Lagrange's Theorem.

Binary relation $E(x,y)$ on G.

$E(x,y) = x^{-1} * y \in H$.

Motivation

for $x = y \Rightarrow \frac{y}{x} = 1 \Rightarrow \frac{1}{x} * y = \underbrace{1}_{\varepsilon}$

Reflexivity

$E(x,x) = x^{-1} * x = \varepsilon \in H$.

Symmetry.

$E(x,y) \to E(y,x)$

$x^{-1} * y = h \to y^{-1} * x \in H$.

$(y^{-1} * x)^{-1} = x^{-1} * y$

Transitivity.

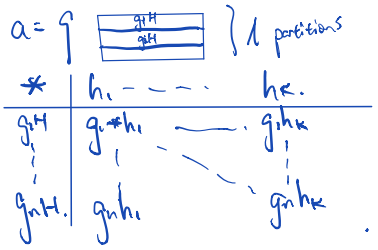
$E(x,y) \wedge E(y,z) \to E(x,z)$.

$x^{-1} * y = h_1, \quad y^{-1} * z = h_2 \quad x^{-1} * z \in H$

$x^{-1} * z = \underbrace{x^{-1}} * y * \underbrace{y^{-1}} * z = h_1 * h_2 \in H$.

Any equivalence relation generate partitions.

$\exists l$. G can be partitioned into l disjoint subset of the same size k such that $n = k \cdot l$.



Claim: $(a*b)^{-1} = a^{-1} * b^{-1}$

Proof:

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

$(a*b) * y = \varepsilon$.

$(a*b) * (a^{-1} * b^{-1}) = \varepsilon$

$a * a^{-1} * b * b^{-1}$

$= \varepsilon * b * b^{-1}$

$= b * b^{-1}$

$= \varepsilon$.

Order of an element a is the smallest integer k such that

$a^k = \varepsilon$.

Example $2^{20} \pmod{15}$.

$G = 0, 1, 2, \cdots 13, 14$.

WT Find $2^k = \varepsilon$ ← such k would exist & k should divide 15.

Given finite group G of order $|G| = n$.

for any a of G, if such order k exist, this k divides n.

$\Downarrow$

$\{\varepsilon, a, a^2, a^3 \cdots a^k\}$. $k \mid n$.

Take a cyclic group generated by a

$\{a^m \mid m \in \mathbb{Z}\} = \{\varepsilon, a, a^2, a^3 \cdots a^k\}$

$G = \{1, 2, 4, 7, 8, 11, 13, 14\}$. ← multiplicative group $\pmod{15}$

$* \Rightarrow * \pmod{15}$

$2^8 \equiv 1 \pmod{15}$

$2^{20} = (2^8)^2 \cdot 2^4$

$= 2^4 \pmod{15}$

$= 1 \pmod{15}$.

Wrong

either $k = 3, 5, 15$.

$2^3 = 8 \equiv 8 \pmod{15}$

$2^5 = 32 \equiv 2 \pmod{15}$

Such that

$2^{15} \equiv 1 \pmod{15}$

$\uparrow \varepsilon$.

$2^{20} = 2^{15} \cdot 2^5 = 1 \cdot 2 \pmod{15} = 2 \pmod{15}$

Having proved $E(x,y)$ on G. $[g] = \{y \mid E(g,y)\}$

$[g] = gH$ ← any Group G can be partitioned in slices

Suppose $a \in G$

$H = \{a, a^2, a^3 \dots\}$ By Lagrange's Theorem $|H| = k$.

$1 \in H$ $a^0 = 1$ why? $n = k \cdot l$.

By Definition. $a^k = 1$.

$a^{-2} = \frac{1}{a^2}$ $a^n = a^{k \cdot l} = (a^k)^l = 1^l = 1$.

$2^{100} \pmod{15} = \underbrace{2^{8 \cdot 12}} \cdot 2^4 = 16 \pmod{15} = 1 \pmod{15}$

8 is the size of multiplication group.

