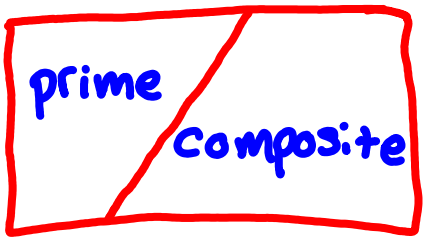
Primes



Def: $p \in \mathbb{N}-\{0,1\}$ is prime if the only positive factors of p are 1 & p

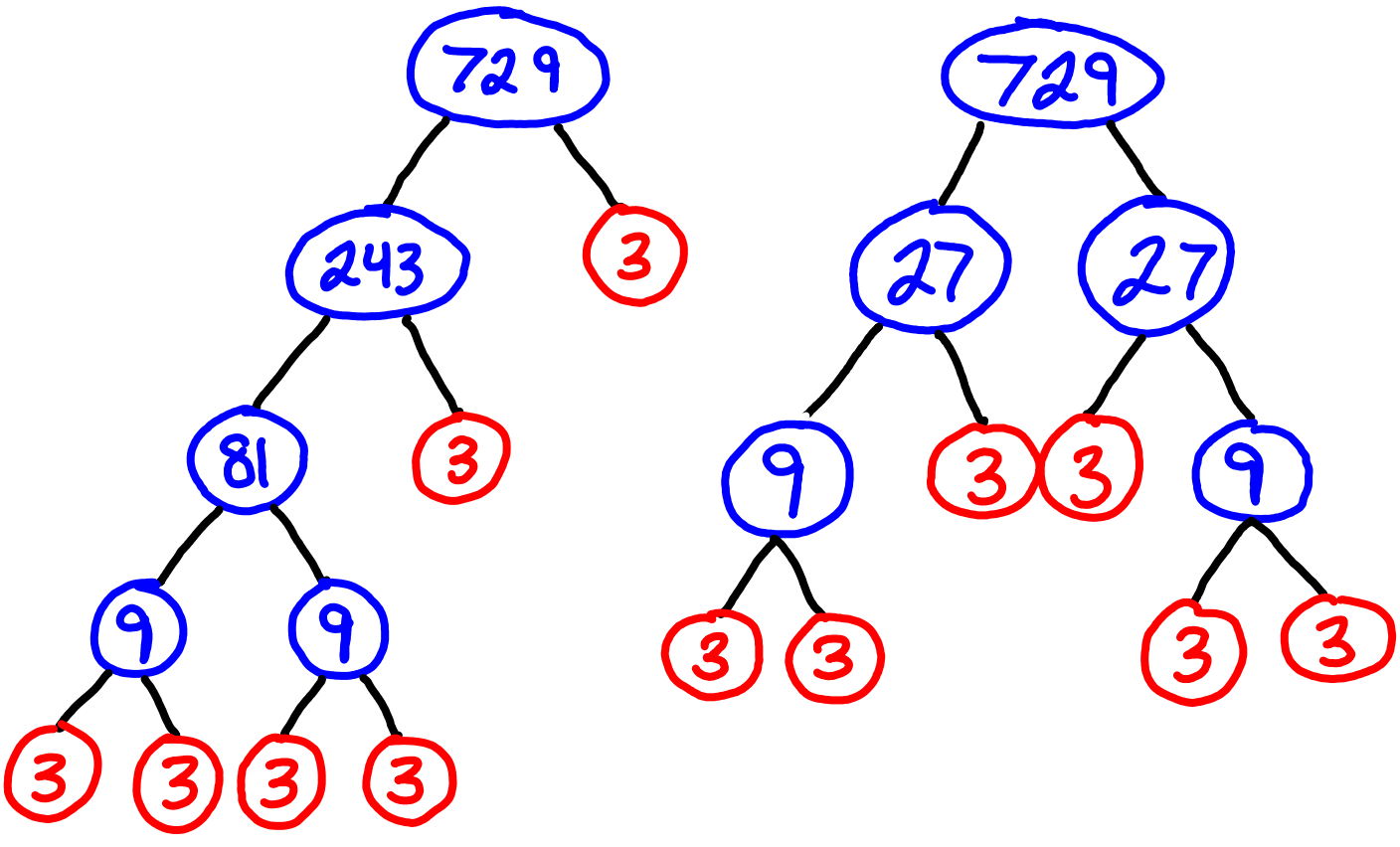
Non-prime numbers are called composite.

