A String of Pearls

Proofs of Fermat's Little Theorem

Hing-Lun Chan[1] Michael Norrish[2]

[1]College of Engineering and Computer Science
Australian National University (ANU)

[2]Software Systems Research Group
Canberra Research Lab., NICTA
(*also*, ANU)

Conference on Certified Programs and Proofs, 2012

Fermat's Letter (1640)

Pierre de Fermat (1601–1665)

- Letter to Frénicle de Bessy dated October 18, 1640:

  p *divides* $a^{p-1} - 1$ *whenever* p *is prime and* a *is coprime to* p*.*
  […] the proof of which I would send to you, if I were not afraid to be too long.

Fermat's Letter (1640)

Pierre de Fermat (1601–1665)

- Letter to Frénicle de Bessy dated October 18, 1640:

  p divides $a^{p-1} - 1$ whenever p is prime and a is coprime to p.
  [. . .] the proof of which I would send to you, if I were not afraid to be too long.

- Modern notation:
  $a^{p-1} \equiv 1 \mod p$ for prime p and a coprime to p, or
  $a^p \equiv a \mod p$ for prime p and any a.

Fermat's Letter (1640)

Pierre de Fermat (1601–1665)

- Letter to Frénicle de Bessy dated October 18, 1640:

  p *divides* $a^{p-1} - 1$ *whenever* p *is prime and* a *is coprime to* p*.*
  [...] the proof of which I would send to you, if I were not afraid to be too long.

- Modern notation:
  $a^{p-1} \equiv 1 \mod p$ for prime p and a coprime to p, or
  $a^p \equiv a \mod p$ for prime p and any a.

- Examples:
  $18^{23} = 74347713614021927913318776832 \equiv 18 \mod 23$
  $19^{23} = 257829627945307727248226067259 \equiv 19 \mod 23$

Euler's Proof (1758)

- The remainders of division by $p = 7$:
  $$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \cdots\} \mod 7$$
  $$= \{0, 1, 2, 3, 4, 5, 6\} \mod 7$$

Euler's Proof (1758)

- The remainders of division by $p = 7$:
  $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \cdots\} \mod 7$
  $= \{0, 1, 2, 3, 4, 5, 6\} \mod 7$
- Multiply each remainder by $a = 3$:
  $\{3 \times 0, 3 \times 1, 3 \times 2, 3 \times 3, 3 \times 4, 3 \times 5, 3 \times 6\} \mod 7$
  $= \{0, 3, 6, 9, 12, 15, 18\} \mod 7$
  $= \{0, 3, 6, 2, \ \ 5, \ \ 1, \ 4\} \mod 7$ (a permutation of above)

Euler's Proof (1758)

- The remainders of division by $p = 7$:
  $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \cdots\} \mod 7$
  $= \{0, 1, 2, 3, 4, 5, 6\} \mod 7$
- Multiply each remainder by $a = 3$:
  $\{3 \times 0, 3 \times 1, 3 \times 2, 3 \times 3, 3 \times 4, 3 \times 5, 3 \times 6\} \mod 7$
  $= \{0, 3, 6, 9, 12, 15, 18\} \mod 7$
  $= \{0, 3, 6, 2, \ \ 5, \ \ 1, \ \ 4\} \mod 7$ (a permutation of above)
- Multiply all nonzero numbers in each set:
  $(3 \times 1)(3 \times 2)(3 \times 3)(3 \times 4)(3 \times 5)(3 \times 6) \mod 7$
  $= (3)(6)(2)(5)(1)(4) \mod 7$

Euler's Proof (1758)

- The remainders of division by $p = 7$:
  $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \cdots\} \mod 7$
  $= \{0, 1, 2, 3, 4, 5, 6\} \mod 7$
- Multiply each remainder by $a = 3$:
  $\{3 \times 0, 3 \times 1, 3 \times 2, 3 \times 3, 3 \times 4, 3 \times 5, 3 \times 6\} \mod 7$
  $= \{0, 3, 6, 9, 12, 15, 18\} \mod 7$
  $= \{0, 3, 6, 2, \quad 5, \quad 1, \ 4\} \mod 7$ (a permutation of above)
- Multiply all nonzero numbers in each set:
  $(3 \times 1)(3 \times 2)(3 \times 3)(3 \times 4)(3 \times 5)(3 \times 6) \mod 7$
  $= (3)(6)(2)(5)(1)(4) \mod 7$
- Collect common factors on the left, rearrange the right:
  $3^6 \times (1)(2)(3)(4)(5)(6) \mod 7 = (1)(2)(3)(4)(5)(6) \mod 7$

Euler's Proof (1758)

- The remainders of division by $p = 7$:
  $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \cdots\} \mod 7$
  $= \{0, 1, 2, 3, 4, 5, 6\} \mod 7$
- Multiply each remainder by $a = 3$:
  $\{3 \times 0, 3 \times 1, 3 \times 2, 3 \times 3, 3 \times 4, 3 \times 5, 3 \times 6\} \mod 7$
  $= \{0, 3, 6, 9, 12, 15, 18\} \mod 7$
  $= \{0, 3, 6, 2, \quad 5, \quad 1, \quad 4\} \mod 7$ (a permutation of above)
- Multiply all nonzero numbers in each set:
  $(3 \times 1)(3 \times 2)(3 \times 3)(3 \times 4)(3 \times 5)(3 \times 6) \mod 7$
  $= (3)(6)(2)(5)(1)(4) \mod 7$
- Collect common factors on the left, rearrange the right:
  $3^6 \times (1)(2)(3)(4)(5)(6) \mod 7 = (1)(2)(3)(4)(5)(6) \mod 7$
- Cancel to give: $3^6 \equiv 1 \mod 7$, or $3^7 \equiv 3 \mod 7$.

Euler's Proof (1758)

- In general, $\{a \times x \mod p\}$ is a permutation of $\{x \mod p\}$ when p is prime. In product form, excluding $x = 0$,

$$\prod (a \times x) \equiv \prod (x) \mod p \quad \text{for prime } p.$$

- Collect common factors a on the left:

$$a^{p-1} \prod (x) \equiv \prod (x) \mod p \quad \text{for prime } p.$$

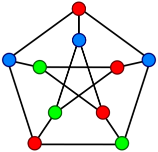
- Cancel non-zero $\prod (x) \mod p$ on both sides gives: $a^{p-1} \equiv 1 \mod p \quad \text{for prime } p.$

- Multiply by a gives the equivalent form: $a^p \equiv a \mod p \quad \text{for prime } p.$

Mechanisation of Fermat's Little Theorem

- Most theorem-proving systems (*e.g.* Coq, ACL2, *etc.*) mechanise this theorem based on Euler's proof.
  - Some prove Fermat's Little Theorem directly.
  - Others prove Euler's generalization first, then derive Fermat's Little Theorem as a special case.
- Why is this number-theoretic approach so popular?
  - Proof is simple to do, found in standard textbooks.
  - Systems have good built-in theories for natural numbers.
- A proof distributed in recent HOL4 is based on induction via binomial expansion.
  - This induction method was used in the first published proof of Fermat's Little Theorem by Euler in 1736.
  - Same method was used by Leibniz (1646–1716) in an unpublished and undated manuscript, discovered in 1894.

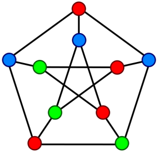
Petersen's Proof (1872)



Julius Petersen (1839–1910), famous for his Petersen Graph.

> *Take p elements from q with repetitions in all ways, that is, in q^p ways. The q sets with elements all alike are not changed by a cyclic permutation of the elements, while the remaining $q^p - q$ sets are permuted in sets of p [when p is prime]. Hence p divides $q^p - q$.*

Petersen's Proof (1872)



Julius Petersen (1839–1910), famous for his Petersen Graph.

> *Take p elements from q with repetitions in all ways, that is, in q^p ways. The q sets with elements all alike are not changed by a cyclic permutation of the elements, while the remaining $q^p - q$ sets are permuted in sets of p [when p is prime]. Hence p divides $q^p - q$.*

- Petersen uses p's and q's, Fermat uses p's and a's.
- $a^p \equiv a \mod p$ is equivalent to: p divides $a^p - a$.

