, not an "isomorphism".[1]

3. Burnside's Lemma. Suppose that the group $(G, *, \varepsilon)$ acts on the set X. Consider the set of pairs $(g, x) \in G \times X$ satisfying $g(x) = x$:

$$S = \{(g, x) : g(x) = x\} \subseteq G \times X.$$

Suppose that G and X are finite so that S is finite.

(a) Explain why $\#S = \sum_{x \in X} \#\mathrm{Stab}(x)$.

(b) For any $g \in G$, let $\mathrm{Fix}(g) = \{x \in X : g(x) = x\} \subseteq X$ be the set of elements of X that are "fixed by g". Explain why $\#S = \sum_{g \in G} \#\mathrm{Fix}(g)$. It follows from (a) and (b) that

$$\sum_{x \in X} \#\mathrm{Stab}(x) = \sum_{g \in G} \#\mathrm{Fix}(g).$$

(c) From Problem 2 we know that X is a disjoint union of orbits. Let X/G denote the set of orbits. Use the Orbit-Stabilizer Theorem to prove that $\sum_{x \in X} \#\mathrm{Stab}(x) = \#G \cdot \#(X/G)$, and conclude that the number of orbits is equal to the average number of elements of X fixed by an element of G:

$$\#(X/G) = \frac{1}{\#G} \cdot \sum_{g \in G} \#\mathrm{Fix}(g).$$

[Hint: Let $k = \#(X/G)$ and let $X = \mathrm{Orb}(x_1) \sqcup \cdots \sqcup \mathrm{Orb}(x_k)$ be the decomposition into orbits. For any element $x \in \mathrm{Orb}(x_i)$ show that $\#\mathrm{Stab}(x) = \#G/\#\mathrm{Orb}(x_i)$. Now add them up.]

[1] Actually, there is a bit more structure here. The bijection from $G/\mathrm{Stab}(x)$ to $\mathrm{Orb}(x)$ is an "isomorphism of G-sets" because it "preserves the action of G" on both sets. The natural action of G on the set of cosets $G/\mathrm{Stab}(x)$ is by left multiplication: $a(b * \mathrm{Stab}(x)) := (a * b) * \mathrm{Stab}(x)$.

(a,b): We will prove (a) and (b) together. Imagine the set $G \times X$ as a rectangular array of cells with rows indexed by the elements of G and columns indexed by the elements of X. If $g(x) = x$ then we put a 1 in the cell indexed by the pair (g, x); otherwise we put 0.

Let $S \subseteq G \times X$ be the set of cells that contain 1, so that $\#S$ is the total number of 1s in the array. Equivalently, $\#S$ is the sum of all entries in the rectangular array. Now consider the column indexed by some element $x \in X$. The sum of the entries in this column is $\#\mathrm{Stab}(x)$ because each 1 in this column corresponds to a group element $g \in G$ with $g(x) = x$. Summing the entries of the array column-by-column gives $\#S = \sum_{x \in X} \#\mathrm{Stab}(x)$.

On the other hand, for a given group element $g \in G$ the 1s in the g-th row correspond to elements $x \in X$ with $g(x) = x$, so the sum of the entries in this row is $\#\mathrm{Fix}(g)$. Then summing the entries of the array row-by-row gives $\#S = \sum_{g \in G} \#\mathrm{Fix}(g)$.

(c): By definition, the orbit $\mathrm{Orb}(x)$ is the equivalence class of x with respect to the equivalence relation from Problem 2(a). Thus the set X is partitioned into orbits:

$$X = \mathrm{Orb}(x_1) \sqcup \mathrm{Orb}(x_2) \sqcup \cdots \sqcup \mathrm{Orb}(x_k)$$

for some randomly chosen orbit representatives $x_1, \ldots, x_k \in X$. Let X/G denote the set of orbits, so that $\#(X/G) = k$. For any point x in the orbit $\mathrm{Orb}(x_i)$ we note that $\mathrm{Orb}(x_i) = \mathrm{Orb}(x)$ so from Orbit-Stabilizer and Lagrange we have