Note 0 & 1 are neither prime nor composite (by definition)

prime decomposition & factor trees

■ = composite
■ = prime

$729 = 3^6$



We might be surprised to see these different looking factor trees yield the same prime factorization. This is not a coincidence.

Fundamental Theorem of Arithmetic (FToA)

(uniqueness of prime factorizations)

$\forall x \in \mathbb{N}$ s.t. $x > 1$ $\exists!$ expression for x as a prime or a product of 2 or more primes

↳ uniqueness here either refers to the collection of primes used (w/ ✻ of repetitions counted) or we can ask that the primes appear in non-decreasing order in the factorization

Lemma:

(i) $a, b, c \in \mathbb{Z}_{>0}$

(ii) $\gcd(a,b) = 1$

(iii) $a \mid bc$.

$\Rightarrow a \mid c$

proof:

(ii) $\Rightarrow \exists s, t \in \mathbb{Z}$ s.t. $sa + tb = 1$ (multiply by c)

Bezout ↑

$csa + ctb = c$ (★)

(iii) $\Rightarrow a \mid tbc$ but also $a \mid cas$

thus $a|(tbc+cas) \overset{(\star)}{\iff} a|c$ □

Exercise. $x|y$ & $x|z \Rightarrow x|(y+z)$

↳ this is the fact we used to conclude the last line above.

Lemma: (primes dividing a product must divide one of the factors)

(i) p is prime

(ii) $a_i \in \mathbb{Z} \quad \forall i \leq n$

(iii) $p \mid a_1 a_2 \cdots a_n$

$\Rightarrow p \mid a_i$ for some i

proof: We use the above lemma & Induction

Base case: $n=1$

(iii) $\iff p \mid a_1$ So we are done

Induction Step:

(IH) $p \mid a_1 a_2 \cdots a_k \Rightarrow p \mid a_i$ for some i

Now suppose $p \mid a_1 a_2 \cdots a_{k+1}$

either

↳ $p \mid a_{k+1}$ (in which case we are done)

↳ $\gcd(p, a_{k+1}) = 1$ $(\text{Div}(p) = \{1, p\})$

(the above lemma then says) $\Rightarrow p \mid a_1 a_2 \cdots a_k$

(IH) $\Rightarrow$ $p \mid a_i$ for some $i \leq k$ $\square$

proof of FToA: Proof by contradiction

Suppose $n \in \mathbb{Z}$ has 2 different prime factorizations

$$n = p_1 p_2 \cdots p_s \quad , \quad p_1 \leq p_2 \leq \cdots \leq p_s$$

$$n = q_1 q_2 \cdots q_t \quad , \quad q_1 \leq q_2 \leq \cdots \leq q_t$$

Remove (divide out) all primes common to both factorizations to get

$$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}$$

Lemma $\Rightarrow$ $p_{i_1} \mid q_{j_k}$ for some k

but $p_{i_1} \neq q_{j_k}$ Since we removed all such pairs of primes

but No prime divides any prime $\neq$ to itself.

this is a contradiction hence

prime factorizations are unique. $\square$

A really old theorem: (300 B.C.E. Euclid)

Theorem: $\exists$ infinitely many prime numbers

Proof: Proof by contradiction

assume $p_1, p_2, \ldots, p_n$ is a complete list of primes. Define $Q := p_1 p_2 \ldots p_n + 1$

Either

↳ Q is prime (which is a contradiction)

↳ Q has ≥ 2 prime factors

(uses Fundamental Theorem of Arithmetic)

However, none of the $p_i \mid Q$ because this would imply $p_i \mid (Q - p_1 p_2 \ldots p_n)$ (i.e. $p_i \mid 1$)

impossible

thus, $\exists$ a prime factor of Q which does not appear on our list

□

Note: Q itself need not be prime. We simply know that it must have some prime factor not already on our list. Our proof does not say what this new prime is only that it must exist!