Petersen's Proof – Necklace Form

Take p elements from q with repetitions in all ways, i.e. q^p ways.

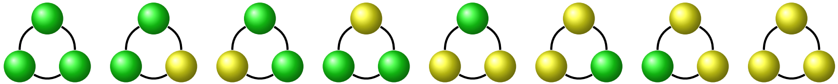
Take p beads from a colours with repetitions, i.e. a^p necklaces.

Petersen's Proof – Necklace Form

Take p elements from q with repetitions in all ways, i.e. q^p ways.

Take p beads from a colours with repetitions, i.e. a^p necklaces.

Example: 3-bead necklaces with 2 colours, $2^3 = 8$.

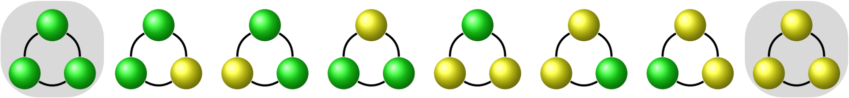


Petersen's Proof – Necklace Form

Take p elements from q with repetitions in all ways, i.e. q^p ways.
The q sets with elements all alike are not changed by a cyclic permutation of the elements,

Take p beads from a colours with repetitions, i.e. a^p necklaces.
Those with beads all alike cycle to themselves, 1 for each colour, so there are a of them.

Example: 3-bead necklaces with 2 colours, $2^3 = 8$.

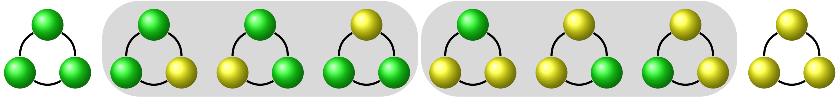


Petersen's Proof – Necklace Form

Take p elements from q with repetitions in all ways, i.e. q^p ways. The q sets with elements all alike are not changed by a cyclic permutation of the elements, while the remaining $q^p - q$ sets are permuted in sets of p when p is prime.

Take p beads from a colours with repetitions, i.e. a^p necklaces. Those with beads all alike cycle to themselves, 1 for each colour, so there are a of them. The other $a^p - a$ necklaces cycle to one another in sets of size p for prime p.

Example: 3-bead necklaces with 2 colours, $2^3 = 8$.

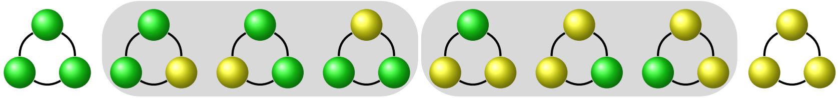


Petersen's Proof – Necklace Form

Take p elements from q with repetitions in all ways, i.e. q^p ways. The q sets with elements all alike are not changed by a cyclic permutation of the elements, while the remaining $q^p - q$ sets are permuted in sets of p when p is prime. Hence p divides $q^p - q$ [, which is Fermat's Little Theorem].

Take p beads from a colours with repetitions, i.e. a^p necklaces. Those with beads all alike cycle to themselves, 1 for each colour, so there are a of them. The other $a^p - a$ necklaces cycle to one another in sets of size p for prime p. Equal size partition is visual divisibility, so p divides $a^p - a$.

Example: 3-bead necklaces with 2 colours, $2^3 = 8$.

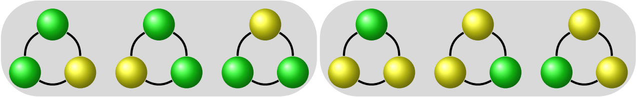


Petersen's Proof – Necklace Form

Take p *elements from* q *with repetitions in all ways, i.e.* q^p *ways. The* q *sets with elements all alike are not changed by a cyclic permutation of the elements, while the remaining* $q^p - q$ *sets are permuted in sets of* p *when* p *is prime. Hence* p *divides* $q^p - q$ *[, which is Fermat's Little Theorem].*

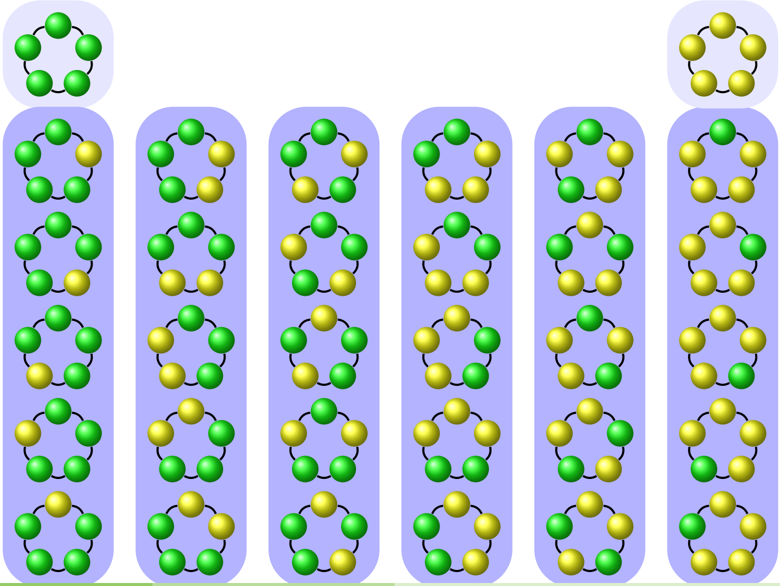
Take p *beads from* a *colours with repetitions, i.e.* a^p *necklaces. Those with beads all alike cycle to themselves,* 1 *for each colour, so there are* a *of them. The other* $a^p - a$ *necklaces cycle to one another in sets of size* p *for prime* p*. Equal size partition is visual divisibility, so* p *divides* $a^p - a$*.*

Example: 3-bead necklaces with 2 colours, $2^3 = 8$. $2^3 - 2 = 6$.



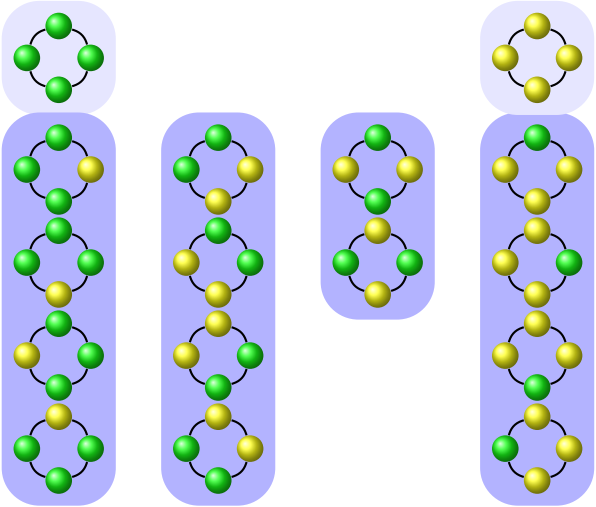
Necklace Proof

5-bead necklaces with 2 colours, $2^5=32$; "good" cycle partitions.



Necklace Proof

4-bead necklaces with 2 colours, $2^4 = 16$; "bad" cycle partitions.



Necklace Theorem

Theorem

For prime p, the p-bead necklaces have "good" cycle partitions:

Of the necklaces with prime p beads made out of a colours:

- *the a monocoloured necklaces cycle in singletons.*
- *the $a^p - a$ multicoloured necklaces cycle in sets of equal size p.*

Necklace Theorem

Theorem

For prime p, the p-bead necklaces have "good" cycle partitions:

Of the necklaces with prime p beads made out of a colours:

- *the a monocoloured necklaces cycle in singletons.*
- *the $a^p - a$ multicoloured necklaces cycle in sets of equal size p.*

Julius Petersen claims:

- Necklace Theorem is straight-forward, easy to see.
- Fermat's Little Theorem follows as a simple corollary.

