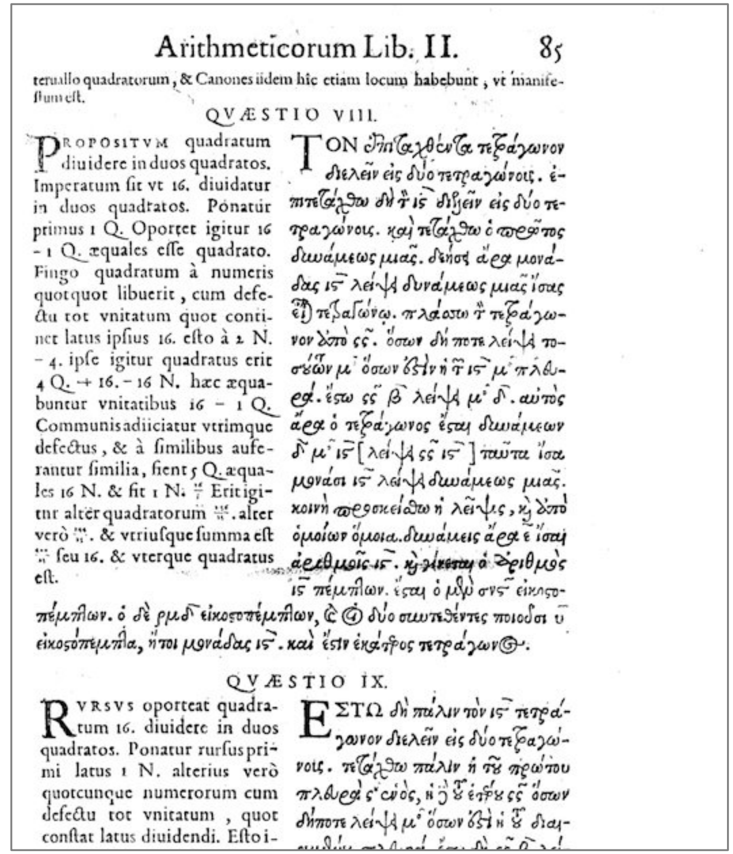
Fermat's Little Theorem

CS 2800: Discrete Structures, Spring 2015

Sid Chaudhuri

Not to be confused with...



Arithmeticorum Lib. II. 85

teruallo quadratorum, & Canones iidem hic etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 - 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quot continet latus ipsius 16. esto à 2 N. - 4. ipse igitur quadratus erit 4 Q. + 16. - 16 N. hæc æquabuntur vnitatibus 16 - 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$. & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

ΤΟΝ ἐπιταχθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους. ἐπιτετάχθω δὴ τὸν ιϛ διελεῖν εἰς δύο τετραγώνους. καὶ τετάχθω ὁ πρῶτος δυνάμεως μιᾶς. δεήσει ἄρα μονάδας ιϛ λείψει δυνάμεως μιᾶς ἴσας εἶναι τετραγώνῳ. πλάσσω τὸν τετράγωνον ἀπὸ ςς. ὅσων δήποτε λείψει τοσούτων μ° ὅσων ἐστὶν ἡ τῶν ιϛ μ° πλευρά. ἔστω ςς β λείψει μ° δ. αὐτὸς ἄρα ὁ τετράγωνος ἔσται δυνάμεων δ μ° ιϛ [λείψει ςς ιϛ] ταῦτα ἴσα μονάσι ιϛ λείψει δυνάμεως μιᾶς. κοινὴ προσκείσθω ἡ λεῖψις, καὶ ἀπὸ ὁμοίων ὅμοια. δυνάμεις ἄρα ε ἴσαι ἀριθμοῖς ιϛ. καὶ γίνεται ὁ ἀριθμὸς ιϛ πέμπτων. ἔσται ὁ μὲν σνϛ εἰκοστοπέμπτων. ὁ δὲ ρμδ εἰκοστοπέμπτων, καὶ οἱ δύο συντεθέντες ποιοῦσι υ εἰκοστόπεμπτα, ἤτοι μονάδας ιϛ. καὶ ἔστιν ἑκάτερος τετράγωνος.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16. diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto i-

ΕΣΤΩ δὴ πάλιν τὸν ιϛ τετράγωνον διελεῖν εἰς δύο τετραγώνους. τετάχθω πάλιν ἡ τοῦ πρώτου πλευρὰ ς ἑνός, ἡ δὲ τοῦ ἑτέρου ςς ὅσων δήποτε λείψει μ° ὅσων ἐστὶν ἡ τοῦ διαι-

Fermat's Last Theorem:

$x^n + y^n = z^n$ has no integer solution for $n > 2$

Recap: Modular Arithmetic

- Definition: $a \equiv b \pmod{m}$ if and only if $m \mid a - b$
- Consequences:
  - $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$

    (congruence $\Longleftrightarrow$ Same remainder)