GCD Revisited

Another way to compute GCDs is by using prime factorizations

Suppose

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} \quad \& \quad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

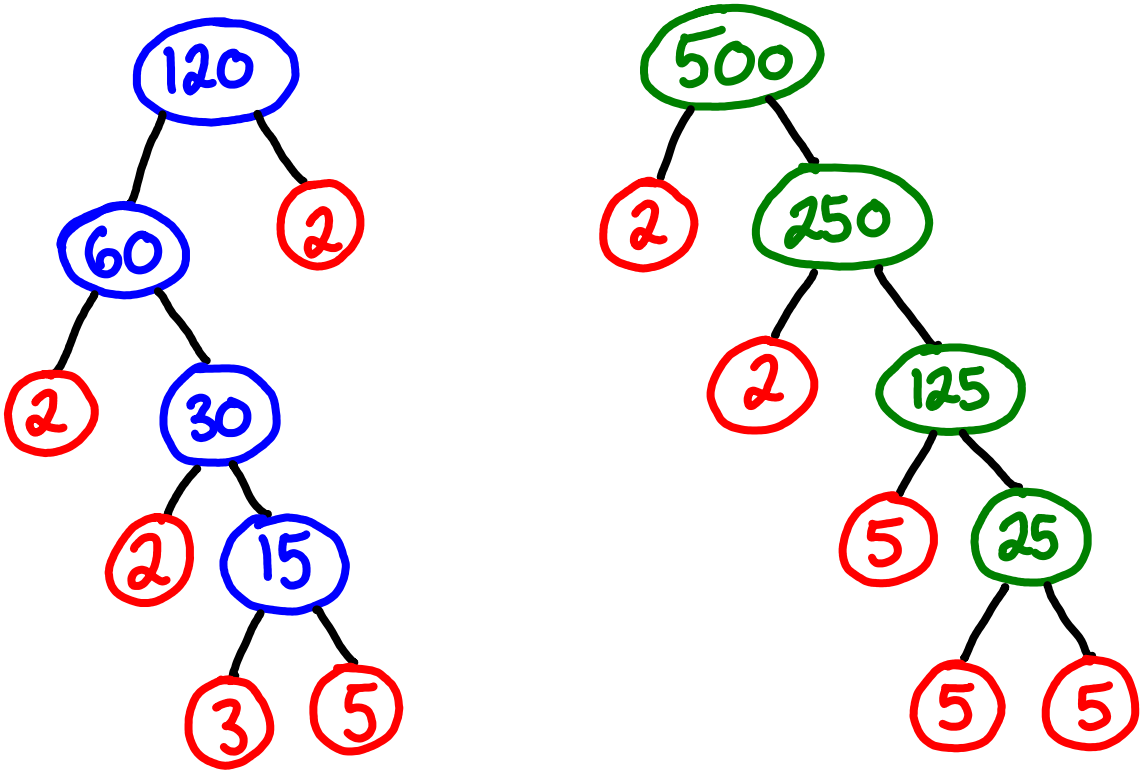
where $a_i, b_i \in \mathbb{N} = \{0, 1, 2, \dots\}$ & p_i are prime