Necklace Theorem

Theorem

For prime p, the p-bead necklaces have "good" cycle partitions:

Of the necklaces with prime p beads made out of a colours:

- *the a monocoloured necklaces cycle in singletons.*
- *the $a^p - a$ multicoloured necklaces cycle in sets of equal size p.*

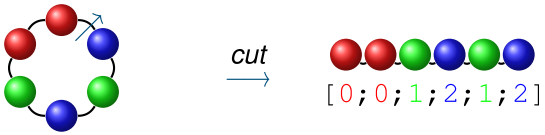
Julius Petersen claims:

- Necklace Theorem is straight-forward, easy to see.
- Fermat's Little Theorem follows as a simple corollary.

However, theorem-provers cannot "see"!

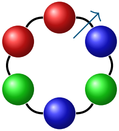
Mechanisation of Necklace Proof – Part 1

- Represent necklaces with n beads by a list of length n.
  Represent a colours by numbers in $\{0, 1, 2, \ldots, (a-1)\}$.

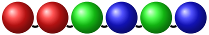


Mechanisation of Necklace Proof – Part 1

- Represent necklaces with n beads by a list of length n.
  Represent a colours by numbers in $\{0, 1, 2, \ldots, (a-1)\}$.



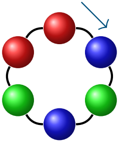
cut $\longrightarrow$



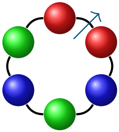
`[0;0;1;2;1;2]`

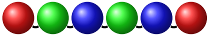
- Cycle of necklace = append list DROP with list TAKE.

```
TAKE 1 [0;0;1;2;1;2] = [0]
DROP 1 [0;0;1;2;1;2] = [0;1;2;1;2]
```



cycle by 1 *bead* $\longrightarrow$





`[0;1;2;1;2] ++ [0] = [0;1;2;1;2;0]`

Mechanisation of Necklace Proof – Part 2

- Define monocoloured and multicoloured necklaces.

$$\vdash \texttt{monocoloured}\ n\ a = \{\ell \mid \ell \in \texttt{necklace}\ n\ a \wedge (\ell \neq [\,] \Rightarrow \texttt{SING}\ (\texttt{set}\ \ell))\}$$

$$\vdash \texttt{multicoloured}\ n\ a = \texttt{necklace}\ n\ a \setminus \texttt{monocoloured}\ n\ a$$

- Count the monocoloured and multicoloured necklaces.

$$\vdash 0 < n \Rightarrow |\texttt{monocoloured}\ n\ a| = a$$

$$\vdash 0 < n \Rightarrow |\texttt{multicoloured}\ n\ a| = a^n - a$$

Mechanisation of Necklace Proof – Part 3

- Two necklaces are similar if they can cycle to one another.

  $\vdash \ell_1 == \ell_2 \iff \exists n.\ \ell_2 = \texttt{cycle}\ n\ \ell_1$

- Being similar is an equivalence relation for necklaces.

  $\vdash \ell == \ell$

  $\vdash \ell_1 == \ell_2 \Rightarrow \ell_2 == \ell_1$

  $\vdash \ell_1 == \ell_2 \land \ell_2 == \ell_3 \Rightarrow \ell_1 == \ell_3$

- For prime p, equivalence classes of similar (associates) are of equal size: 1 for monocoloured, p for multicoloured.

  $\vdash \ell \neq [] \land \texttt{prime}\ |\ell| \Rightarrow$
  $\quad |\texttt{associates}\ \ell| = 1 \lor |\texttt{associates}\ \ell| = |\ell|$

- From this, Necklace Theorem can be proved *(see paper)*, and Fermat's Little Theorem follows.

Group and Group Action

- A Group $\longrightarrow$ acts on $\longrightarrow$ A Set of Objects.
- Each group element $\longrightarrow$ acts on $\longrightarrow$ an object in the Set.

Group and Group Action

- A Group $\longrightarrow$ acts on $\longrightarrow$ A Set of Objects.
- Each group element $\longrightarrow$ acts on $\longrightarrow$ an object in the Set.

+	Odd	Even
Odd	Even	Odd
Even	Odd	Even

$\oplus$	1	0
1	0	1
0	1	0

Group and Group Action

- A Group $\longrightarrow$ acts on $\longrightarrow$ A Set of Objects.
- Each group element $\longrightarrow$ acts on $\longrightarrow$ an object in the Set.

+	Odd	Even
Odd	Even	Odd
Even	Odd	Even

Parity Group

$\oplus$	1	0
1	0	1
0	1	0

$$\mathbb{Z}_2^+ = \{0, 1\}$$

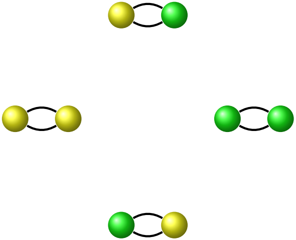
Group and Group Action

- A Group $\longrightarrow$ acts on $\longrightarrow$ A Set of Objects.
- Each group element $\longrightarrow$ acts on $\longrightarrow$ an object in the Set.

+	Odd	Even
Odd	Even	Odd
Even	Odd	Even

Parity Group

acts on
2-bead necklaces:



$\oplus$	1	0
1	0	1
0	1	0

$$\mathbb{Z}_2^+ = \{0, 1\}$$

Group and Group Action

- A Group $\longrightarrow$ acts on $\longrightarrow$ A Set of Objects.
- Each group element $\longrightarrow$ acts on $\longrightarrow$ an object in the Set.

+	Odd	Even
Odd	Even	Odd
Even	Odd	Even

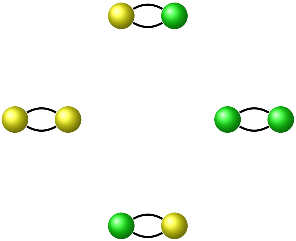
Parity Group

acts on
2-bead necklaces:

$\oplus$	1	0
1	0	1
0	1	0

0 cycle by 0 bead

1 cycle by 1 bead



$$\mathbb{Z}_2^+ = \{0, 1\}$$

Group and Group Action

- A Group $\longrightarrow$ acts on $\longrightarrow$ A Set of Objects.
- Each group element $\longrightarrow$ acts on $\longrightarrow$ an object in the Set.

+	Odd	Even
Odd	Even	Odd
Even	Odd	Even

$\oplus$	1	0
1	0	1
0	1	0

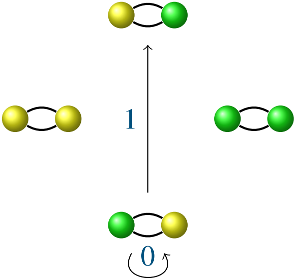
Parity Group

acts on
2-bead necklaces:

0 cycle by 0 bead

1 cycle by 1 bead

$$\mathbb{Z}_2^+ = \{0, 1\}$$



Group and Group Action

- A Group $\longrightarrow$ acts on $\longrightarrow$ A Set of Objects.
- Each group element $\longrightarrow$ acts on $\longrightarrow$ an object in the Set.

+	Odd	Even
Odd	Even	Odd
Even	Odd	Even

$\oplus$	1	0
1	0	1
0	1	0

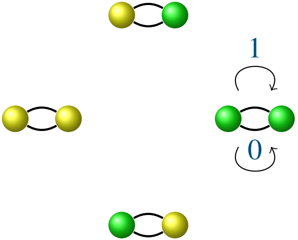
Parity Group

acts on
2-bead necklaces:

0 cycle by 0 bead

1 cycle by 1 bead

$\mathbb{Z}_2^+ = \{0, 1\}$



Group and Group Action

- A Group $\longrightarrow$ acts on $\longrightarrow$ A Set of Objects.
- Each group element $\longrightarrow$ acts on $\longrightarrow$ an object in the Set.

+	Odd	Even
Odd	Even	Odd
Even	Odd	Even

$\oplus$	1	0
1	0	1
0	1	0

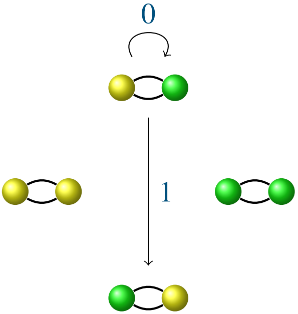
Parity Group

acts on
2-bead necklaces:

0 cycle by 0 bead

1 cycle by 1 bead

$$\mathbb{Z}_2^+ = \{0, 1\}$$



Group and Group Action

- A Group $\longrightarrow$ acts on $\longrightarrow$ A Set of Objects.
- Each group element $\longrightarrow$ acts on $\longrightarrow$ an object in the Set.