$$\#\mathrm{Stab}(x) = \#G/\#\mathrm{Orb}(x) = \#G/\mathrm{Orb}(x_i).$$

Finally, from parts (a) and (b) we have

$$\begin{aligned}
\sum_{g \in G} \#\mathrm{Fix}(g) &= \sum_{x \in X} \#\mathrm{Stab}(x) \\
&= \sum_{i=1}^{k} \sum_{x \in \mathrm{Orb}(x_i)} \#\mathrm{Stab}(x_i) \\
&= \sum_{i=1}^{k} \sum_{x \in \mathrm{Orb}(x_i)} \#G/\#\mathrm{Orb}(x_i) \\
&= \sum_{i=1}^{k} \#G \cdot \left(\sum_{x \in \mathrm{Orb}(x_i)} 1/\#\mathrm{Orb}(x_i) \right) \\
&= \sum_{i=1}^{k} \#G \cdot (1) \\
&= k \cdot \#G \\
&= \#(X/G) \cdot \#G.
\end{aligned}$$

4. Counting Necklaces. Fix some integers $n, k \geq 1$. Let X be the set of words $(x_1, \ldots, x_n)$ with $x_i \in \{1, 2, \ldots, k\}$ for all i, so that $\#X = k^n$. The symmetric group S_n acts on the set X by permuting entries. Let $c = (1, 2, \ldots, n) \in S_n$ be the standard n-cycle and consider the cyclic group $G = \langle c \rangle$ of size n. The orbits of G acting on X are called *necklaces*. We can think of a necklace as a cyclic configuration of n beads using k possible colors.

(a) Explain why $\#\mathrm{Fix}(c^i) = k^{\gcd(i,n)}$. [Hint: You investigated the permutations c^i in Problem 3 of Homework 2.]

(b) Use Burnside's Lemma to show that

$$\#\{\text{necklaces}\} = \frac{1}{n} \cdot \sum_{i=0}^{n-1} k^{\gcd(i,n)}.$$

(c) Compute the number of necklaces with 12 beads of 2 possible colors.

(a): For a general permutation $f \in S_n$ I claim that

$$\#\mathrm{Fix}(f) = k^{\#\text{ of cycles of } f}.$$

Indeed, the words $\mathbf{x} = (x_1, \ldots, x_n)$ in the set $\mathrm{Fix}(f)$ have the property that $x_i = x_j$ if and only if i and j occur in the same cycle of f. We can choose such a word by choosing one color for each cycle of f. For example, if $f = (13)(245)$ then $\mathrm{Fix}(f)$ is the set of words $(x_1, x_2, x_3, x_4, x_5)$ satisfying $x := x_1 = x_3$ and $y := x_2 = x_4 = x_5$. Such a word is specified by choosing two colors $x, y \in \{1, \ldots, k\}$, and there are k^2 ways to do this.

If $c = (1, 2, \ldots, n)$ is the standard n-cycle then we know from Homework 2 that the cycle decomposition of c^i consists of $\gcd(i, n)$ cycles, each of length $n/\gcd(i, n)$. From the above remarks this implies that

$$\#\mathrm{Fix}(c^i) = k^{\#\text{ of cycles of } c_i} = k^{\gcd(i,n)}.$$

(b): Let $G = \langle c \rangle$ be the cyclic group generated by the n-cycle c, so that $\#G = n$. Then from Burnside's Lemma we have

$$\begin{aligned}
\#\{\text{necklaces}\} &= \frac{1}{\#G} \sum_{g \in G} \#\mathrm{Fix}(g) \\
&= \frac{1}{n} \sum_{i=0}^{n-1} \#\mathrm{Fix}(c^i) \\
&= \frac{1}{n} \sum_{i=0}^{n-1} k^{\gcd(i,n)}.
\end{aligned}$$

(c): For example, the number of necklaces with 12 beads of 2 possible colors is

$$\begin{aligned}
\frac{1}{12} \sum_{i=0}^{11} 2^{\gcd(i,12)} &= \frac{1}{12} \left(2^{12} + 2^1 + 2^2 + 2^3 + 2^4 + 2^1 + 2^6 + 2^1 + 2^4 + 2^3 + 2^2 + 2^1\right) \\
&= \frac{1}{12} \left(4096 + 2 + 4 + 8 + 16 + 2 + 64 + 2 + 16 + 8 + 4 + 2\right) \\
&= 352.
\end{aligned}$$