Then $$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)}$$

e.g

$$\gcd(2^4 3^2 5^0 7^1, 2^3 3^2 5^1 7^3) = 2^3 3^2 5^0 7^1 = 504$$

$$\gcd(120, 500) = \gcd(2^3 3^1 5^1, 2^2 5^3) = 2^2 5^1 = 20$$



Least Common Multiples

$\text{lcm}(a,b)$ is defined by the following properties

- $a \mid \text{lcm}(a,b)$
- $b \mid \text{lcm}(a,b)$

} it is a multiple of both a & b

- If $a \mid d$ & $b \mid d$ then $\text{lcm}(a,b) \leq d$

} it is the smallest thing to do so

Similar to how we can use prime factorizations to compute GCDs, we can compute LCMs

$$\text{lcm}(p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n})$$

$$= p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

Theorem: $a \cdot b = \gcd(a,b) \cdot \text{lcm}(a,b)$

Idea for the proof:

$a = 2^3 3^5 7^2$

$b = 2^4 3^3$

$\gcd(a,b) = 2^3 3^3$

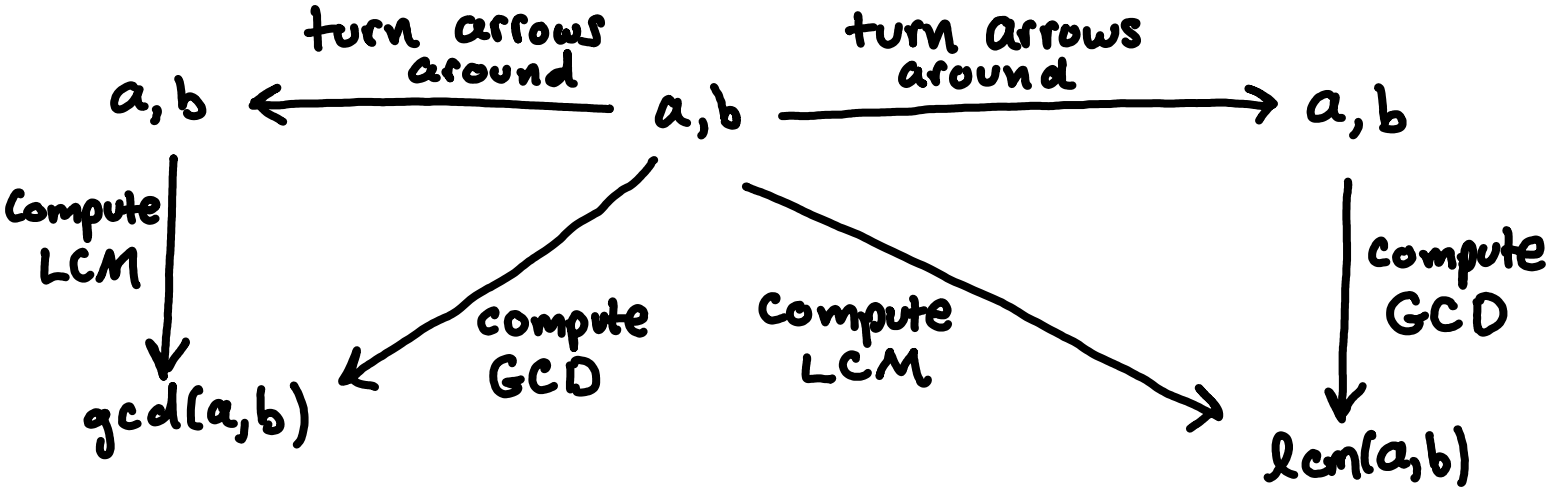
$\text{lcm}(a,b) = 2^4 3^5 7^2$

All factors appear as either max(exponent) or min(exponent)

