RSA vs. Factoring

the following problems are <u>equivalent</u>:

1. given $N = pq$, compute p, q
2. given $N = pq$, compute $\varphi(N) = (p-1)(q-1)$
3. given $N = pq$, e, compute d where $ed \equiv_{\varphi(N)} 1$
4. given $N = pq$, compute <u>any</u> $x \not\equiv_N \pm 1$ where $x^2 \equiv_N 1$

"equivalent" means: either <u>all</u> have poly-time algos.
or <u>none</u> of them do.

How to show equivalence ("reduction")

- If a poly-time algo exists for #1, I could use it as subroutine to solve #2 in poly-time
- #2 ⇒ #3, #3 ⇒ #4, #4 ⇒ #1

Note: #1 ⇒ #2, #2 ⇒ #3 are trivial

(#4 ⇒ #1)

Def: x is a <u>square root of unity</u> mod N if

$$x^2 \equiv_N 1$$

If $x \equiv_N \pm 1$ then x is a <u>trivial</u> sqrt unity
otherwise <u>nontrivial</u> sqrt unity

Ex: $N = 15 = 3 \times 5$

				(-7	-4	-2	-1)	
$x \in \mathbb{Z}_{15}^*$:	1	2	4	7	8	11	13	14
$x^2 \bmod 15$:	1	4	1	4	4	1	4	1

= sqrts of unity

Claim: If $N = pq$ (RSA modulus) then there are 4 sqrts of unity mod N

Proof:

$$x^2 \equiv_N 1$$

$$\Big\Updownarrow \text{ CRT}$$

$$\text{AND} \begin{cases} x^2 \equiv_p 1 & \Leftrightarrow & x \equiv_p \pm 1 \\ x^2 \equiv_q 1 & \Leftrightarrow & x \equiv_q \pm 1 \end{cases}$$

since p, q primes

So $\begin{cases} x \equiv_p 1 \\ x \equiv_q 1 \end{cases}$ $\begin{cases} x \equiv_p 1 \\ x \equiv_q -1 \end{cases}$ $\begin{cases} x \equiv_p -1 \\ x \equiv_q 1 \end{cases}$ $\begin{cases} x \equiv_p -1 \\ x \equiv_q -1 \end{cases}$

are the 4 possible values of x

Claim: If you can find nontrivial sqrt unity x mod $N = pq$ then $\gcd(x \pm 1, N)$ are the factors of N

Ex: $N = 15$, $x = 4$:

$$\gcd(4+1, 15) = 5$$
$$\gcd(4-1, 15) = 3$$

$x = 11$:

$$\gcd(11+1, 15) = 3$$
$$\gcd(11-1, 15) = 5$$

Proof: $x^2 \equiv_N 1 \Leftrightarrow x^2 - 1$ is multiple of N

$\Leftrightarrow$ $\cancel{N}$ pq divides $(x^2-1) = (x-1)(x+1)$

$x \not\equiv_N \pm 1 \Leftrightarrow x \pm 1$ is NOT multiple of N

$\Leftrightarrow$ $\cancel{N}$ pq doesn't divide $x+1$ or $x-1$

So $(x-1)(x+1)$ has factors of p & q both
but p & q not both factors of either term

$\rightarrow$ $p \mid x-1$ but $q \nmid x-1$

$\rightarrow$ $\gcd(x-1, pq) = p$

(#3 $\Rightarrow$ #4) If you can find d given $N=pq$, e
then you can find nontriv. sqrt unity

Idea: Given (N, e)

compute $d \equiv_{\varphi(N)} e^{-1}$ (by assumption)

write $ed-1 = 2^s \cdot r$ where r is even

$$ed-1 = \underbrace{\boxed{\text{binary}\ \ 0\cdots0}}_{s \text{ zeroes}}$$

choose $w \leftarrow \mathbb{Z}_N$

compute (mod N)

$$1,\ w^r,\ w^{2r},\ w^{4r},\ w^{8r},\ \ldots,\ w^{2^s r}$$

square

Claim: eventually this sequence reaches "1"

$$w^{2^s r} = w^{ed-1} = (w^{ed})(w^{-1}) \equiv w\,(w^{-1}) = 1$$

RSA correctness

Therefore: Item before first "1" in sequence
is a sqrt of unity