Remark. Since the number of necklaces is a whole number it follows from our formula that the integer $\sum_{i=0}^{n-1} k^{\gcd(i,n)}$ is always divisible by n, which is not at all obvious. In fact, the easiest case of this observation is just Fermat's Little Theorem. To see this, let $n = p$ be **prime**, so that $\gcd(i, p) = 1$ when $p \nmid i$ and $\gcd(i, p) = p$ when $p | i$. If N is the number of necklaces with p beads in k possible colors then

$$N = \frac{1}{p} \sum_{i=0}^{p-1} k^{\gcd(i,p)} = \frac{1}{p} \left(k^p + \underbrace{k^1 + \cdots + k^1}_{p-1 \text{ times}} \right) = \frac{1}{p} \left(k^p + (p-1)k^1\right).$$

Rearranging gives $k^p - k = p(N + k)$, which shows that $k^p \equiv k \bmod p$.

Remark. Now consider the action of the full symmetric group S_n on the set of words X. To determine an orbit we just need to choose the number of beads of each color, since any two words with the same number of beads of each color will be equivalent by some permutation of the beads. For each $i \in \{1, 2, \ldots, k\}$ let m_i be the number of beads of color i. Our goal is to count the number of possible solutions to the equation $n = m_1 + m_2 + \cdots + m_k$ with $m_i \geq 0$. A standard combinatorial argument says that the answer is $\binom{n+k-1}{k-1}$.[2] Now let $s(n, i)$ be the number of permutations $f \in S_n$ having i cycles. These are called the *Stirling numbers of the first kind.* Putting all of this together, Burnside's Lemma gives a combinatorial identity:

$$\binom{n+k-1}{k-1} = \frac{1}{n!} \cdot \sum_{i=1}^{n} s(n, i) k^i.$$

Since this is just a remark, let me go one step further. By examining $\binom{n+k-1}{k-1}$ more closely we can obtain explicit formulas for the numbers $s(n, i)$. First we note that

$$\binom{n+k-1}{k-1} = \frac{1}{n!} \cdot (k + n - 1)(k + n - 2) \cdots (k + 1).$$

Then expanding the right hand side as a polynomial in k shows that $s(n, i)$ is the sum of products of $n - i$ distinct numbers from the set $\{1, 2, \ldots, n - 1\}$. For example,[3]

$$\begin{aligned} s(4, 1) &= 1 \cdot 2 \cdot 3, \\ s(4, 2) &= 1 \cdot 2 + 1 \cdot 3 + 2 \cdot 3, \\ s(4, 3) &= 1 + 2 + 3, \\ s(4, 4) &= 1. \end{aligned}$$

I find this result surprising.

5. Euler's Totient Function. For any integer $n \geq 1$ we define

$$\phi(n) := \#(\mathbb{Z}/n\mathbb{Z})^\times = \#\{a \in \mathbb{Z} : 1 \leq a \leq n \text{ and } \gcd(a, n) = 1\}.$$

(a) Consider any integer $k \geq 1$ and prime $p \geq 2$. Explain why $\phi(p^k) = p^k - p^{k-1}$. [Hint: The only integers less than p^k that are not coprime to p^k are the multiples of p.]

(b) Let R and S be rings. The *direct product ring* $R \times S$ is defined analogously to groups. It is straightforward to check that the groups of units satisfy

$$(R \times S)^\times = R^\times \times S^\times.$$

Combine this with the Chinese Remainder Theorem to prove for all $m, n \in \mathbb{Z}$ that

$$\gcd(m, n) = 1 \quad \Longrightarrow \quad \phi(mn) = \phi(m)\phi(n).$$

(c) Combine parts (a) and (b) to prove for any integer $n \geq 1$ that

$$\phi(n) = n \cdot \prod_{p \mid n} \frac{p - 1}{p},$$

where the product is over the distinct prime divisors of n. [Hint: Write the prime factorization of n as $n = p_1^{k_1} \cdots p_N^{k_N}$. From part (a) we have $\phi(p_i^{k_i}) = p_i^{k_i} - p_i^{k_i - 1} = p_i^{k_i}(p_i - 1)/p_i$. Now use part (b).]

---

[2] Such a solution corresponds to a binary sequence of length $n + k - 1$ containing n zeros and $k - 1$ ones. The the lengths of the sequences of zeros are the numbers $m_1, \ldots, m_k$ and the ones are the dividers.

[3] A sum of no numbers equals 1 by convention.