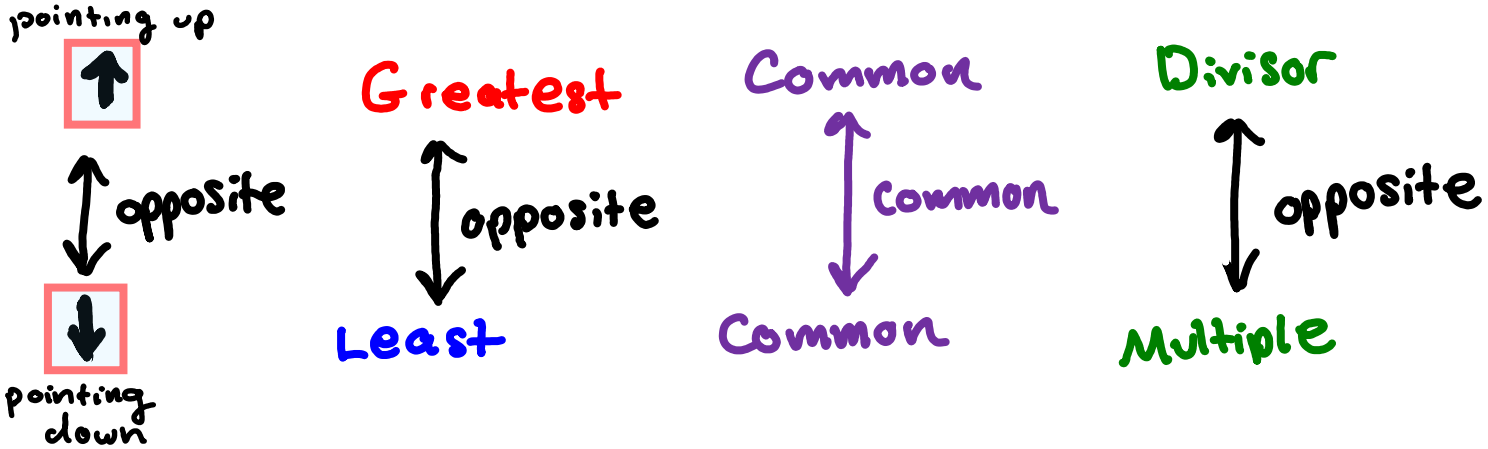
GCD / LCM Duality

The apparent "opposite" relationship shared by Greatest Common Divisors and Least Common Multiples is no mistake. They are computed similarly because each, when paired with the notion of turning arrows around, can be used to define the other.

This is explained by the following schematic.



What happens when we turn arrows around?



How do we compute these quantities?

↑ GCD $\prod_{p \mid a,\ p \mid b,\ p \text{ prime}} p^{\min(a_p, b_p)}$

($\prod$ means take the product of the numbers described)