+	Odd	Even
Odd	Even	Odd
Even	Odd	Even

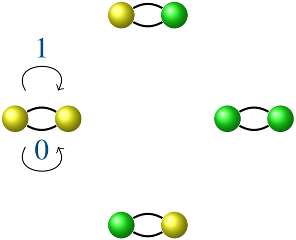
$\oplus$	1	0
1	0	1
0	1	0

Parity Group

acts on
2-bead necklaces:

0 cycle by 0 bead

1 cycle by 1 bead



$$\mathbb{Z}_2^+ = \{0, 1\}$$

Group and Group Action

- A Group $\longrightarrow$ acts on $\longrightarrow$ A Set of Objects.
- Each group element $\longrightarrow$ acts on $\longrightarrow$ an object in the Set.

+	Odd	Even
Odd	Even	Odd
Even	Odd	Even

$\oplus$	1	0
1	0	1
0	1	0

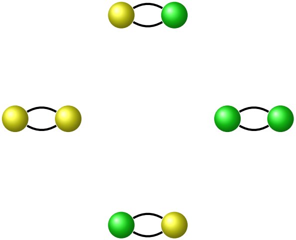
Parity Group

acts on
2-bead necklaces:

0 cycle by 0 bead

1 cycle by 1 bead

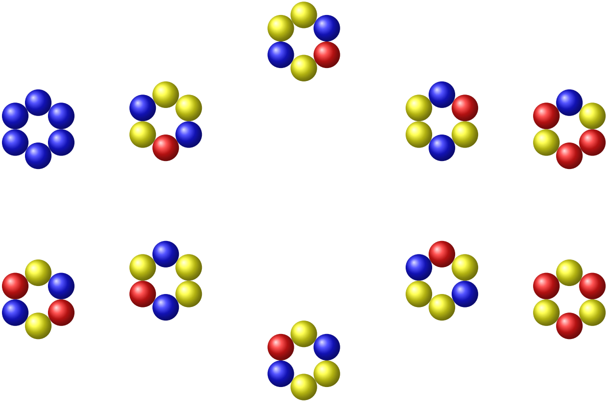
$$\mathbb{Z}_2^+ = \{0, 1\}$$



- Group $\mathbb{Z}_n^+$ acts on the set of n-bead necklaces, for any n (prime or not prime).

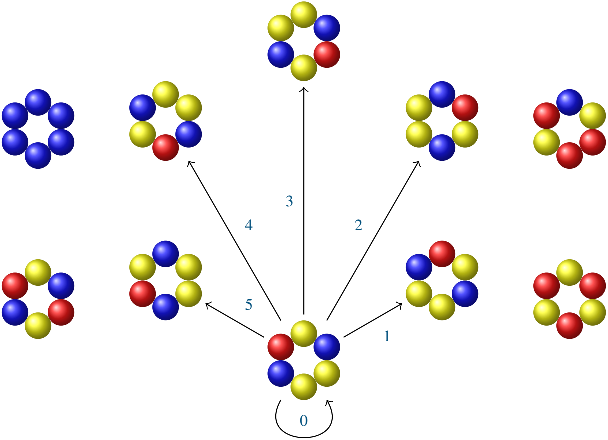
Group Action on Necklaces

- Cycle: action of $\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\}$ on 6-bead necklaces.



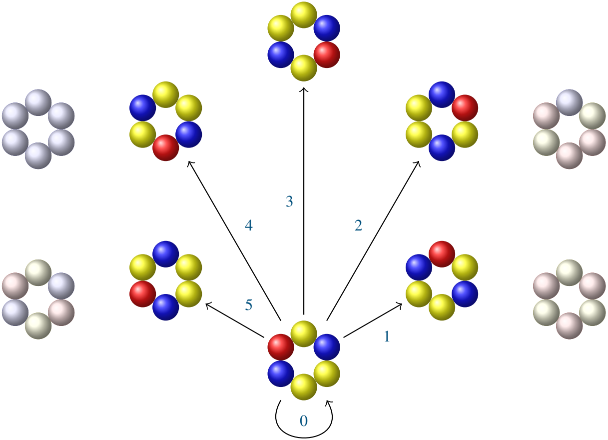
Group Action on Necklaces

- Cycle: action of $\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\}$ on 6-bead necklaces.



Group Action on Necklaces

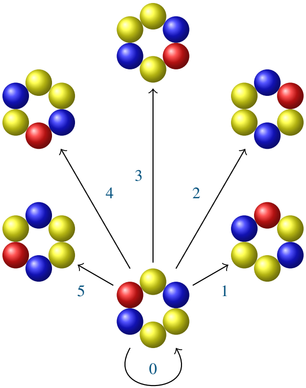
- Cycle: action of $\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\}$ on 6-bead necklaces.



- Similar necklaces of cycle = Orbit.
- Group elements that give loop action = Stabilizer.

Orbit and Stabilizer – Part 1

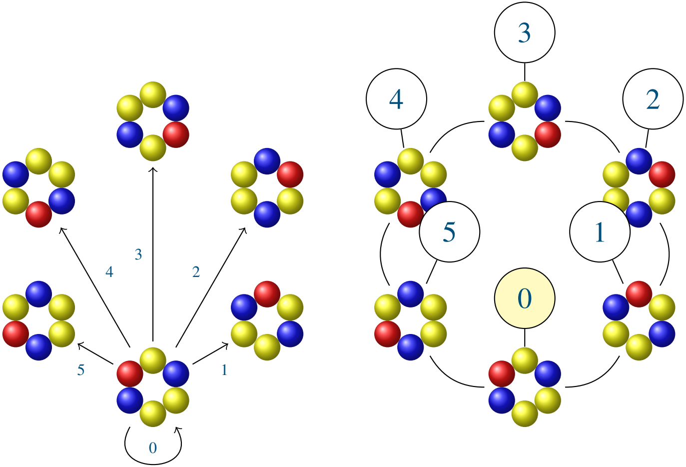
- Action of $\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\}$ on one 6-bead necklace.



- Orbit = similar necklaces of cycle.
- Stabilizer = elements that give loop.

Orbit and Stabilizer – Part 1

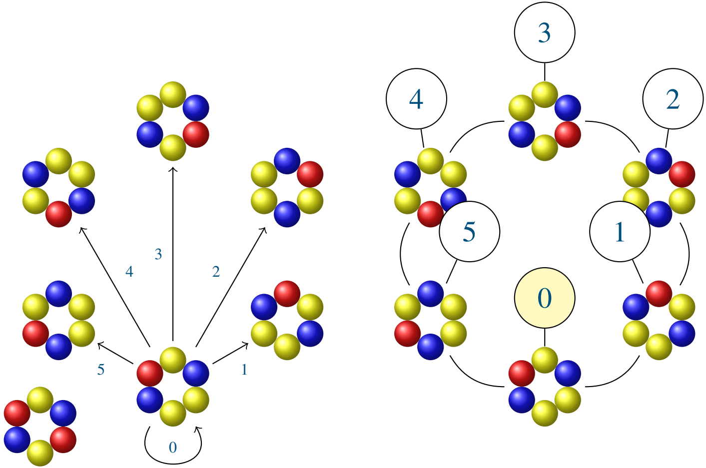
- Action of $\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\}$ on one 6-bead necklace.



- Orbit = similar necklaces of cycle. Size of orbit = 6.
- Stabilizer = elements that give loop. Size of stabilizer = 1.

Orbit and Stabilizer – Part 1

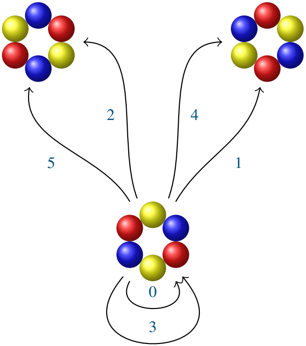
- Action of $\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\}$ on one 6-bead necklace.