  - If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
    - $a + c \equiv b + d \quad \pmod{m}$
    - $ac \equiv bd \quad \pmod{m}$

    (congruences can sometimes be treated like equations)

Fermat's Little Theorem

- If p is a prime number, and a is any integer, then

$$a^p \equiv a \pmod{p}$$

Fermat's Little Theorem

- If p is a prime number, and a is any integer, then

$$a^p \equiv a \pmod{p}$$

- If a is not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Fermat's Little Theorem

- Examples:
  - $21^7 \equiv 21 \pmod 7$

    ... but $21^6 \not\equiv 1 \pmod 7$

  - $111^{12} \equiv 1 \pmod{13}$

  - $123{,}456{,}789^{\,2^{57{,}885{,}161} - 2} \equiv 1 \pmod{2^{57{,}885{,}161} - 1}$

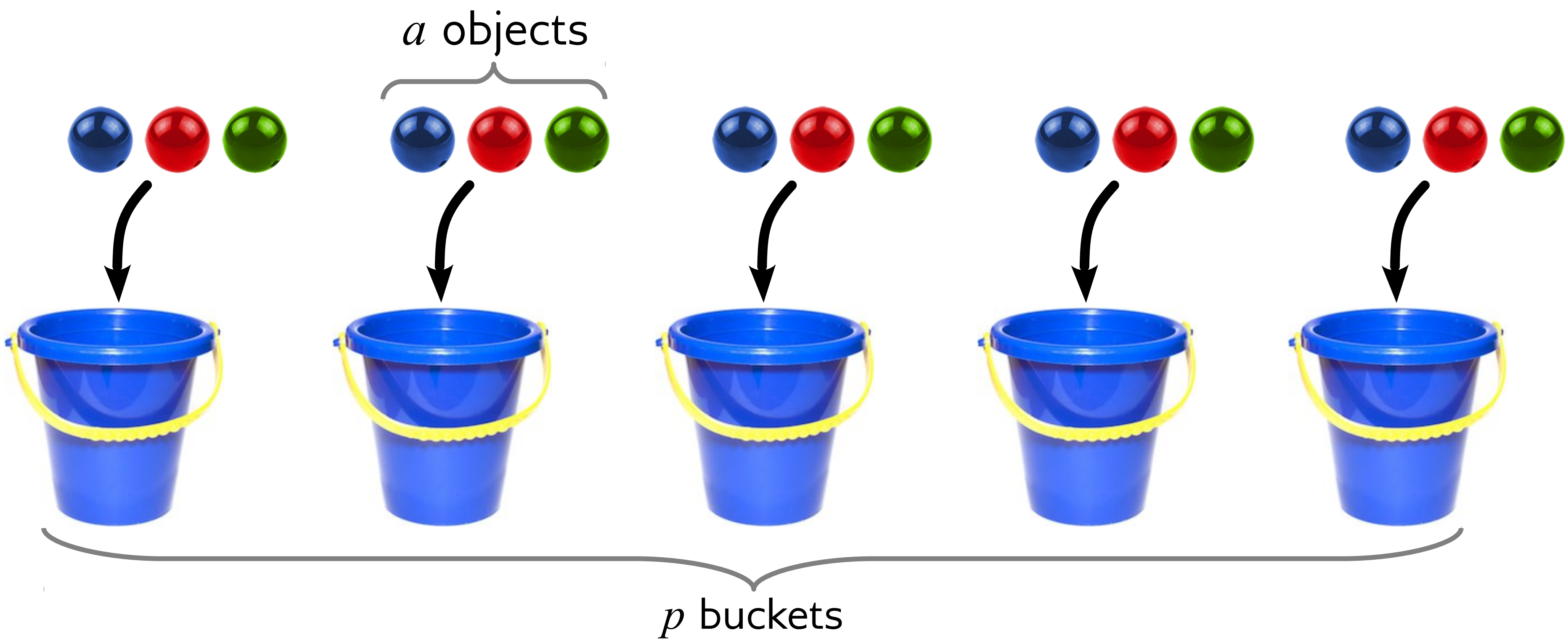
Two proofs

- Combinatorial
  - … counting things
- Algebraic
  - … induction
- We'll consider only non-negative a
  - … the result for non-negative a can be extended to negative integers

    (try it using what we know of congruences!)

