INCLUSION - EXCLUSION "Fermat's last Theorem" 2013-09-10 (A)

TH. (FERMAT) For any prime p and any a not div. by p, $a^{p-1} \equiv 1 \pmod{p}$

DEF (EULER TOTIENT) $\varphi(n)$ = # of positive integers $\leq n$ that are relatively prime to n.
EX. For prime p, $\varphi(p) = p-1$.
TH (EULER) For any positive integer n and any a relatively prime to n, $a^{\varphi(n)} \equiv 1 \pmod{n}$
~~But how~~
PF. See Putnam Seminar, or Algebraic Structures.
But how to calculate $\varphi(n)$???
Oh! Whoops, wrong class. I thought I was substituting Fermat's Last Thm... What class is this?

Let's now switch to Combinatorics... inclusion-exclusion.

Q. ~~How many multiples of 2, 3, 5 are there in $\{1, 2, \ldots, 100\}$~~ ?

A.

DEF. Let S be a subset of a ground set X. Then $\mathbb{1}_S : X \to \mathbb{R}$ is fn that takes value:
$$\mathbb{1}_S(x) = \begin{cases} 0 & \text{if } x \notin S \\ 1 & \text{if } x \in S \end{cases}$$

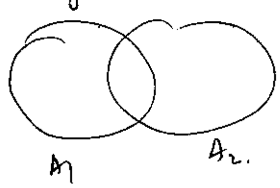
EX. If $S = \{2,4,5\}$ and $X = \{1,2,\ldots,10\}$, $\mathbb{1}_{\{2,4,5\}}$ sends $2,4,5 \mapsto 1$
else $\mapsto 0$

Could this function be useful for anything at all?

Let $A_1, A_2, \ldots, A_n$ be subsets (possibly overlapping) of some ground set X, and let $A = \bigcup_{i=1}^{n} A_i$.
Then consider:

$$f(x) := (\mathbb{1}_A(x) - \mathbb{1}_{A_1}(x)) \cdots (\mathbb{1}_A(x) - \mathbb{1}_{A_n}(x)), \text{ it's a fn } X \to \mathbb{R}.$$

Let's draw Venn diagram for $n = 2$,



Then what values does f take?
$$= (\mathbb{1}_A(x) - \mathbb{1}_{A_1}(x))(\mathbb{1}_A(x) - \mathbb{1}_{A_2}(x))$$

It's always 0!!

2013-09-11 (B)

So, $(\mathbb{1}_A - \mathbb{1}_{A_1})\cdots(\mathbb{1}_A - \mathbb{1}_{A_n}) = 0$ on all inputs

Expand! $\mathbb{1}_A(x)^n + \cdots + (-1)^n \mathbb{1}_{A_1}\mathbb{1}_{A_2}\cdots\mathbb{1}_{A_n} = 0$ on all inputs (*)

How many terms? 2^n of them.

How to simplify them?

OBS. $\mathbb{1}_S(x)\cdot\mathbb{1}_T(x) = \begin{cases} 0 & \text{if } x \in S \text{ and } x \in T \\ 1 & \text{else} \end{cases}$

so $\mathbb{1}_S\mathbb{1}_T = \mathbb{1}_{S\cap T}$.

So (*) is:

$$\begin{aligned}
&\mathbb{1}_A^n - \mathbb{1}_A^{n-1}\mathbb{1}_{A_1} - \mathbb{1}_A^{n-1}\mathbb{1}_{A_2} - \cdots - \mathbb{1}_A^{n-1}\mathbb{1}_{A_n} \\
&\quad + \mathbb{1}_A^{n-2}\mathbb{1}_{A_1}\mathbb{1}_{A_2} + \cdots \mathbb{1}_{A_n}^{n-2}\mathbb{1}\mathbb{1} \quad \text{all pairs} \\
&\quad - \mathbb{1}_A^{n-3}\mathbb{1}_{A_1}\mathbb{1}_{A_2}\mathbb{1}_{A_3} - \cdots \quad \text{all triples} \\
&\quad \vdots \\
&\quad + (-1)^n \mathbb{1}_{A_1}\mathbb{1}_{A_2}\cdots\mathbb{1}_{A_n}
\end{aligned} = 0.$$

Simplify with products

$$\begin{aligned}
&\mathbb{1}_A - \mathbb{1}_{A_1} - \mathbb{1}_{A_2} - \cdots \text{ all singles} \\
&\quad + \mathbb{1}_{A_1\cap A_2} + \cdots + \mathbb{1}_{A_{n-1}\cap A_n} \quad \text{all pairs} \\
&\quad - \mathbb{1}_{A_1\cap A_2\cap A_3} - \cdots \quad \text{all triples} \\
&\quad \vdots \\
&\quad \pm \mathbb{1}_{A_1\cap\cdots\cap A_n}
\end{aligned} = 0 \quad \text{for all } x \in X.$$

Sum over all $x \in X$.

OBS. $\sum_{x\in X} \mathbb{1}_S(x) = |S|$, so:

$$\begin{aligned}
&|A| - |A_1| - \cdots - |A_n| \quad \text{all singles} \\
&\quad + |A_1\cap A_2| + \cdots + |A_{n-1}\cap A_n| \quad \text{all pairs} \\
&\quad \vdots \\
&\quad + (-1)^n |A_1\cap\cdots\cap A_n|
\end{aligned} = 0 \Rightarrow$$

$|A| = |A_1\cup\cdots\cup A_n|$.

$$\begin{aligned}
&|A_1 \cup A_2 \cup \cdots \cup A_n| \\
&= |A_1| + \cdots + |A_n| \\
&- |A_1\cap A_2| - \cdots - |A_{n-1}\cap A_n| \\
&+ \text{all triples} \\
&\vdots \\
&+ (-1)^{n+1}|A_1\cap\cdots\cap A_n|.
\end{aligned}$$

2013-09-11 ©

Application: How to calculate $\varphi(n)$?

Prime factors: let $n = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$, where all p_i are distinct primes

# of ints in $\{1, 2, \cdots, n\}$ relatively prime to n?

↳ iff NO factor of any p_i.

So let $A_1 = $ # in $\{1, 2, \cdots, n\}$ that are div by p_1

$\vdots$

$A_t = $ # in ———— p_t.

(NOT rel. prime to n) $\Leftrightarrow$ in $A_1 \cup \cdots \cup A_t$.

So $\varphi(n) = n - |A_1 \cup \cdots \cup A_t|$

$$= n - \begin{pmatrix} |A_1| + \cdots + |A_t| \\ - |A_1 \cap A_2| \cdots - |A_{t-1} \cap A_t| \\ + \text{all triples} \\ \text{etc} \end{pmatrix} \quad \begin{matrix} \longrightarrow |A_i| = \frac{n}{p_i} \\ \longrightarrow |A_i \cap A_j| = \frac{n}{p_i p_j} \\ \vdots \\ \longrightarrow |A_1 \cap \cdots \cap A_n| = \frac{n}{p_1 p_2 \cdots p_t} \end{matrix}$$

$$= n \cdot \begin{bmatrix} 1 - \frac{1}{p_1} - \frac{1}{p_2} - \cdots - \frac{1}{p_t} \\ + \frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} + \cdot \text{all pairs} \\ - \frac{1}{p_1 p_2 p_3} \quad \text{triples} \\ \vdots \\ (-1)^{n} \frac{1}{p_1 \cdots p_n} \end{bmatrix} = n \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_t}\right)$$

$$= n \cdot \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

Ex. $\varphi(72) = 72 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 72 \times \frac{1}{2} \times \frac{2}{3} = \underline{24}$