- Orbit = similar necklaces of cycle. Size of orbit = 6.
- Stabilizer = elements that give loop. Size of stabilizer = 1.

Orbit and Stabilizer – Part 2

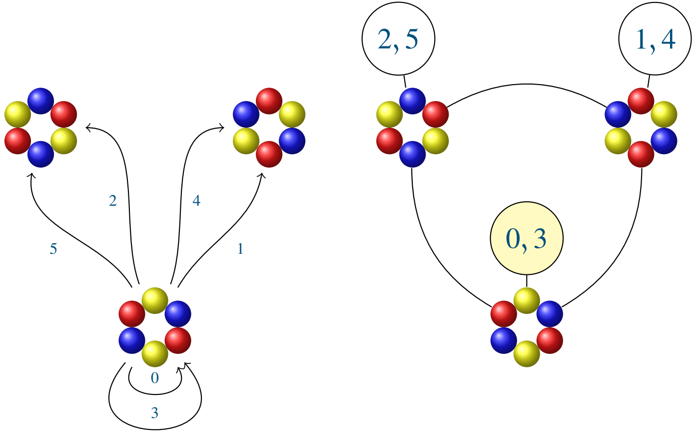
- Action of $\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\}$ on another 6-bead necklace.



- Orbit = similar necklaces of cycle.
- Stabilizer = elements that give loop.

Orbit and Stabilizer – Part 2

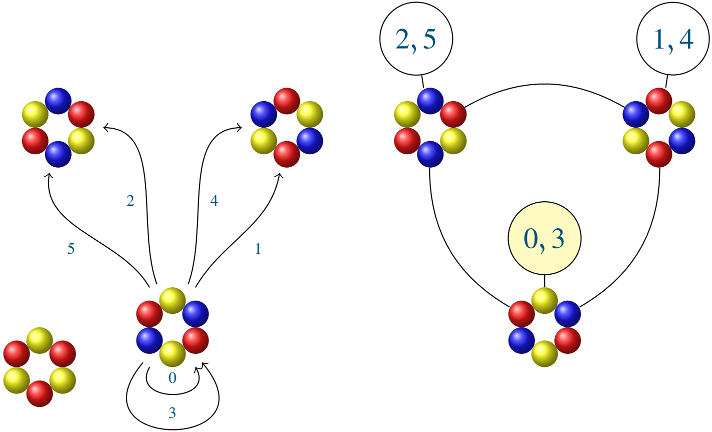
- Action of $\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\}$ on another 6-bead necklace.



- Orbit = similar necklaces of cycle. Size of orbit = 3.
- Stabilizer = elements that give loop. Size of stabilizer = 2.

Orbit and Stabilizer – Part 2

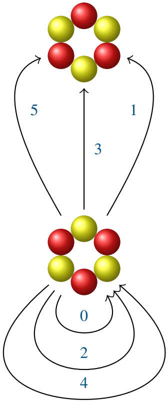
- Action of $\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\}$ on another 6-bead necklace.



- Orbit = similar necklaces of cycle. Size of orbit = 3.
- Stabilizer = elements that give loop. Size of stabilizer = 2.

Orbit and Stabilizer – Part 3

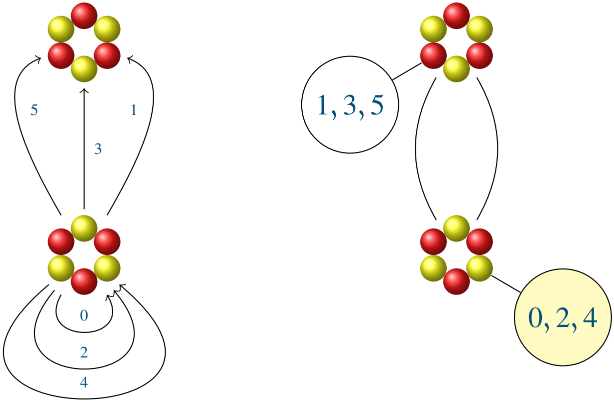
- Action of $\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\}$ on another 6-bead necklace.



- Orbit = similar necklaces of cycle.
- Stabilizer = elements that give loop.

Orbit and Stabilizer – Part 3

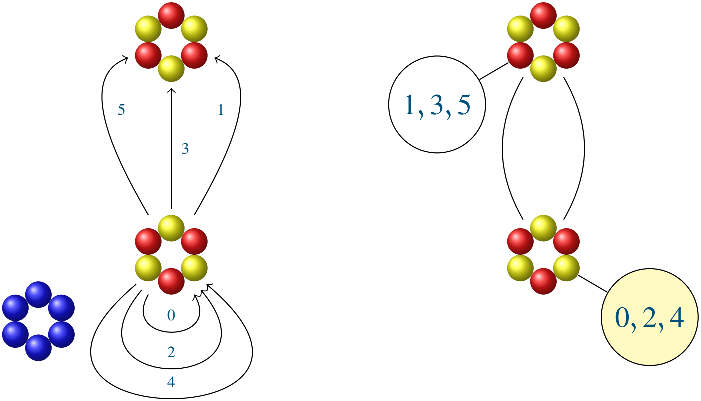
- Action of $\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\}$ on another 6-bead necklace.



- Orbit = similar necklaces of cycle. Size of orbit = 2.
- Stabilizer = elements that give loop. Size of stabilizer = 3.

Orbit and Stabilizer – Part 3

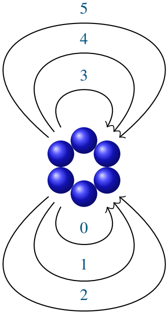
- Action of $\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\}$ on another 6-bead necklace.



- Orbit = similar necklaces of cycle. Size of orbit = 2.
- Stabilizer = elements that give loop. Size of stabilizer = 3.

Orbit and Stabilizer – Part 4

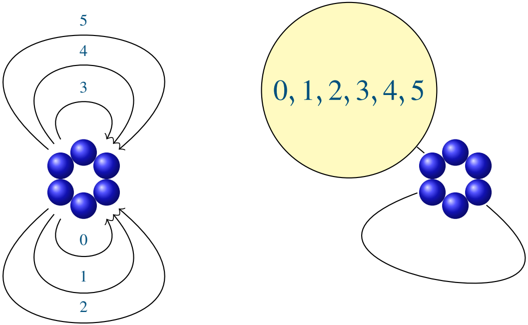
- Action of $\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\}$ on another 6-bead necklace.



- Orbit = similar necklaces of cycle.
- Stabilizer = elements that give loop.

Orbit and Stabilizer – Part 4

- Action of $\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\}$ on another 6-bead necklace.



- Orbit = similar necklaces of cycle. Size of orbit = 1.
- Stabilizer = elements that give loop. Size of stabilizer = 6.

Orbit-Stabilizer Theorem

An action from Group G to Set X gives Orbits and Stabilizers.
For $x \in X$, its Orbit and Stabilizer have sizes related by:

Theorem

$|\textit{Orbit of } x| \times |\textit{Stabilizer of } x| = |\textit{action Group } G|$

Orbit-Stabilizer Theorem

An action from Group G to Set X gives Orbits and Stabilizers.
For $x \in X$, its Orbit and Stabilizer have sizes related by:

Theorem

|Orbit of x| $\times$ |Stabilizer of x| $=$ |action Group G|

Apply to Necklaces

- $X =$ set of n-bead necklaces, action group has $|\mathbb{Z}_n^+| = n$.

Orbit-Stabilizer Theorem

An action from Group G to Set X gives Orbits and Stabilizers.
For $x \in X$, its Orbit and Stabilizer have sizes related by:

Theorem

$|$*Orbit of* $x| \times |$*Stabilizer of* $x| = |$*action Group* $G|$

Apply to Necklaces

- $X =$ set of n-bead necklaces, action group has $|\mathbb{Z}_n^+| = n$.
- For a monocoloured necklace, orbit size $= 1$.
- For a multicoloured necklace, orbit size $\neq 1$.