Counting necklaces

- Due to Solomon W. Golomb, 1956
- Basic idea: a^p suggests we see how to fill p buckets, where each is filled with one of a objects



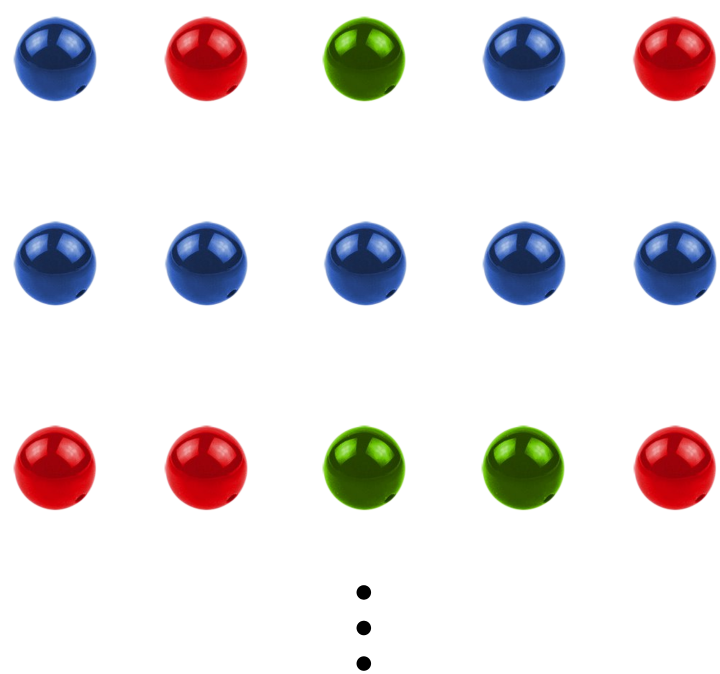
Strings of beads

- Each way of filling the buckets gives a different sequence of p objects ("beads")
  - a^p such sequences

