14 February 2012

Fermat's Little Theorem

Take 2 integers m p where p is prime.

then, $m^p = m \mod p$.

Proof: Let $M = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$

The list $\{m \cdot 1 \mod p, m \cdot 2 \mod p, \ldots, m \cdot (p-1) \mod p\}$

is exactly the same as the list $\{1, 2, \ldots, (p-1)\}$

They are equal because p is prime and unless p divides m

$\gcd(p, m) = 1$

So m is a unit in $\mathbb{Z}/p\mathbb{Z}$ and multiplication by m is reversible? (meaning that $m \cdot 1, m \cdot 2 \ldots \pmod p$ each have a unique n such that $m \cdot n = 1 \mod p$. with $p-1$ terms, each unique and ~~below~~ $\leq (p-1)$: the list must be the same)

Since the two lists are the same:

$$M = 1 \cdot 2 \cdot \ldots \cdot (p-1) = (m \cdot 1)(m \cdot 2) \cdot \ldots \cdot (m \cdot (p-1)) \mod p$$
$$= m^{p-1}(1 \cdot 2 \cdot \ldots \cdot (p-1)) \mod p$$
$$= m^{p-1} M \mod p$$

Then, $M - m^{p-1} M = M(1 - m^{p-1}) = 0 \mod p$.

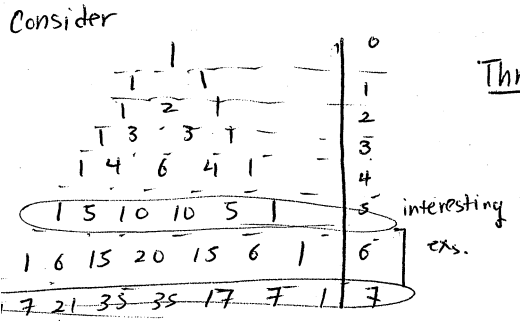
so either M is divisible by p or $1 - m^{p-1}$ is divisible by p.

We defined $M = 1 \cdot 2 \cdot \ldots (p-1)$, and it is not a multiple of p.

$\Rightarrow p \mid 1 - m^{p-1}$

$\Rightarrow 1 = m^{p-1} \mod p$; $m = m^1 \mod p = m \mod p$ ✓

Consider



Thm If we take p = prime, the Δ-numbers in row p are either 1 or mult of p

Proof: Δ-numbers are "choose" numbers. In fact the k^{th} number in row p is $\binom{p}{k}$ ← (View binomial thm)

$$\binom{p}{k} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-k+1)}{1 \cdot 2 \cdot \ldots \cdot k}$$

take $k \neq 0$ and $k \neq p$ (non "1" elements of row p)

Since none of the numbers $1, 2, \ldots, k$ has a factor of p,

$$\binom{p}{k} = p \underbrace{\frac{(p-1) \cdot (p-2) \cdot \ldots \cdot (p-k+1)}{1 \cdot 2 \cdot \ldots \cdot k}} \quad (p < k,\ p \text{ is prime})$$

then, it can be seen that the underbraced fraction is an integer. (We know $\binom{p}{k}$ is an integer... it's counting.)

$\Rightarrow \binom{p}{k}$ is a multiple of p $\quad \binom{p}{k} = p \cdot n$ where $n = \frac{(p-1)\ldots(p-k+1)}{1 \cdot \ldots \cdot k}$

In contrast, if $p \neq$ prime, then some entries in row p is not a multiple of p.

e.g. row 4: 1 4 6 4 1

$$\binom{4}{2} = \frac{4 \cdot 3}{1 \cdot 2}$$ ← because $p=4$ is divided by 2, the result is not divisible by 4.

Suppose $n = a \cdot b$ where a = smallest prime dividing n.

$$\binom{n}{a} = \frac{n(n-1)\cdots(n-a+1)}{1 \cdot 2 \cdot \ldots \cdot a}$$

what # is divisible by a

upstairs: n and n only (next smallest mult of a, $n-a$) does not make it)

downstairs: a (a is ~~does~~ defined to be smallest mult of a, obviously)

Then, $\binom{n}{a}$ has 1 less power of a in it than n ever did.

$\Rightarrow$ n cannot divide $\binom{n}{a}$, $n \nmid \binom{n}{a}$.

Art of counting, cont.

Q1) How many "words" can be created using the letters of the word "Mississippi"

Q0) .... CAR?

A0 Q0) is easy because there is no repetition of letters. Answer is factorial.

How can we recast Q1 to a problem w/o repetition?