Orbit-Stabilizer Theorem

An action from Group G to Set X gives Orbits and Stabilizers.
For $x \in X$, its Orbit and Stabilizer have sizes related by:

Theorem

|Orbit of x| $\times$ |Stabilizer of x| $=$ |action Group G|

Apply to Necklaces

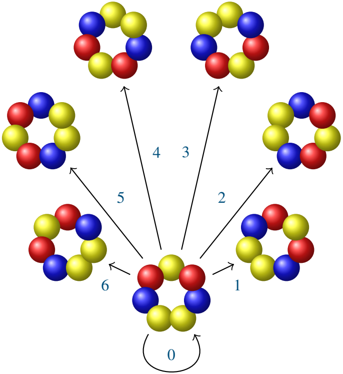
- $X =$ set of n-bead necklaces, action group has $|\mathbb{Z}_n^+| = n$.
- For a monocoloured necklace, orbit size $= 1$.
- For a multicoloured necklace, orbit size $\neq 1$.
- What is the orbit size for a multicoloured necklaces with prime number of beads?

Mulitcoloured Necklace with Prime Number of Beads

- For necklaces with prime p beads, size of action group $|\mathbb{Z}_p^+| = p$, with trivial factorisation $p = 1 \times p = p \times 1$.
- Only monocoloured necklaces have orbits of size 1; so in this case multicoloured necklaces have orbits of size p.

Mulitcoloured Necklace with Prime Number of Beads

- For necklaces with prime p beads, size of action group $|\mathbb{Z}_p^+| = p$, with trivial factorisation $p = 1 \times p = p \times 1$.
- Only monocoloured necklaces have orbits of size 1; so in this case multicoloured necklaces have orbits of size p.

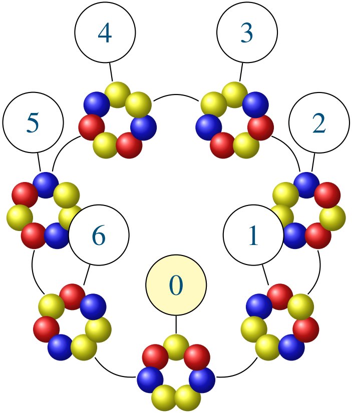


$\mathbb{Z}_7^+ = \{0, 1, 2, 3, 4, 5, 6\}$

number of beads $= 7$

Mulitcoloured Necklace with Prime Number of Beads

- For necklaces with prime p beads, size of action group $|\mathbb{Z}_p^+| = p$, with trivial factorisation $p = 1 \times p = p \times 1$.
- Only monocoloured necklaces have orbits of size 1; so in this case multicoloured necklaces have orbits of size p.



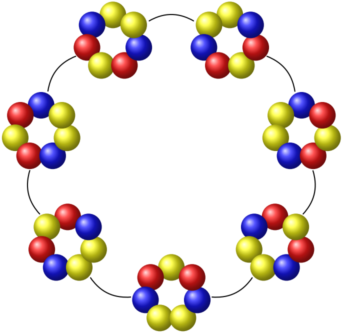
$\mathbb{Z}_7^+ = \{0, 1, 2, 3, 4, 5, 6\}$

number of beads $= 7$

orbit size $= 7$

Mulitcoloured Necklace with Prime Number of Beads

- For necklaces with prime p beads, size of action group $|\mathbb{Z}_p^+| = p$, with trivial factorisation $p = 1 \times p = p \times 1$.
- Only monocoloured necklaces have orbits of size 1; so in this case multicoloured necklaces have orbits of size p.



$\mathbb{Z}_7^+ = \{0, 1, 2, 3, 4, 5, 6\}$

number of beads $= 7$

orbit size $= 7$

Orbit is isomorphic to necklace

Necklace Theorem by Orbit-Stabilizer in HOL4

- Prove the Orbit-Stabilizer theorem.

  $\vdash$ `FiniteGroup` g $\wedge$ `action` $(\circ)$ g X $\wedge$ $x \in X$ $\wedge$
  `FINITE` X $\Rightarrow$ $|\mathtt{G}|$ = $|\mathit{orbit}\ x| \times |\mathit{stabilizer}\ x|$

- Prove that `cycle` is an action from $\mathbb{Z}_n^+$ to necklaces.

  $\vdash$ `0` $<$ n $\wedge$ `0` $<$ a $\Rightarrow$
  `action cycle` $\mathbb{Z}_n^+$ `(necklace` n a`)`

- For multicoloured necklaces of length p, a prime,
  the orbit size of each necklace equals p.

  $\vdash$ `prime` p $\wedge$ `0` $<$ a $\wedge$ $\ell \in$ `multicoloured` p a $\Rightarrow$
  $|$`orbit cycle` $\mathbb{Z}_p^+$ `(multicoloured` p a`)` $\ell|$ = p

Group insight for Necklace Theorem

- Necklace Theorem says:
  - When n is prime, cycle partitions of necklaces are "good".
  - When n is not prime, cycle partitions of necklaces are "bad".
  - But why good for primes, and how bad for non-primes?

Group insight for Necklace Theorem

- Necklace Theorem says:
  - When n is prime, cycle partitions of necklaces are "good".
  - When n is not prime, cycle partitions of necklaces are "bad".
  - But why good for primes, and how bad for non-primes?
- Group action reveals:
  - Cycle partitions are orbits of $\mathbb{Z}_n^+$ to n-bead necklaces.
  - For any n, $|$orbit of n-bead monocoloured necklace$| = 1$.
  - For any n, $|$orbit of n-bead multicoloured necklace$| \neq 1$.

Group insight for Necklace Theorem

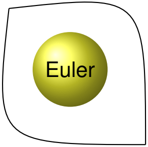
- Necklace Theorem says:
  - When n is prime, cycle partitions of necklaces are "good".
  - When n is not prime, cycle partitions of necklaces are "bad".
  - But why good for primes, and how bad for non-primes?
- Group action reveals:
  - Cycle partitions are orbits of $\mathbb{Z}_n^+$ to n-bead necklaces.
  - For any n, $|$orbit of n-bead monocoloured necklace$| = 1$.
  - For any n, $|$orbit of n-bead multicoloured necklace$| \neq 1$.
- Orbit-Stabilizer Theorem gives:
  - For multicoloured necklaces with n beads:
    $|$orbit of necklace$| \times |$stabilizer of necklace$| = |\mathbb{Z}_n^+| = n$
  - Therefore, for multicoloured necklaces with prime n beads, orbit size must be n.
  - Also, for multicoloured necklaces with non-prime n beads, orbit size is either n or a proper factor of n.

The Missing Piece

- Proofs of Fermat's Little Theorem, so far.

The Missing Piece

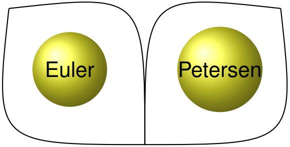
- Proofs of Fermat's Little Theorem, so far.



- Euler's proof using permutation of modulo multiplication.

The Missing Piece

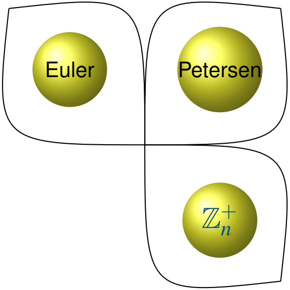
- Proofs of Fermat's Little Theorem, so far.



- Euler's proof using permutation of modulo multiplication.
- Petersen's proof using necklaces and cycles.

The Missing Piece

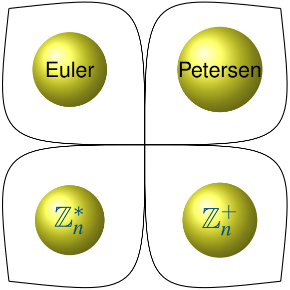
- Proofs of Fermat's Little Theorem, so far.



- Euler's proof using permutation of modulo multiplication.
- Petersen's proof using necklaces and cycles.
- Group action on necklaces by $\mathbb{Z}_n^+$.

The Missing Piece

- Proofs of Fermat's Little Theorem, so far.