$S_1 =$

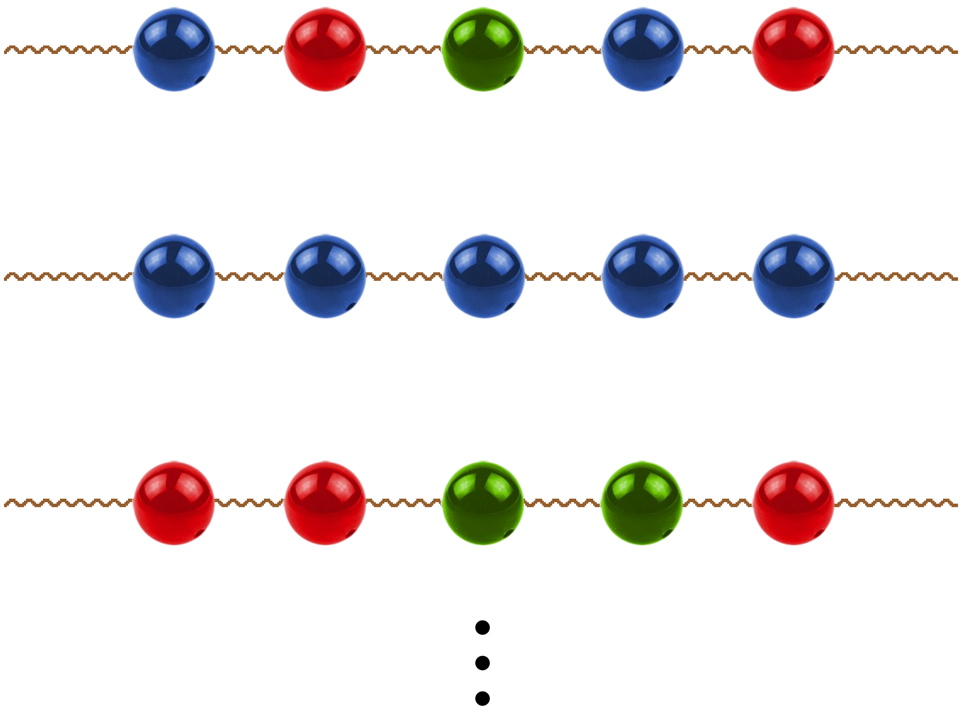
$S_2 =$

$S_3 =$



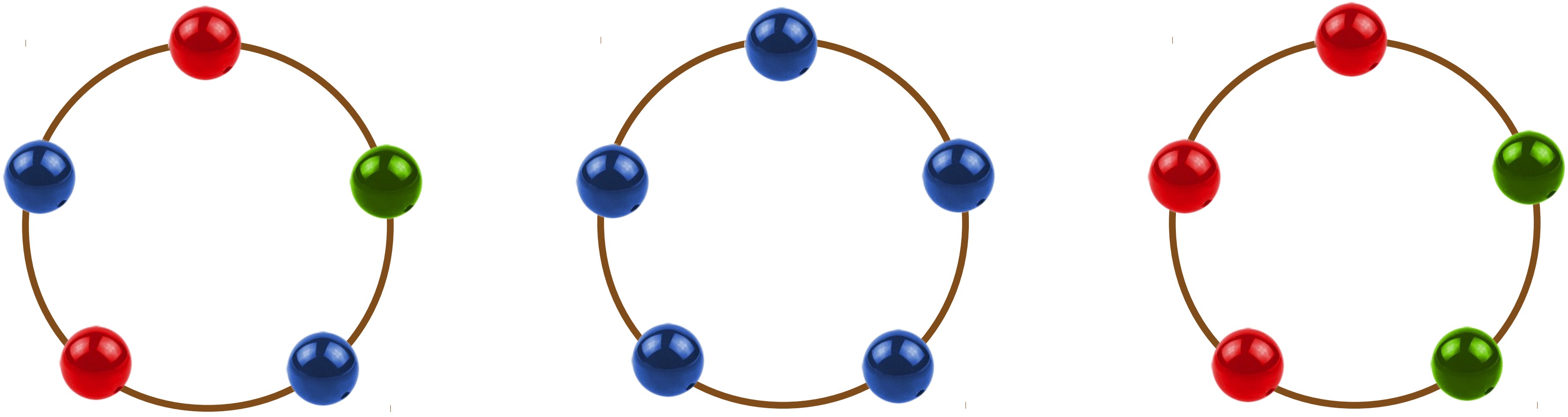
Strings of beads

- Now string the beads together...



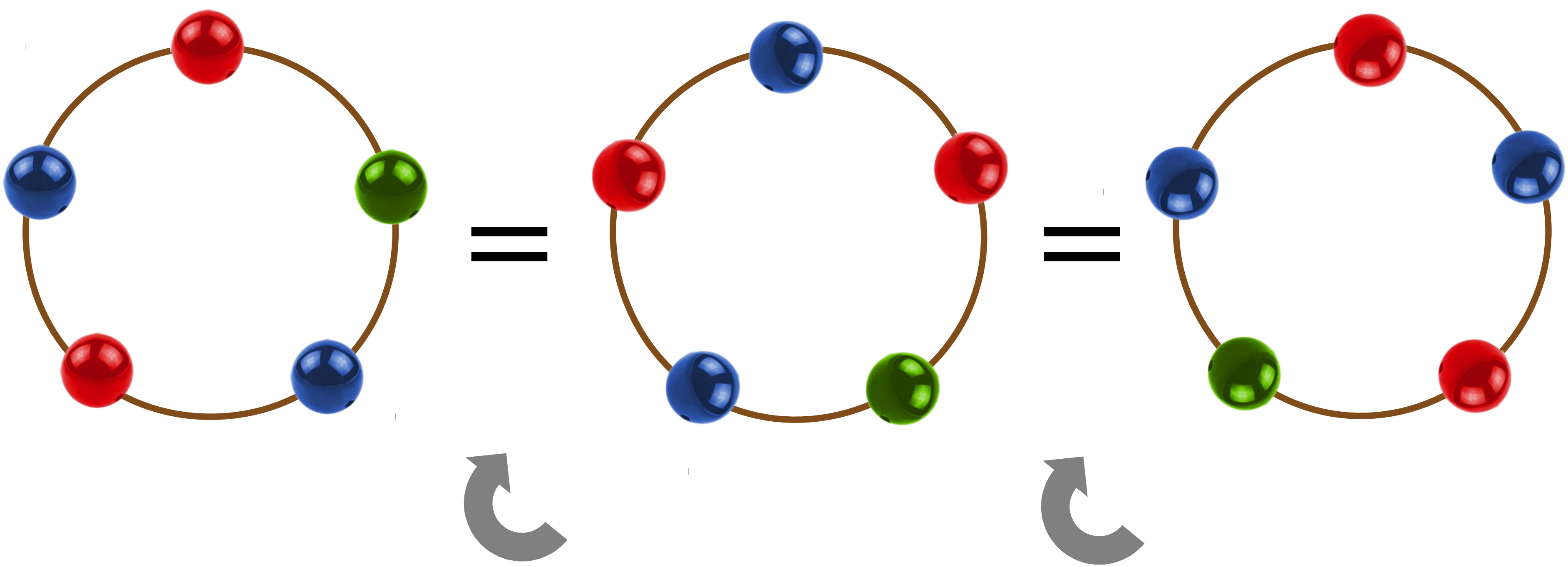
Strings of beads

- … and join the ends to form “necklaces”



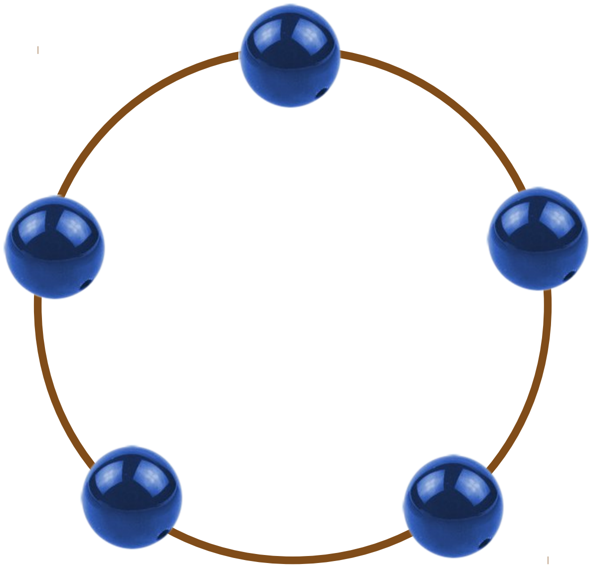
A necklace rotated…

- … is the same necklace
  - Different strings can produce the same necklace when the ends are joined



