A COUNTING PROOF
OF FERMAT'S LITTLE THEOREM

Suprio Dutta, 6th Sem, Nabadwip Vidyasagar College

Statement of Fermat's Little Theorem

If p is a prime number, then for any integer k, the number $(k^p - k)$ is an integer multiple of p.

$$\textbf{i.e. } k^p \equiv k \ (mod\ p)$$

History of the Theorem

Pierre de Fermat first stated the theorem in a letter dated October 18, 1640, to his friend Frénicle de Bessy.

Fermat's original statement was:

"Tout nombre premier mesure infailliblement une des puissances −1 de quelque progression que ce soit, et l'exposant de la dite puissance est sous-multiple du nombre premier donné −1 ; et, après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question. Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers; de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long. "

Translation of the statement:

Every prime number p divides necessarily one of the powers minus one of any geometric progression $\{a, a^2, a^3, \ldots\}$ that is, there exists t such that p divides $(a^t - 1)$, and the exponent of this power t divides the given prime minus one i.e. $p - 1$. After one has found the first power t that satisfies the question, all those whose exponents are multiples of the exponent of the first one satisfy similarly the question [that is, all multiples of the first t have the same property]. And this proposition is generally true for all series and for all prime numbers; I would send you a demonstration of it, if I did not fear going on for too long.

As with many of Fermat's theorems, no proof by him is known to exist. The first known published proof of this theorem was by the Swiss mathematician Leonhard Euler in 1736. Though a proof in an unpublished manuscript dating to about 1683 was given by German mathematician Gottfried Wilhelm Leibniz. A special case of Fermat's theorem, known as the Chinese hypothesis, maybe some 2,000 years old. The Chinese hypothesis, which replaces a with 2, states that a number n is prime if and only if it divides exactly into $(2^n - 2)$. As proved later in the West, the Chinese hypothesis is only half right.

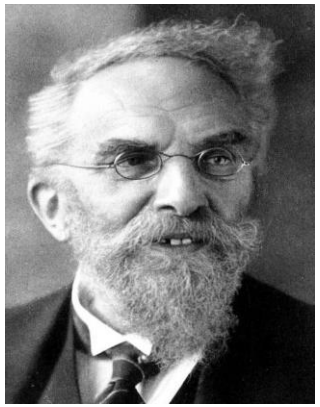
The term "Fermat's little theorem" was probably first used in print in 1913 in Zahlentheorie by Kurt Hensel:

"Für jede endliche Gruppe besteht nun ein Fundamentalsatz, welcher der kleine Fermatsche Satz genannt zu werden pflegt, weil ein ganz spezieller Teil desselben zuerst von Fermat bewiesen worden ist." This means - There is a fundamental theorem holding in every finite group, usually called Fermat's little theorem because Fermat was the first to have proved a very special part of it.

An early use in English occurs in A.A. Albert's Modern Higher Algebra (1937), which refers to "the so-called 'little' Fermat theorem" on page 206.

Leonhard Euler

Gottfried Wilhelm Leibniz



Kurt Hensel

Abraham Adrian Albert

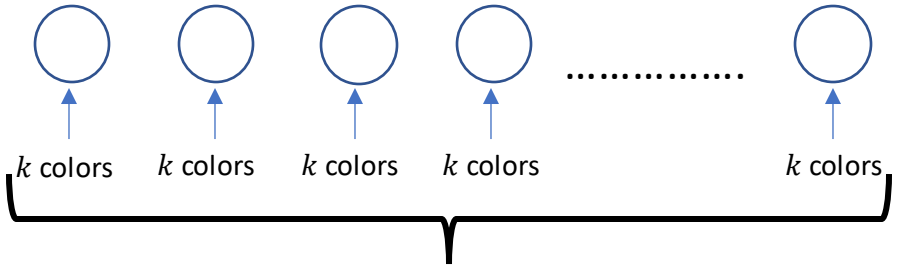
Ughh!!!

Boring History

Ohh sorry … here we go…

Suppose you have beads that come in k colors. You are going to select p of these beads to arrange along a string. It is perfectly acceptable to repeat colors. How many ways?