- Euler's proof using permutation of modulo multiplication.
- Petersen's proof using necklaces and cycles.
- Group action on necklaces by $\mathbb{Z}_n^+$.
- Finite Group elementary property, apply to $\mathbb{Z}_n^*$.

Property of Finite Group

- Group G is a set with a binary operation $*$ satisfying four properties: Closure, Associativity, Identity and Inverse.
  - Closure: for $x \in G$ and $y \in G$, the result $x * y \in G$ always.
  - Identity: there is $e \in G$ such that, for any $a \in G$, $e * a = a$.

Property of Finite Group

- Group G is a set with a binary operation $*$ satisfying four properties: Closure, Associativity, Identity and Inverse.
  - Closure: for $x \in G$ and $y \in G$, the result $x * y \in G$ always.
  - Identity: there is $e \in G$ such that, for any $a \in G$, $e * a = a$.
- Take an element $a \in G$, write $a^1 = a$, $a^2 = a * a$, $a^3 = a * a * a$, *etc.*
- Consider the sequence $a^1, a^2, a^3, \ldots$
  - These are all $\in G$, by Closure property.
  - For a finite group G, they cannot be all distinct.

Property of Finite Group

- Group G is a set with a binary operation $*$ satisfying four properties: Closure, Associativity, Identity and Inverse.
  - Closure: for $x \in G$ and $y \in G$, the result $x * y \in G$ always.
  - Identity: there is $e \in G$ such that, for any $a \in G$, $e * a = a$.
- Take an element $a \in G$, write $a^1 = a$, $a^2 = a * a$, $a^3 = a * a * a$, *etc.*
- Consider the sequence $a^1, a^2, a^3, \ldots$
  - These are all $\in G$, by Closure property.
  - For a finite group G, they cannot be all distinct.

  This fact leads to:

Theorem

For a finite group G and any $a \in G$, $a^{|G|} = e$, the identity.

Property of Finite Group

- Group G is a set with a binary operation $*$ satisfying four properties: Closure, Associativity, Identity and Inverse.
  - Closure: for $x \in G$ and $y \in G$, the result $x * y \in G$ always.
  - Identity: there is $e \in G$ such that, for any $a \in G$, $e * a = a$.
- Take an element $a \in G$, write $a^1 = a$, $a^2 = a * a$, $a^3 = a * a * a$, *etc.*
- Consider the sequence $a^1, a^2, a^3, \ldots$
  - These are all $\in G$, by Closure property.
  - For a finite group G, they cannot be all distinct.

  This fact leads to:

Theorem

For a finite group G and any $a \in G$, $a^{|G|} = e$, the identity.

- This is the Finite Group version of Fermat's Little Theorem.

Groups of Modulo Multiplication – Part 1

- Besides $\mathbb{Z}_n^+$, there is also $\mathbb{Z}_n^*$, first investigated by Euler.
- For $n = 7$, a prime, all nonzero remainders $\{1, 2, 3, 4, 5, 6\}$ are well-behaved,

$\otimes$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Groups of Modulo Multiplication – Part 1

- Besides $\mathbb{Z}_n^+$, there is also $\mathbb{Z}_n^*$, first investigated by Euler.
- For $n = 7$, a prime, all nonzero remainders $\{1, 2, 3, 4, 5, 6\}$ are well-behaved, and all are coprime to the prime 7.

$\otimes$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

a	a^2	a^3	a^4	a^5	a^6
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

- Number of coprimes to $7 = \varphi(7) = 6$, and for these $a^6 = 1$.

Groups of Modulo Multiplication – Part 2

- For $n = 6$, not all nonzero remainders $\{1, 2, 3, 4, 5\}$ are well-behaved (*e.g.* some nonzero can multiply to zero),

$\otimes$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Groups of Modulo Multiplication – Part 2

- For $n = 6$, not all nonzero remainders $\{1, 2, 3, 4, 5\}$ are well-behaved (*e.g.* some nonzero can multiply to zero), but those coprime to 6 are.

$\otimes$	1	5	a	a^2
1	1	5	1	1
5	5	1	5	1

- Let $\mathbb{Z}_6^* = \{1, 5\}$, those coprime to 6.
- Then $|\mathbb{Z}_6^*| = \varphi(6) = 2$, and for these $a^2 = 1$.

Groups of Modulo Multiplication – Part 3

- For $n = 8$, not all nonzero remainders $\{1, 2, 3, 4, 5, 6, 7\}$ are well-behaved (*e.g.* some nonzero can multiply to zero),

$\otimes$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

Groups of Modulo Multiplication – Part 3

- For $n = 8$, not all nonzero remainders $\{1, 2, 3, 4, 5, 6, 7\}$ are well-behaved (*e.g.* some nonzero can multiply to zero), but those coprime to 8 are.

$\otimes$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

a	a^2	a^3	a^4
1	1	1	1
3	1	3	1
5	1	5	1
7	1	7	1

- Let $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$, those coprime to 8.
- Then $|\mathbb{Z}_8^*| = \varphi(8) = 4$, and for these $a^4 = 1$.

Generalization of Fermat's Little Theorem

- $\mathbb{Z}_n^* =$ nonzero remainders of $\mod n$ that are coprime to n, $|\mathbb{Z}_n^*| = \varphi(n)$.
- For prime p, all nonzero remainders are coprime to p, $|\mathbb{Z}_p^*| = \varphi(p) = (p-1)$.

Generalization of Fermat's Little Theorem

- $\mathbb{Z}_n^* =$ nonzero remainders of $\mod n$ that are coprime to n, $|\mathbb{Z}_n^*| = \varphi(n)$.
- For prime p, all nonzero remainders are coprime to p, $|\mathbb{Z}_p^*| = \varphi(p) = (p-1)$.
- $\mathbb{Z}_n^*$ always form a multiplicative group *(see paper)*, with multiplicative identity $e = 1$.

Generalization of Fermat's Little Theorem

- $\mathbb{Z}_n^* =$ nonzero remainders of $\mod n$ that are coprime to n, $|\mathbb{Z}_n^*| = \varphi(n)$.
- For prime p, all nonzero remainders are coprime to p, $|\mathbb{Z}_p^*| = \varphi(p) = (p-1)$.
- $\mathbb{Z}_n^*$ always form a multiplicative group *(see paper)*, with multiplicative identity $e = 1$.
- From property of Finite Group:

Theorem

For a finite group G and any $a \in G$, $a^{|G|} = e$, the identity.

Generalization of Fermat's Little Theorem

- $\mathbb{Z}_n^* =$ nonzero remainders of $\mod n$ that are coprime to n, $|\mathbb{Z}_n^*| = \varphi(n)$.
- For prime p, all nonzero remainders are coprime to p, $|\mathbb{Z}_p^*| = \varphi(p) = (p-1)$.
- $\mathbb{Z}_n^*$ always form a multiplicative group *(see paper)*, with multiplicative identity $e = 1$.
- From property of Finite Group:

Theorem

For a finite group G and any $a \in G$, $a^{|G|} = e$, the identity.

- Given a prime p, $a^{(p-1)} \equiv 1 \mod p$ for all a coprime to p.
  – Fermat's statement of his "Little Theorem" in 1640.

Generalization of Fermat's Little Theorem

- $\mathbb{Z}_n^* =$ nonzero remainders of $\mod n$ that are coprime to n, $|\mathbb{Z}_n^*| = \varphi(n)$.
- For prime p, all nonzero remainders are coprime to p, $|\mathbb{Z}_p^*| = \varphi(p) = (p-1)$.
- $\mathbb{Z}_n^*$ always form a multiplicative group *(see paper)*, with multiplicative identity $e = 1$.
- From property of Finite Group:

Theorem

For a finite group G and any $a \in G$, $a^{|G|} = e$, the identity.

- Given a prime p, $a^{(p-1)} \equiv 1 \mod p$ for all a coprime to p.
  – Fermat's statement of his "Little Theorem" in 1640.
- Given any number n, $a^{\varphi(n)} \equiv 1 \mod n$ for all a coprime to n.
  – Euler's generalisation of Fermat's result in 1760.