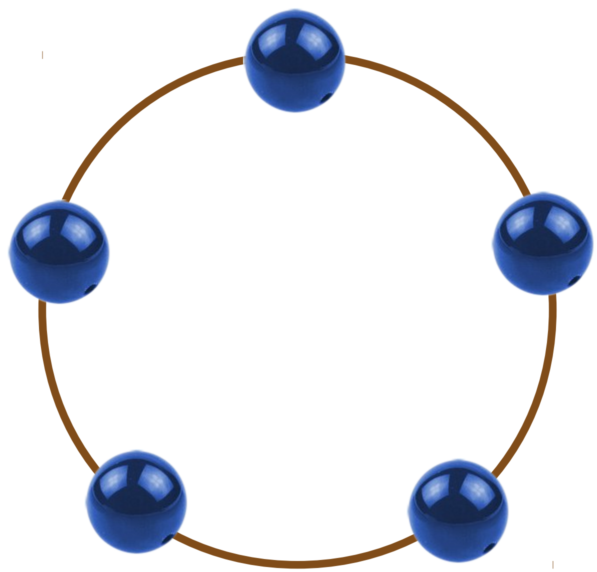
Two types of necklaces

- Containing beads of a single color



Two types of necklaces

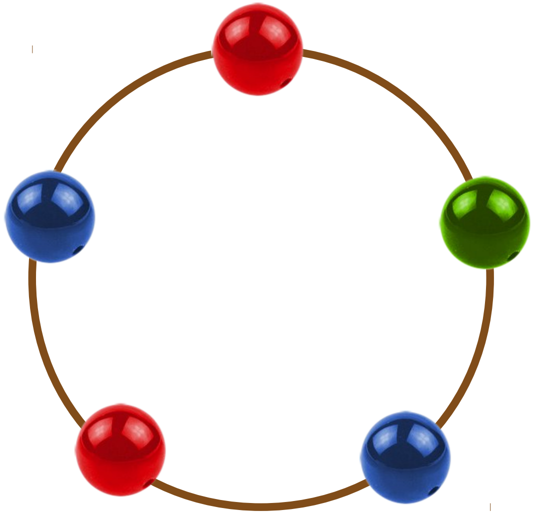
- Containing beads of a single color



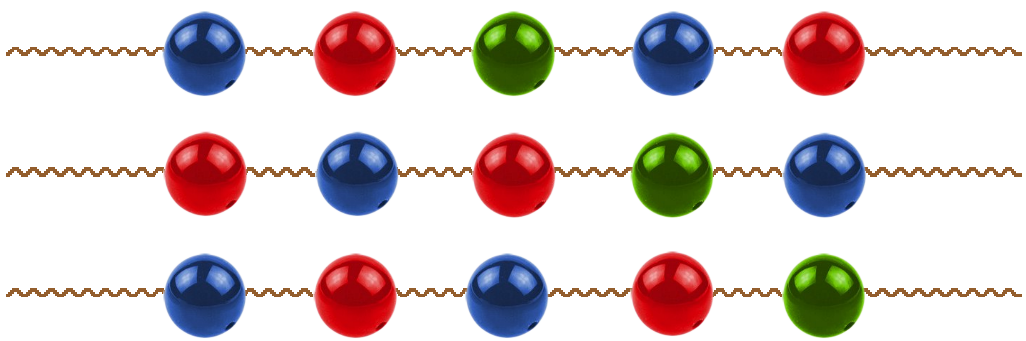
- Only one possible string

Two types of necklaces

- Containing beads of different colors

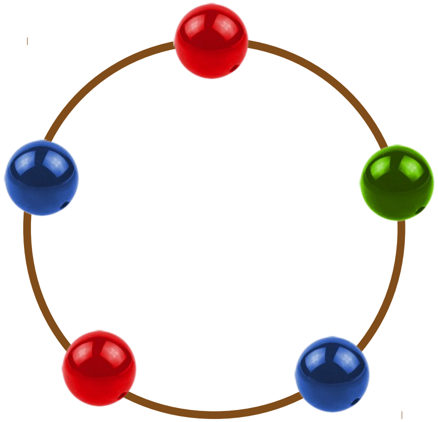


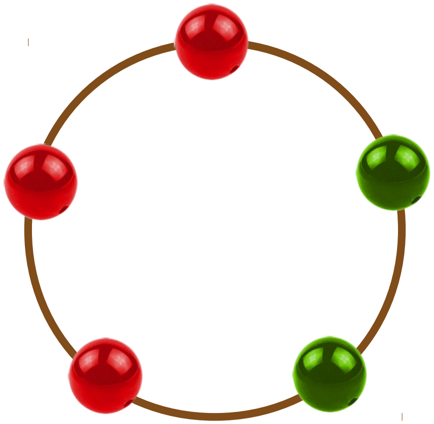
- Many possible strings