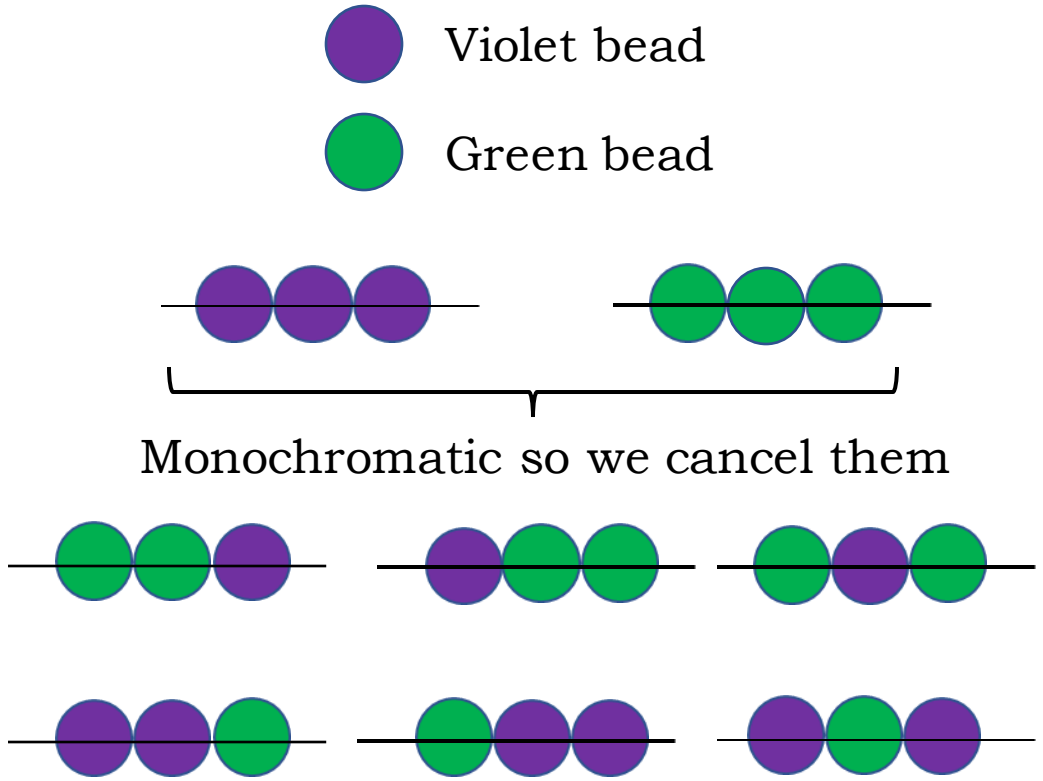
Obviously k^p !!



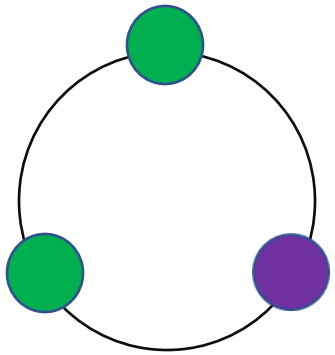
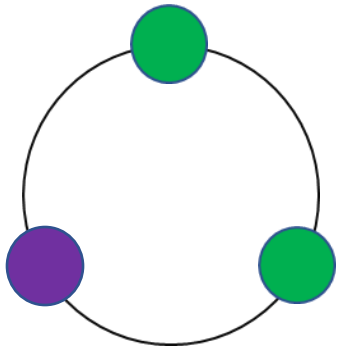
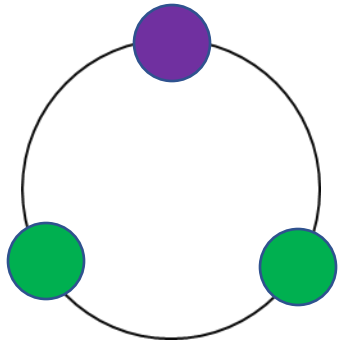
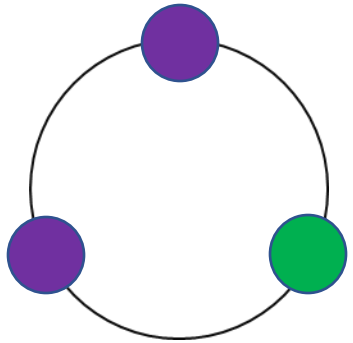
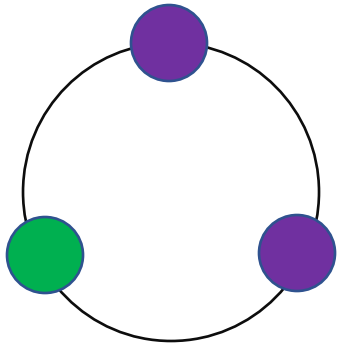
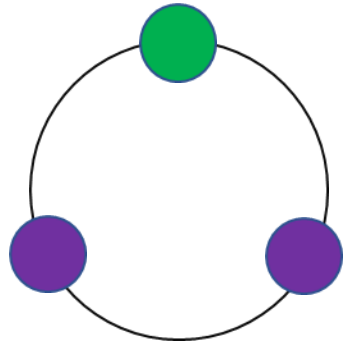
p times