HOL4 Proof Scripts

for Fermat's Little Theorem

Type of Proof	Approach	Total
Combinatorial	Direct *via* cycles	824
	Group *via* action	1387
Number-theoretic	Direct *via* modulo arithmetic	473
	Group *via* generated subgroups	839
	Euler *via* generated subgroups	871

Table : Line counts for theories developing each approach.

HOL4 Proof Scripts

for Fermat's Little Theorem

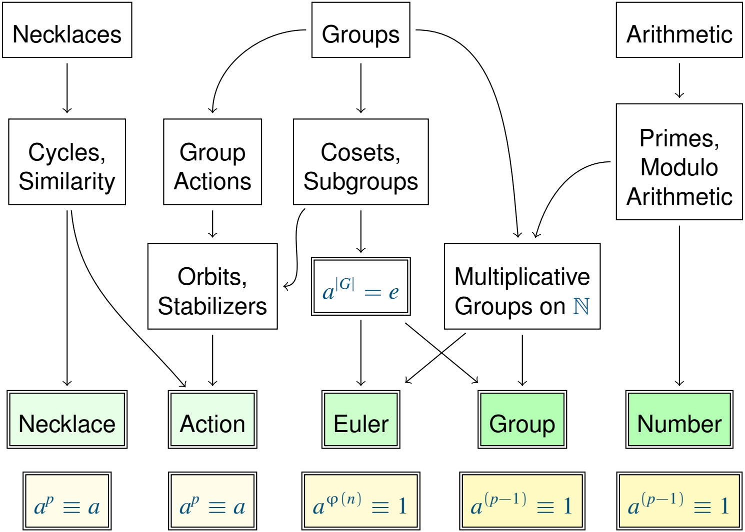
Type of Proof	Approach	Total
Combinatorial	Direct *via* cycles	824
	Group *via* action	1387
Number-theoretic	Direct *via* modulo arithmetic	473
	Group *via* generated subgroups	839
	Euler *via* generated subgroups	871

Table : Line counts for theories developing each approach.

- Number-theoretic approach is best in terms of lines-of-code.
- Group and group action can be packaged into useful libraries.

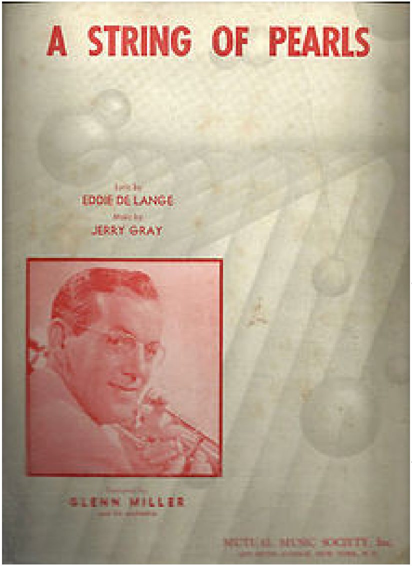
A String of Pearls

Proofs of Fermats Little Theorem

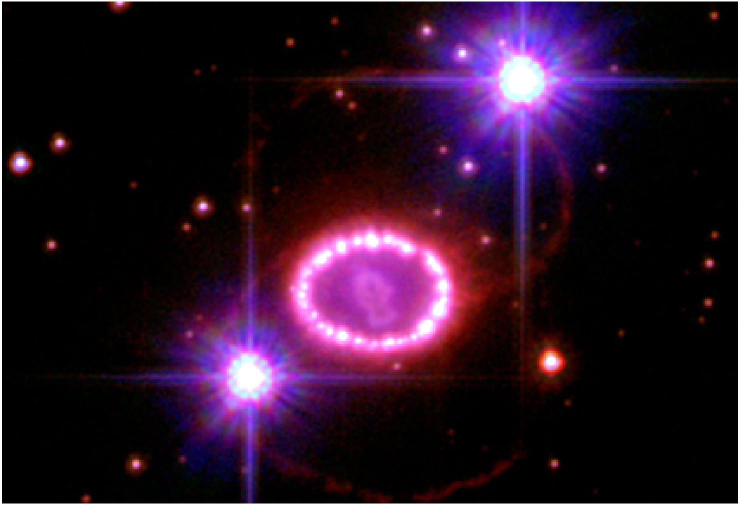


String of Pearls – Plant

A String of Pearls – Song

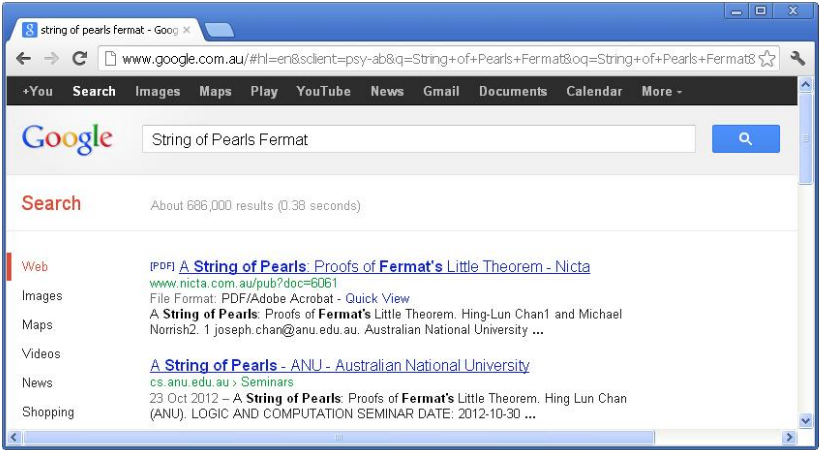


String of Pearls – Nature



The “String of Pearls”, a glowing gas ring encircling the remnant of Supernova 1987A. (credit: NASA)

String of Pearls – Google



Very easy to look up our paper with essential keywords.

Summary

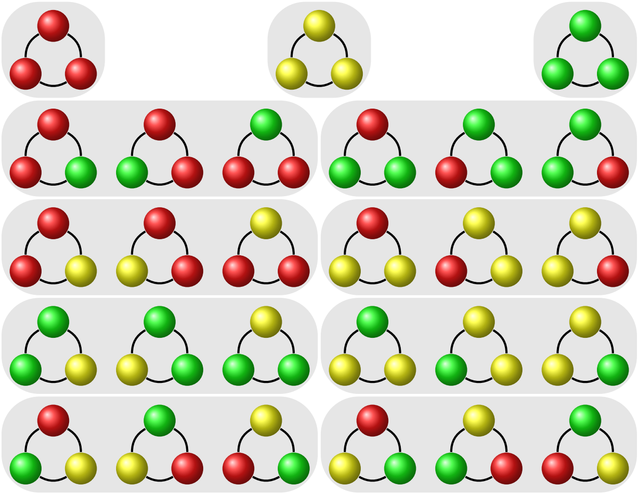
- Two styles to mechanise Fermat's Little Theorem:
  - Number-theoretic
  - Combinatoric

- Each style can be enhanced by a Group approach:
  - Underlying Euler's proof based on permutations is a finite group property of $\mathbb{Z}_n^*$.
  - Underlying the Necklace proof based on cycles is group action on necklaces by $\mathbb{Z}_n^+$.

- Which proof style is "better"?
  - Number-theoretic proofs are short, as Fermat's Little Theorem is about numbers.
  - Combinatoric proofs are elegant, as Necklace Theorem is about set partitions.
  - Group theory provides invaluable insight.

Necklace Proof

3-bead necklaces with 3 colours, $3^3{=}27$; "good" cycle partitions.



Orbit-Stabilizer Theorem

An action from Group G to Set X gives Orbits and Stabilizers.
For $x \in X$, its Orbit and Stabilizer have sizes related by:

Theorem

$|\textit{Orbit of } x| \times |\textit{Stabilizer of } x| = |\textit{action Group } G|$

Orbit-Stabilizer Theorem

An action from Group G to Set X gives Orbits and Stabilizers.
For $x \in X$, its Orbit and Stabilizer have sizes related by:

Theorem

$|$Orbit of $x| \times |$Stabilizer of $x| = |$action Group $G|$