Lemma

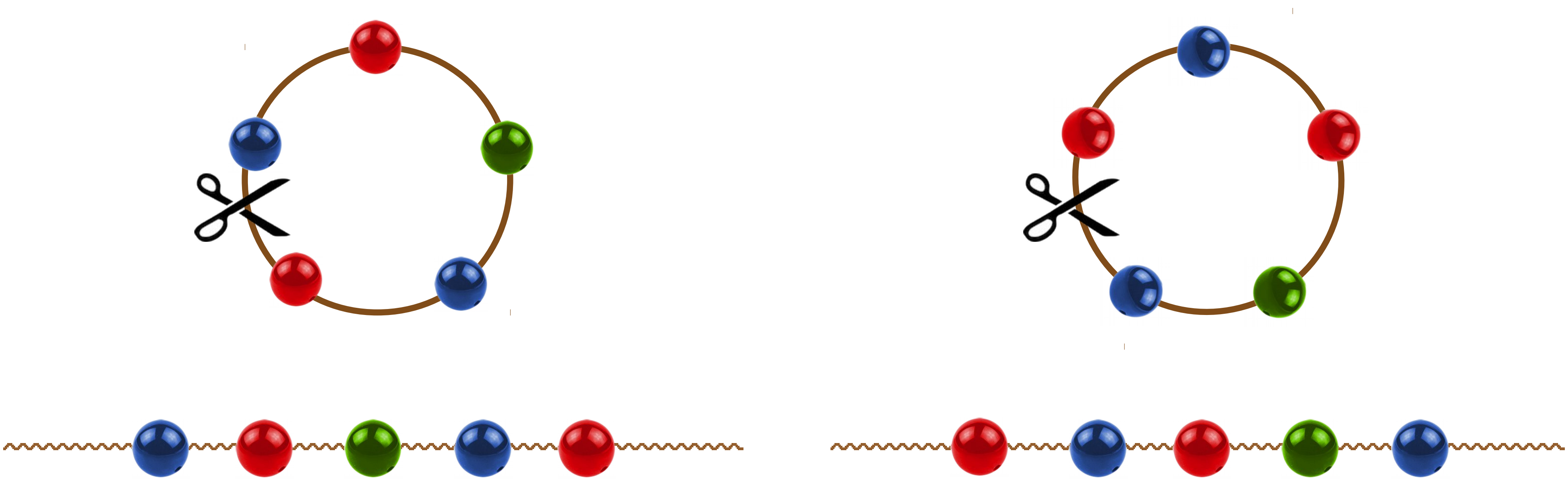
- If p is a prime number and N is a necklace with at least two colors, every rotation of N corresponds to a different string
  - … i.e. there are exactly p different strings that form the same necklace N





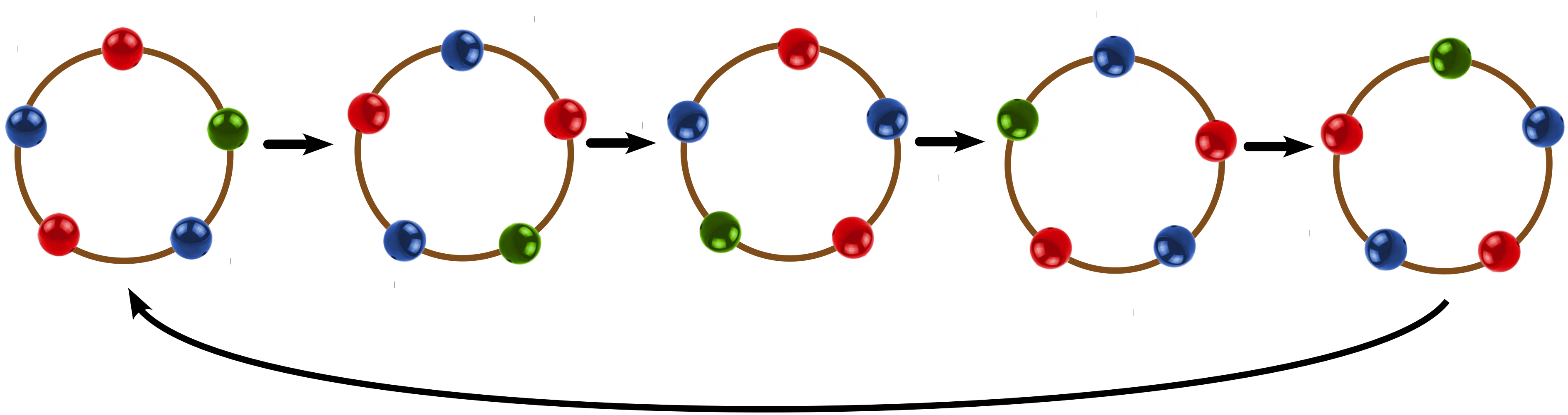
Proof of Lemma

- First, note that each string corresponds to
  - a rotation of the necklace, and then…
  - … cutting it at a fixed point