(a): For any integer $a \in \mathbb{Z}$ we note that $\gcd(a, p^k) = 1$ if and only if p divides a. Thus $\phi(p^k)$ is the number of integers in the set $\{1, 2, \ldots, p^k\}$ that are **not** multiples of p. The multiples of p in this set are just

$$1p, \quad 2p, \quad 3p, \ldots (p^{k-1})p,$$

and there are p^{k-1} of these. Hence we have

$$\begin{aligned}
\phi(p^k) &= \#(\text{numbers from 1 to } p^k \text{ that are coprime to } p^k) \\
&= \#(\text{numbers from 1 to } p^k \text{ that are not a multiple of } p) \\
&= \#(\text{numbers from 1 to } p^k) - \#(\text{numbers from 1 to } p^k \text{ that are a multiple of } p) \\
&= p^k - p^{k-1} \\
&= p^k \cdot \frac{p-1}{p}.
\end{aligned}$$

(b): If $\gcd(m, n) = 1$ then the Chinese Remainder Theorem gives an isomorphism between the ring $\mathbb{Z}/mn\mathbb{Z}$ and the direct product of rings $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Comparing the groups of units gives

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

and then taking cardinality gives

$$\begin{aligned}
\phi(mn) &= \#(\mathbb{Z}/mn\mathbb{Z})^\times \\
&= \#\left[(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times\right] \\
&= \#(\mathbb{Z}/m\mathbb{Z})^\times \cdot \#(\mathbb{Z}/n\mathbb{Z})^\times \\
&= \phi(m)\phi(n).
\end{aligned}$$

Remark. Here is the ring theory. Let $(R, +, \cdot, 0, 1)$ and $(S, +, \cdot, 0, 1)$ be rings. The direct product ring is just the set of pairs

$$R \times S = \{(r, s) : r \in R, s \in S\}$$

with the componentwise operations $(r, s) + (r', s') = (r + r', s + s')$ and $(r, s)(r', s') = (rr', ss')$. The "zero" and "one" elements of $R \times S$ are $(0, 0)$ and $(1, 1)$. A pair $(r, s) \in R \times S$ is a unit precisely when there exists a pair $(r', s') \in R \times S$ satisfying $(rr', ss') = (r, s)(r', s') = (1, 1) = (r', s')(r, s) = (r'r, ss')$. This is equivalent to saying that $rr' = 1 = r'r$ and $ss' = 1 = s's$ so that r is a unit in R and s is a unit in S. In summary, we have shown that

$$(R \times S)^\times = R^\times \times S^\times.$$

(c): Consider an integer $n \in \mathbb{Z}$ with prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_N^{k_N}$. Then by combining parts (a) and (b) we have

$$\begin{aligned}
\phi(n) &= \phi(p_1^{k_1} p_2^{k_2} \cdots p_N^{k_N}) \\
&= \phi(p_1^{k_1})\phi(p_2^{k_2}) \cdots \phi(p_N^{k_N}) && \text{(b)} \\
&= p_1^{k_1} \cdot \frac{p_1 - 1}{p_1} \cdot p_2^{k_2} \cdot \frac{p_2 - 1}{p_2} \cdots p_N^{k_N} \cdot \frac{p_N - 1}{p_N} && \text{(a)} \\
&= p_1^{k_1} p_2^{k_2} \cdots p_N^{k_N} \cdot \prod_{i=1}^{N} \frac{p_i - 1}{p_i}
\end{aligned}$$

$$= n \cdot \prod_{p|n} \frac{p-1}{p},$$

where the product runs over the distinct prime divisors of n. For example, the distinct prime divisors of $4704 = 2^5 \cdot 3^1 \cdot 7^2$ are just $2, 3, 7$, and hence

$$\phi(4704) = 4704 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7} = 1344.$$

Then since $\gcd(5, 4707) = 1$ we see from Euler's Totient Theorem that

$$5^{1344} = 5^{\phi(4704)} \equiv 1 \bmod 4704.$$

This kind of computation is central to cryptography.

Remark. Multiplying n by $(p-1)/p$ just throws away all of the numbers less than n that are multiples of p. It makes sense that by doing this for every prime divisor of n we are left with just the numbers that are coprime to n. The fact that this procedure gives the correct answer is equivalent to saying that the events $\{a$ is a multiple of $p\}$ are statistically independent for different primes p. I guess this idea could lead to an alternative proof.