$\Rightarrow$ ~~Consider~~ Suppose that we have unique letters.

$$M_1\ i_1\ s_1\ s_2\ i_2\ s_3\ s_4\ i_3\ p_1\ p_2\ i_4$$

we have 11! ways to rearrange subscripted letters

We "cluster" all arrangement that look alike (eg look like Mississippi)

in the same cluster, we put things that become equal when subscripts are erased.

the size of clusters;

e.g. "Mississippi" : ~~suppose~~ ~~we~~ ~~mark~~ we have 2 ways to rearrange Mississippi with 2 diff ps = 2!

Likewise...

Cluster size → ways for p's to "mingle" around $\cdot$ $\underbrace{2!}$ s's to mingle $\cdot$ $\underbrace{4!}$ i's to mingle $\cdot$ $\underbrace{4!}$ M's to mingle $\cdot$ $\underbrace{1!}$

(think of a scene where each identical letters stands and swap places with one another)

thus $\frac{11!}{2!\cdot 4!\cdot 4!\,1!}$ = # of rewriting Mississippi.

Thm: If you have n_1 times L_1 ; n_2 times L_2, ... n_k times L_k letters. there are

$$\frac{(n_1+n_2+\dots+n_k)!}{n_1!\dots n_k!}$$ words that can be made using all letters.

Def: Let $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_k)$ a vector of natural numbers.

we define $\alpha! = \alpha_1! \cdot \alpha_2! \cdot \dots \cdot \alpha_k!$

and if $N = \alpha_1+\alpha_2+\dots+\alpha_k$, we say $\binom{N}{\alpha} = \frac{N!}{\alpha!} = \frac{(\alpha_1+\alpha_2+\dots+\alpha_k)!}{\alpha_1!\cdots\alpha_k!}$

= "the α-th multinomial coefficient"

$\binom{N}{\alpha}$ counts the number of words length N that uses α_1 times L_1, ..., α_k times L_k.

... consider its name (multinomial = many binomial?)

$(x_1+x_2+\dots+x_k)^N$ = sum of monomials in $x_1, \dots, x_k$ all degree n.

If you explicitly multiply out this product, then a specific monomial $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_k^{\alpha_k}$ picks up the coefficient the numbers of ways of picking x_1 exactly α_1 times, x_2 exactly α_2 times, ... x_k exactly α_k times (ω word length L using # of aforementioned variable)

This is the same as the number of ways of making a word w/ N letters which have: α_1 times letter x_1

α_k times letter x_k = $\binom{N}{\alpha}$

example

$(x_1 + x_2 + x_3)^2 =$

$(2,0,0) \longleftrightarrow \binom{2}{(2,0,0)}\, x_1^2 = \frac{2!}{2!} = 1\, x_1^2$

$(1,1,0) \longleftrightarrow \binom{2}{(1,1,0)}\, x_1 x_2 = \left(\frac{2!}{1!1!}\right) = 2\, x_1 x_2$

$(1,0,1) \longleftrightarrow x_1 x_3$

$(0,2,0) \longleftrightarrow x_2^2$

$(0,1,1) \longleftrightarrow x_2 x_3$

$(0,0,2) \longleftrightarrow x_3^2$

returning to Mississippi

Algorithm: First, place "M" : $= \binom{11}{1}$

Second, place "S" $= \binom{10}{4}$

Third, place "P" $= \binom{6}{2}$

Fourth, place "I" $= \binom{4}{4}$

} multiply = number of runs of algorithm

✱ has no overcount!

(binom sort of takes care of it)

$= \binom{11}{(1,4,2,4)}$

we learn:

$\binom{11}{1}\binom{10}{4}\binom{6}{2}\binom{4}{4} = \binom{11}{(1,2,4,2)} =$ ~~any~~ $\frac{11!}{2!4!4!1!}$

→ also equals any variant of the algorithm (pick i, M, S, P = $\binom{11}{4}\binom{7}{1}\binom{6}{4}\binom{2}{2}$)

~~Q1 Given are~~

Q1 Given are 20 unmarked ping pong balls and 4 empty buckets labeled 1,2,3,4

How many ways can the balls be stored in the bucket?

A: Recall last lesson:

$$x_1 + x_2 + x_3 + x_4 = 20 ;$$

≈ fruit basket size 20 of 4 fruits

$= \binom{20+4-1}{4-1}$ (stars & bars)

Q2 How many words of length 20 can you make using ABCD.

A

= ~~4~~ choices for first letter · 4 choices for 2nd letter . . .

$= 4^{20}$ (w/o repetition)