Proof of Lemma

- No more than p strings can give the same necklace
  - There are only p (say clockwise) rotations of the necklace (that align the beads) before we loop back to the original orientation



Proof of Lemma

- Now we'll show that no *less* than p strings give the same necklace

Proof of Lemma

- Now we'll show that no *less* than p strings give the same necklace
- Consider clockwise rotations by $1/p$ of a full circle

Proof of Lemma

- Now we'll show that no *less* than p strings give the same necklace
- Consider clockwise rotations by $1/p$ of a full circle
- Let k be the <u>minimum</u> number of such rotations before the original configuration is repeated

Proof of Lemma

- Now we'll show that no *less* than p strings give the same necklace
- Consider clockwise rotations by $1/p$ of a full circle
- Let k be the <u>minimum</u> number of such rotations before the original configuration is repeated
  - Clearly, $k \le p$ (p rotations bring us back to the start)

Proof of Lemma

- Now we'll show that no *less* than p strings give the same necklace
- Consider clockwise rotations by $1/p$ of a full circle
- Let k be the <u>minimum</u> number of such rotations before the original configuration is repeated
  - Clearly, $k \leq p$ (p rotations bring us back to the start)
- Claim: $k \mid p$

Proof of Claim

- Claim: $k \mid p$

Proof of Claim

- Claim: $k \mid p$
- Proof:
  - Let $p = qk + r$, with $0 \leq r < k$ (division algorithm)

Proof of Claim

- Claim: $k \mid p$
- Proof:
  - Let $p = qk + r$, with $0 \leq r < k$ (division algorithm)
  - q iterations, each of k rotations, restores the original configuration (by definition of k)

Proof of Claim

- Claim: $k \mid p$
- Proof:
  - Let $p = qk + r$, with $0 \leq r < k$ (division algorithm)
  - q iterations, each of k rotations, restores the original configuration (by definition of k)
  - So do p rotations (full circle)

Proof of Claim

- Claim: $k \mid p$
- Proof:
  - Let $p = qk + r$, with $0 \leq r < k$ (division algorithm)
  - q iterations, each of k rotations, restores the original configuration (by definition of k)
  - So do p rotations (full circle)
  - ... therefore so do r rotations

Proof of Claim

- Claim: $k \mid p$
- Proof:
  - Let $p = qk + r$, with $0 \leq r < k$ (division algorithm)
  - q iterations, each of k rotations, restores the original configuration (by definition of k)
  - So do p rotations (full circle)
  - ... therefore so do r rotations
  - But $r < k$ and we said k was the minimum "period"!

Proof of Claim

- Claim: $k \mid p$
- Proof:
  - Let $p = qk + r$, with $0 \leq r < k$ (division algorithm)
  - q iterations, each of k rotations, restores the original configuration (by definition of k)
  - So do p rotations (full circle)
  - ... therefore so do r rotations
  - But $r < k$ and we said k was the minimum "period"!
  - ... which is a contradiction, unless $r = 0$

Proof of Lemma

- Since $k \mid p$ and $k \leq p$ and p is prime, we must have either

Proof of Lemma

- Since $k \mid p$ and $k \leq p$ and p is prime, we must have either
  - $k = 1$ (impossible if necklace has at least two colors)

Proof of Lemma

- Since $k \mid p$ and $k \leq p$ and p is prime, we must have either
  - $k = 1$ (impossible if necklace has at least two colors)

    or
  - $k = p$

Proof of Lemma

- Since $k \mid p$ and $k \leq p$ and p is prime, we must have either
  - $k = 1$ (impossible if necklace has at least two colors)

    or
  - $k = p$
- This proves the lemma

What we have so far

What we have so far

- Necklaces with one color

What we have so far

- Necklaces with one color
  - a such strings (one for each color), therefore a such necklaces

What we have so far

- Necklaces with one color
  - a such strings (one for each color), therefore a such necklaces
- Necklaces with multiple colors

What we have so far

- Necklaces with one color
  - a such strings (one for each color), therefore a such necklaces
- Necklaces with multiple colors
  - Each corresponds to p different strings

