CIS 3362 10/20/21

(1) Factoring

(2) Discrete Log Problem

(1a) Fermat Factoring
works better when #s (factors) are close together

$$23 \times 29 = (26-3)(26+3)$$
$$= 26^2 - 3^2$$

$$N = (x-y)(x+y)$$
$$N = x^2 - y^2$$
$$N + y^2 = x^2$$
$$\boxed{y^2 = x^2 - N}$$

Make guesses for x, in order and see if $x^2 - N$ is a perfect square

$N = 667$

$\sqrt{N} > 25$

x	$x^2 - N$	Square?
26	9	Yes $\Rightarrow (26-\sqrt{9})(26+\sqrt{9})$ 23×29

$N = 15347$

$X > 123$

X	$X^2 - N$	Square
124	29	No
125	278	No
126	529	Yes 23

$(126-23)(126+23)$

103×149 ✓

(1b) Pollard-Rho Factorization

~~$2^1, 2^2, 2^3, 2^4, \ldots 2^9, 2^{2a}$~~

~~gcd of these mod n.~~

$2, 5, 26, 277, 277^2+1$

$S_k = \left((S_{k-1})^2 + 1\right) \bmod n$ ← sequence

Discrete Log Problem → primitive root

prime p, generator a

we know from Fermat that

$a^{p-1} \equiv 1 \bmod p$ and for all $0 < k < p-1$

$a^k \not\equiv 1 \bmod p$.

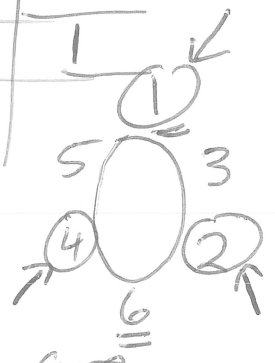
Given the equal $a^k \equiv X \bmod p$

a, X, p are known

What is k?

$a=3$, $p=7$

exp	0	1	2	3	4	5	6
base $a=3$	1	3	2	6	4	5	1



$$3^x \equiv 6 \pmod 7$$

Multiple Public Key Crypto Schemes are based on the "fact" that this is hard to solve quickly!

Other public key crypto schemes are based on the "fact" that factoring is hard to solve quickly.

How many primitive roots does a prime number have?

Pretend that a is a primitive root mod p. What are other primitive roots mod p?

a is such that $a^{p-1} \equiv 1 \bmod p$ and $a^k \not\equiv 1 \bmod p$, $0 < k < p-1$.

Consider $a' = a^2$, since $p-1$ is even, we see that

$$(a')^{\frac{p-1}{2}} = a^{2 \times \frac{(p-1)}{2}} = a^{p-1} \equiv 1 \bmod p.$$

a^k is NOT a primitive root if $\gcd(k, p-1) \neq 1$.

Alternatively a^k IS a primitive root if $\gcd(k, p-1) = 1$. Now previous exponent on (a^k) will be a multiple of $p-1$.

For

How many numbers is this true?

$\phi(p-1)$

# of primitive roots of a prime p