last time \( \rightarrow \) Fermat's Thm

1) Euler Phi Function \( \phi(n) \)

2) Euler's Thm (generalization of Fermat's)

\( \phi(n) \) = the \# of values in the set \( \{1, 2, 3, \ldots, n-1\} \)

that are relatively prime with \( n \).

\( \phi(6) = 2 \), \( \gcd(1, 6) = \gcd(5, 6) = 1 \), but \( \gcd(2, 6) \neq 1 \)

\( \gcd(3, 6) \neq 1 \)

\( \gcd(4, 6) \neq 1 \)

\( \phi(7) = 6 \)

\( \phi(p) = p-1 \), \( p \in \text{Prime} \)

Goal: Can we derive a formula for \( \phi(n) \) given \( n \)'s prime factorization?

What about \( \phi(p^k) \) when \( p \in \text{Prime} \) \( k \in \mathbb{Z}^+ \)

\[
\begin{array}{cccc}
1, 2, 3, \ldots & p & 2p & \vdots \\
\vdots & 3p & \vdots & \ddots \\
\end{array}
\]

\( p^2 \) took \( \frac{p^2}{p} \) = \( p-1 \) values

- \( p \) values share common factor w/ \( p \)

\( \phi(p^2) = p^2 - p \), out of \( p^2 \) values \( p^{k-1} \) are divisible by \( p \)

Thus \( \phi(p^k) = p^k - p^{k-1} \)

Prove a critical fact:

if \( \gcd(m, n) = 1 \), then \( \phi(mn) = \phi(m) \phi(n) \).

This means \( \phi \) is a multiplicative function.

(All we have to do is multiply each term of form \( \phi(p^k) \) to get \( \phi(\text{any int}) \).}
Let's prove if \( \gcd(m,n) = 1 \), \( \phi(mn) = \phi(m)\phi(n) \).

1. Cross off values that share common factor w/n.

\[
\begin{array}{ccccccc}
1 & \times & 3 & \times & \ldots & \times & \times \\
\times & \times & \times & n+3 & \times & \ldots & \times \\
\times & \times & \times & \times & \times & \ldots & \times \\
2 & \times & 2\times 2 & \times & \times & \times & \times \\
\times & \times & \times & \times & \times & \times & \times \\
(\text{m-1})\times 1 & \times & \times & \times & \times & \times & \times \\
\end{array}
\]

Nature of GCD is: if \( \gcd(i,n) > 1 \) then \( \gcd(i+n,n) > 1 \) and \( \gcd(i+nj,n) > 1 \) if \( 1 \leq i \leq \text{m-1} \), \( j \in \mathbb{Z} \), \( 0 \leq j \leq \text{m-1} \).

By definition \( \phi(n) \) columns survive!

Next goal: Prove that in each column, exactly \( \phi(m) \) values "survive", they are relatively prime with \( m \).

Column \( i \) has the \( m \) values described in this set
\[
U = \{ i+nj \mid j \in \mathbb{Z} \land 0 \leq j \leq m-1 \}.
\]

Prove that each item in \( U \) is distinct mod \( m \).
We use proof by contradiction to prove this. Assume to the contrary that \( \exists j_1, j_2 \in \mathbb{Z} \wedge j_1 \neq j_2 \wedge 0 \leq j_1, j_2 \leq m-1 \)

such that

\[
i + nj_1 \equiv i + nj_2 \pmod{m} \\
nj_1 \equiv nj_2 \pmod{m} \\
nj_1 - nj_2 \equiv 0 \pmod{m} \\
n(j_1 - j_2) \equiv 0 \pmod{m}
\]

\[\Rightarrow m \mid (n*(j_1-j_2))\]

By Rule if \( \gcd(a,b)=1 \) and \( a \mid bc \), then \( a \mid c \).

Since \( \gcd(m,n)=1 \), it follows that \( m \mid (j_1-j_2) \)

\[1 \leq |j_1-j_2| \leq m-1\] so the divisibility assertion is contradicted by our known info about the difference between \( j_1 \) and \( j_2 \).

\[\Rightarrow \text{each column has exactly } \phi(m) \text{ values relatively prime with } m.\]

Total # of surviving values = \( \phi(n) \times \frac{\phi(m)}{\text{# columns in each col}} \)