What we have so far

- Necklaces with one color
  - a such strings (one for each color), therefore a such necklaces
- Necklaces with multiple colors
  - Each corresponds to p different strings
  - $a^p - a$ strings of multiple colors, therefore $(a^p - a)/p$ such necklaces

What we have so far

- Necklaces with one color
  - a such strings (one for each color), therefore a such necklaces
- Necklaces with multiple colors
  - Each corresponds to p different strings
  - $a^p - a$ strings of multiple colors, therefore $(a^p - a)/p$ such necklaces

  $\Rightarrow \; p \mid a^p - a$ (can't have half a necklace)

What we have so far

- Necklaces with one color
  - a such strings (one for each color), therefore a such necklaces
- Necklaces with multiple colors
  - Each corresponds to p different strings
  - $a^p - a$ strings of multiple colors, therefore $(a^p - a) / p$ such necklaces

$\Rightarrow p \mid a^p - a$ (can't have half a necklace)

$\Rightarrow a^p \equiv a \pmod{p}$ QED!

Another proof (algebraic)

Another proof (algebraic)

- For a given prime p, we'll do induction on a

Another proof (algebraic)

- For a given prime p, we'll do induction on a
- Base case: Clear that $0^p \equiv 0 \pmod{p}$

Another proof (algebraic)

- For a given prime p, we'll do induction on a
- Base case: Clear that $0^p \equiv 0 \pmod{p}$
- Inductive hypothesis: $a^p \equiv a \pmod{p}$

Another proof (algebraic)

- For a given prime p, we'll do induction on a
- Base case: Clear that $0^p \equiv 0 \pmod{p}$
- Inductive hypothesis: $a^p \equiv a \pmod{p}$
- Consider $(a+1)^p$

Another proof (algebraic)

- For a given prime p, we'll do induction on a
- Base case: Clear that $0^p \equiv 0 \pmod{p}$
- Inductive hypothesis: $a^p \equiv a \pmod{p}$
- Consider $(a+1)^p$
- By the Binomial Theorem,

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \binom{p}{3} a^{p-3} + \ldots + \binom{p}{p-1} a + 1$$

Another proof (algebraic)

- For a given prime p, we'll do induction on a
- Base case: Clear that $0^p \equiv 0 \pmod{p}$
- Inductive hypothesis: $a^p \equiv a \pmod{p}$
- Consider $(a+1)^p$
- By the Binomial Theorem,

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \binom{p}{3} a^{p-3} + \ldots + \binom{p}{p-1} a + 1$$

  - All RHS terms except last & perhaps first are divisible by p

Another proof (algebraic)

- For a given prime p, we'll do induction on a
- Base case: Clear that $0^p \equiv 0 \pmod{p}$
- Inductive hypothesis: $a^p \equiv a \pmod{p}$
- Consider $(a+1)^p$
- By the Binomial Theorem,

Binomial coefficient $\binom{p}{k}$ is $p!/k!(p-k)!$, which is always an integer. p is prime, so it isn't canceled out by terms in the denominator

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \binom{p}{3} a^{p-3} + \ldots + \binom{p}{p-1} a + 1$$

  - All RHS terms except last & perhaps first are divisible by p

Another proof (algebraic)

- Therefore $(a+1)^p \equiv a^p + 1 \pmod{p}$

Another proof (algebraic)

- Therefore $(a+1)^p \equiv a^p + 1 \pmod p$
- But by the inductive hypothesis, $a^p \equiv a \pmod p$

Another proof (algebraic)

- Therefore $(a+1)^p \equiv a^p + 1 \pmod p$
- But by the inductive hypothesis, $a^p \equiv a \pmod p$

$$\Rightarrow a^p + 1 \equiv a + 1 \pmod p$$ (properties of congruence)

Another proof (algebraic)

- Therefore $(a+1)^p \equiv a^p + 1 \pmod{p}$
- But by the inductive hypothesis, $a^p \equiv a \pmod{p}$

  $\Rightarrow a^p + 1 \equiv a + 1 \pmod{p}$ (properties of congruence)
- Therefore $(a+1)^p \equiv a + 1 \pmod{p}$

Another proof (algebraic)

- Therefore $(a+1)^p \equiv a^p + 1 \pmod{p}$
- But by the inductive hypothesis, $a^p \equiv a \pmod{p}$

  $\Rightarrow a^p + 1 \equiv a + 1 \pmod{p}$ (properties of congruence)
- Therefore $(a+1)^p \equiv a + 1 \pmod{p}$

(congruence is transitive - prove!)

Another proof (algebraic)

- Therefore $(a+1)^p \equiv a^p + 1 \pmod{p}$
- But by the inductive hypothesis, $a^p \equiv a \pmod{p}$

  $\Rightarrow a^p + 1 \equiv a + 1 \pmod{p}$ (properties of congruence)
- Therefore $(a+1)^p \equiv a + 1 \pmod{p}$

  (congruence is transitive - prove!)
- Hence proved by induction