list of properties we ask each factor to have: $p \mid a$, $p \mid b$, p prime

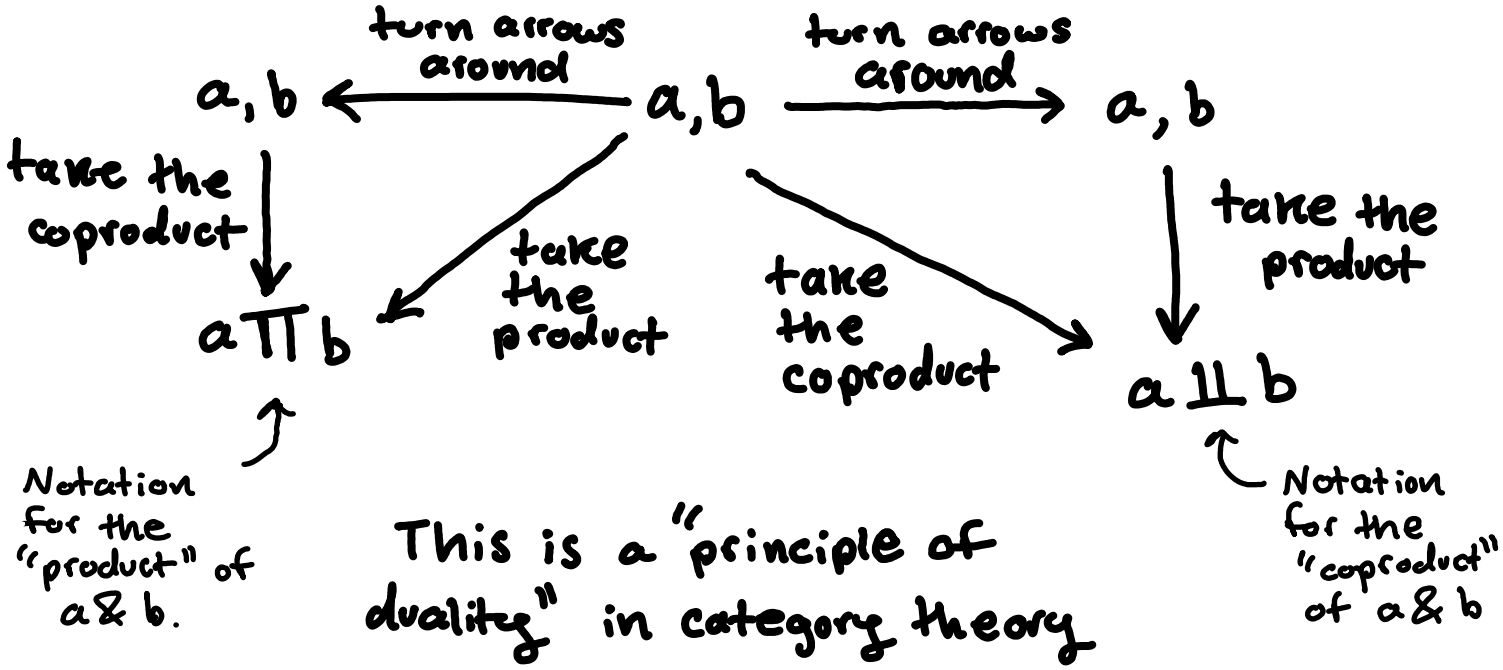
$\min(a_p, b_p)$: the multiplicity (i.e., exponent) of p in b.

a_p: the multiplicity of p in a.

opposite

↓ LCM $\prod_{p \mid a,\ p \mid b,\ p \text{ prime}} p^{\max(a_p, b_p)}$

This is a special case of the following schematic



This is a "principle of duality" in category theory

Main Consequence: Every fact about GCDs should have an interpretation in terms of LCDs (called the dual fact).

The CoEuclidean Algorithm

Recall:

The Division Algorithm

$a = qb + r$

$0 \leq r < b$

Lemma →

The Euclidean Algorithm

Compute: $\gcd(a,b)$

$\gcd(a,b) = \gcd(b,r)$

Fact: $x \cdot y = \gcd(x,y)\,\mathrm{lcm}(x,y)$

⇓

The Division Algorithm

$a = qb + r$

$0 \leq r < b$

Lemma →

The CoEuclidean Algorithm

Compute: $\mathrm{lcm}(a,b)$

$r \mid a\,\mathrm{lcm}(b,r)$

& moreover

$$\frac{a\,\mathrm{lcm}(b,r)}{r} = \mathrm{lcm}(a,b)$$

proof of lemma:

$$ab = \gcd(a,b)\,\mathrm{lcm}(a,b) = \gcd(b,r)\,\mathrm{lcm}(a,b)$$

$$br = \gcd(b,r)\,\mathrm{lcm}(b,r)$$

dividing these equations we get

$$\frac{a}{r} = \frac{ab}{br} = \frac{\gcd(b,r)\,\mathrm{lcm}(a,b)}{\gcd(b,r)\,\mathrm{lcm}(b,r)} = \frac{\mathrm{lcm}(a,b)}{\mathrm{lcm}(b,r)}$$

now, multiply both sides by $\mathrm{lcm}(b,r)$ □

The Euclidean algorithm allows us to solve a difficult form of a problem (computing a GCD) in terms of an easier form of the same problem (easier because the numbers involved are smaller). Eventually this process bottoms out with a trivial version (eventually $x|y$ & when this is the case $\gcd(x,y)=x$). This is to say, the lemma stating

$$a=qb+r,\ 0\le r<b \Rightarrow \gcd(a,b)=\gcd(b,r)$$

allows for a "recursive" calculation of $\gcd(a,b)$.