So $\underbrace{k \times k \times \cdots k}_{p \text{ times}} = k^p$ ways

Since it is boring to have all the beads be of the same color, we will require that at least two colors be used. k colors so we have k monochromatic string and we kick them out, so now there are $k^p - k$ strings left. Let consider the case for $p = 3, k = 2$

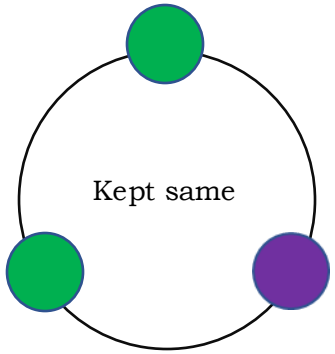


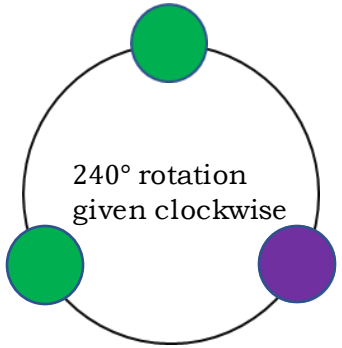
Now we will tie together the ends of the string to form a bracelet.

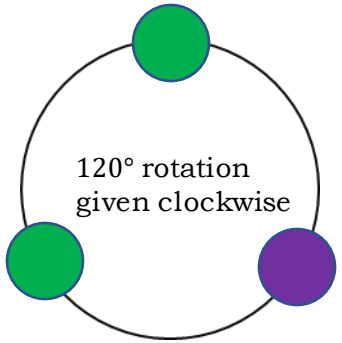







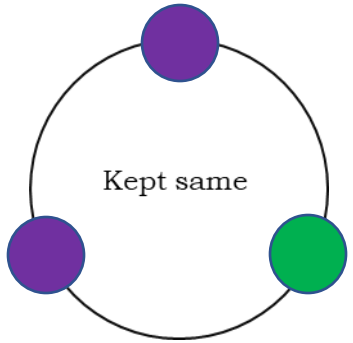
And I give some rotation to them, When this happens some of our strings become indistinguishable

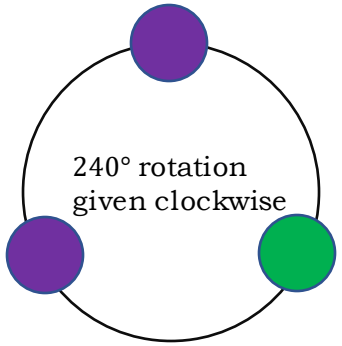
See!!!

