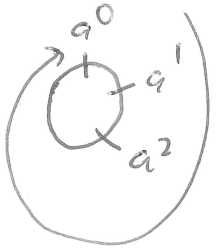
Fermat's Formula p prime $\gcd(a,p)=1$ $a^{p-1} \equiv 1 \bmod p$

Euler ϕ func: $\phi(n)$ = # values $\{1,2,\ldots,n\}$ rel prime w/ n.

Euler's formula $\gcd(a,n)=1$, $a^{\phi(n)} \equiv 1 \bmod n$

$\text{ord}_{a,n} = \min_{k>0}(k) \mid a^k \equiv 1 \bmod n$.

for all a,n $\gcd(a,n)=1$, $\text{ord}_{a,n} \mid \phi(n)$.



In modular exponentiation, each base has a cycle.
For primes, the longest possible cycle is length $p-1$.
For all primes, there exist values a, such that $\text{ord}_{a,p} = p-1$.
But for composites, n, there may or may not be an a such that $\text{ord}_{a,n} = \phi(n)$.

↳ last time we showed for all a, $n=15$
$\text{ord}_{a,n} = 1, 2$ or 4 none $= 8$.

Primality Testing (we need large primes to run RSA + other public key schemes)

- Trial Division is <u>TOO</u> slow!

Need to Differentiate btw primes, composites.
for all primes $a^{p-1} \equiv 1 \bmod p$.

Idea: Given n, Pick random a.
Calculate $a^{n-1} \bmod n$. If answer $\neq 1$, proof n is composite.

Problem: for some composites and some choices of a, perhaps $a^{n-1} \equiv 1 \bmod n$.

→ Call these pseudoprimes!

In general for random choice of n, a where n is composite, this is true less than 50% of time.

Unfortunately, for a very few values of n, it turns out that for ALL a's $\gcd(a,n)=1$ $a^{n-1} \equiv 1 \bmod n$. (Carmichael Numbers)
561, 17__?

A Pretty Good Primality Test

Repeat $100^{(k)}$ times:

1. Pick random a $1 < a < n-1$
2. Calculate $a^{n-1} \bmod n$, Calculate $\gcd(a,n)$.
3. If value $\neq 1$, return composite

* Return "IS PROBABLY PRIME"

2b) If gcd $\neq 1$ return false

As long as $n \neq$ Carmichael, this generally works!

Main Primality Test Used: Miller-Rabin

Improves on "pretty good test" by trying to catch Carmichael #s.

MillerRabin(int n)

1. $n-1 = 2^k n'$, $n' \in$ Odd, $k \geq 1$
2. ~~Calculate~~ Pick random a
3. if gcd(a,n) ≠ 1, return false (composite)
4. Calculate $X = a^{n'} \bmod n$.
5. If value in step 4 == 1, return is prob prime.
6. for (i = 0; i < k-1; i++) {
   $X = X^2 \bmod n$
   if (X == -1) is prob prime
   if (X == 1) return composite

for composite chance fails 1 trial is $\leq \frac{1}{4}$.

$n = 101$, $n-1 = 100 = 2^2 \cdot 25$, $(a^{25})^2 = a^{50}$, $(a^{50})^2 = a^{100}$

$n = 97$, $n-1 = 96 = 2^5 \cdot 3$, $a^3, a^6, a^{12}, a^{24}, a^{48}, a^{96} = 1$

Discrete Log Problem

Given a base a, and a result X, determine the exponent e s.t. $a^e \equiv X \bmod p$.

p is prime

$\log_2 64 = 6$

$2^{\square} \equiv 47 \bmod 97$.

10/23/19 (4)

This is a HARD problem. No one yet knows how to do this efficiently (poly time).

for each prime p, $\exists a \in \{1, 2, \ldots p-1\}$ s.t $\text{ord}_{a,p} = p-1$. These values of a are called generators, primitive roots.

$p = 11$

base \ exp	(1)	2	(3)	4	5	6	(7)	8	(9)	10
2	2	4	8	5	10	9	7	3	6	(1)
8	8	9	6	4	10	3	2	5	7	1
7	7	5	2	3	10	4	6	9	8	1
6	6	3	7	9	10	5	8	4	2	1
4	4	5	9	3	1					

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

not but not small

$(a^{(12)})^{p-1} \equiv 1$