Similarly, the lemma stating

$$a=qb+r,\ 0\le r<b \Rightarrow \operatorname{lcm}(a,b)=\frac{a\operatorname{lcm}(b,r)}{r}$$

allows for a "recursive" calculation of $\operatorname{lcm}(a,b)$

(because eventually $x|y$ & in this case $\operatorname{lcm}(x,y)=y$)

Note: $x|y \Rightarrow \gcd(x,y)=x,\ \operatorname{lcm}(x,y)=y$

thus $x=y \Leftrightarrow \gcd(x,y)=\operatorname{lcm}(x,y)$

↑

this is easy to prove using the prime factorization definition of lcm & gcd.

Fermat's Little Theorem

$\forall_{\text{primes } p} \quad p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

& $\forall a \in \mathbb{Z} \quad a^p \equiv a \pmod{p}$

proof:

First we show $x, y \in \{a, 2a, 3a, \ldots, (p-1)a\}$

& $x \neq y \Rightarrow x \not\equiv y \pmod{p}$

$p \mid (x-y) \Leftrightarrow p \mid (ia - ja) = (i-j)a$

either $p \mid a$ (but we know this is not the case)

or $p \mid (i-j)$ (but $i < p$, $j < p$ so $p \nmid (i-j)$)

Next we show $(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$

- there are only $p-1$ nonzero equivalence classes in $\mathbb{Z}/p\mathbb{Z}$
- $p \nmid a \cdot i$ for any $i \leq p-1$ (so none of the elements in $\{a, 2a, 3a, \ldots, (p-1)a\}$ represent the zero class)
- Since all pairs represent distinct classes (by the above) we conclude that each class $[1], [2], \ldots, [p-1]$ is represented exactly once by $[a], [2a], \ldots, [(p-1)a]$

Finally we conclude the result of the theorem

first notice $p \nmid (p-1)!$ because otherwise (by the second lemma proven above) p would divide one of the factors of $(p-1)!$ (which we know is not the case since each factor is $< p$).

The rest of the proof is taken care of by the following fact.

Fact:

$$\left.\begin{array}{l} m \in \mathbb{Z}_{>0} \\ a, b, c \in \mathbb{Z} \\ ac \equiv bc \pmod{m} \\ \gcd(c, m) = 1 \end{array}\right| \Rightarrow a \equiv b \pmod{m}$$

proof 1: $\gcd(c,m) = 1 \Rightarrow \exists$ inverse of c mod m □

proof 2: $ac \equiv bc \pmod{m} \Leftrightarrow m \mid ac - bc = c(a-b)$

but $\gcd(c,m) = 1 \Rightarrow m \nmid c \Rightarrow m \mid a-b$

hence $a \equiv b \pmod{m}$ □

Recall: We proved $(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$

& $\gcd((p-1)!, p) = 1$ Thus $a^{p-1} \equiv 1 \pmod{p}$

multiply both sides by a gives $a^p \equiv a \pmod{p}$

provided $p \nmid a$. If $p \mid a$ then $a \equiv 0 \pmod{p}$

hence $a^p \equiv a \pmod{p}$ so $a^p \equiv a \pmod{p}$ $\forall a \in \mathbb{Z}$ □

In particular, $a^{p-1} = 1$ in $\mathbb{Z}/p\mathbb{Z}$ $\forall_{\text{prime}}$ p

Application: (efficient computation of remainders mod primes)

Find $7^{222} \mod 11 = ?$

we know $7^{10} \equiv 1 \pmod{11}$

$$7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} \, 7^2$$

thus $7^{222} \mod 11 = 7^2 \mod 11$

$= 49 \mod 11 = 5$