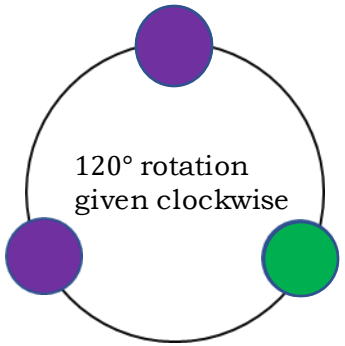












We now ask, "Of the $k^p - k$ many bracelets using at least two colors, how many of them are distinguishable from one another?" The answer is that each string of p beads can be shifted cyclically without producing a different bracelet. Since each of the p cyclic shifts of a given color string will lead to indistinguishable bracelets, we can always match them based on the rotation needed to get the original one (kept fixed), so the size of these groups must be based on the rotation it takes to return to the original or how many rotations to complete the cycle, where each style forms a group(original is kept fixed). We see that the number of indistinguishable bracelets using at least two colors is given by $k^p - k$ divided by p. And since the number of such bracelets is plainly an integer, our proof is complete ■

Very cool. Combinatorial proofs are always very pretty!!

Student Mr. Why asks an important question

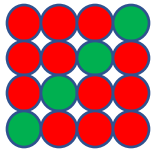
why is p needed to be a prime? We never used this while giving the argument.

Nice point !! Now see

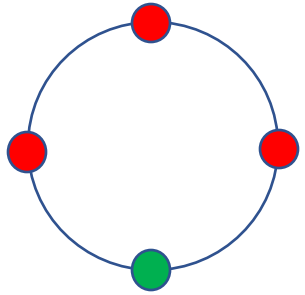
It came in the step where we asserted that each color string gets counted p different times, once for each of the possible cyclic shifts. That is true for a prime number.

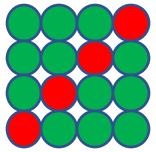
Let us think by taking composite values of p.

Consider the case $k = 2, p = 4$ with 🔴 -red and 🟢 -green beads.

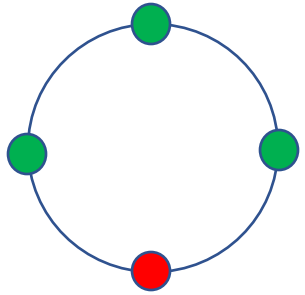


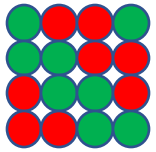
After forming a bracelet and giving necessary rotations



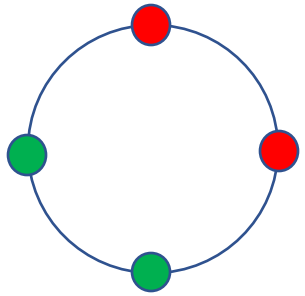


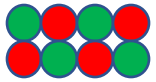
After forming a bracelet and giving necessary rotations



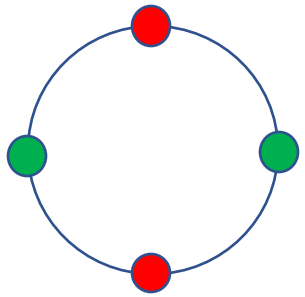


After forming a bracelet and giving necessary rotations

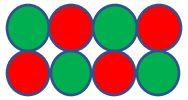




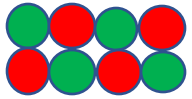
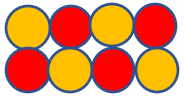
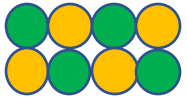
After forming a bracelet and giving necessary rotations



We will have $2^4 - 2 = 14$ strings. And see there is one style that has only 2 members –



If $k = 3, p = 4$ then we will get such 3 styles causing the trouble

And this is because it was built out of a repeating unit of length two. So only two rotations are required to complete a cycle, therefore this group contains only two. None can split them into an equal number of styles. Then what is the benefit if we take p as a prime? It must work because if it is taken prime $p > 2$, they are odd, cannot be broken up into equal parts and it is a prime number, so no matter what kind of multicolored string we start with, it will always take p rotations or bead swaps to return to itself – the cycle length of every string must be p. The case of $p = 2$ is always true as $k^2 - k = k(k - 1)$ is always divisible by 2.

So the conclusion we can make – any multi-colored bracelet with a prime number of beads $p > 2$, must have a cycle length of $p > 2$, which can't be broken into equal-sized units, but not for the case of composite, then we will always have certain strings with shorter cycle lengths since it is actually built out of a repeating unit, and therefore will form smaller groups.

Reference: 1. AoPS Online
2. Khan Academy


THANK
YOU...