$2^{20} \pmod{17}$

$G = \{1, 2, 3, 4 \dots, 15, 16\}$

$|G| = 16 = p - 1$

prime.

guarantee $2^{16} \equiv 1 \pmod{17}$

$2^{16+4} = 2^{16} \cdot 2^4 \equiv 16 \pmod{17}$

$2^{100} = 2^{16 \cdot 6 + 4} = 16 \pmod{17}$

Euclidean Algorithm

gcd(a,b)

E.g. gcd(90, 32)

$90 = 2 \cdot 32 + 26$

$32 = 1 \cdot 26 + 6$

$26 = 6 \cdot 4 + 2$

$6 = 3 \cdot 2 + 0$

$\gcd(90, 32) = 2.$

partial correctness (Correctness of Result) + termination = total correctness

Proof: gcd(a,b) $\Leftarrow$ Termination.

$a = q_0 \cdot b + r_1$

$b = q_1 \cdot r_1 + r_2$

$r_1 = q_2 \cdot r_2 + r_3$

$\vdots$

$r_{N-1} = q_N \cdot r_N + r_{N+1}$

$r_N = q_{N+1} \cdot r_{N+1} + 0$

$\gcd(a,b) = r_{N+1}$

$a > b > 0.$

$0 < r_1 < b$

$0 < r_2 < r_1$

$\{r_1, \dots, r_{N+1}\}$ integers over 0.

$0 < r_3 < r_2$

$\vdots$

$0 < r_{N+1} < r_N$

Natural numbers are finite.

Guarantee that this algo will eventually stop.

State k $d_k = \gcd(r_{k-1}, r_k)$

$k+1$ $d_{k+1} = \gcd(r_k, r_{k+1})$

WTS $d_k = d_{k+1}$

$r_{k-1} = d_k \cdot n.$

$r_k = d_k \cdot n'$

$r_{k-1} = q_k \cdot r_k + r_{k+1}.$

$r_{k+1} = r_{k-1} - q_k \cdot r_k = d_k(n - q_k \cdot h')$

d_k is a common divisor of (r_k, r_{k+1}, r_{k-1})

$d_k \geq d_{k+1}$

conversely $d_{k+1} \geq d_k.$

$d_{k+1} = d_k.$

$d_0 = \dots = d_{N+1} = \gcd(r_N, r_{N+1}) = r_{N+1}.$

$r_0 = r_{n+1} = \gcd(a,b)$.

$\gcd(a,b)$ as a linear combination of a and b.

E.g. $2 = k_1 \cdot 90 + k_2 \cdot 32$.

$a = 2 \cdot b + r_1$
$b = 1 \cdot r_1 + r_2$
$r_1 = 4 \cdot r_2 + r_3$
$r_2 = 3 \cdot r_3$

$r_3 = 2$.
$r_3 = r_1 - 4r_2$
$= r_1 - 4(b - r_1)$
$= -4b + 5r_1$
$= -4b + 5(a - 2b)$
$= 5a - 14b$

$\gcd(90, 32) = 5 \times 90 - 14 \times 32 = 2$.

4^{-1} : Find y such that $4 \times y = 1 \pmod{17}$

$\gcd(4, 17) = 1 = k_1 \cdot 4 + k_2 \cdot 17$

$k_1 = -4 \quad k_2 = 1$

$4^4 \equiv 1 \pmod{17}$

$\gcd(34, 13) = 1$

$34 = 2 \cdot 13 + 8$
$13 = 1 \cdot 8 + 5$
$8 = 1 \cdot 5 + 3$
$5 = 1 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 2 \cdot 1$

$1 = k_1 \cdot 34 + k_2 \cdot 13$.

$1 = r_3 - r_4 = r_3 - (r_2 - r_3)$
$= -r_2 + 2r_3 = -r_2 + 2(r_1 - r_2)$
$= 2r_1 - 3r_2 = 2r_1 - 3(b - r_1)$
$= -3b + 5r_1 = -3b + 5(a - 2b)$
$= 5a - 13b$

$a = 34 \quad b = 13$

$5a = 1 + 13b$
$a \cdot 5 = 1 \pmod{169}$
$5 = (34)^{-1} \pmod{169}$