Theorems for RSA

Definition. *The congruence class* $[a]_n = \{x \in \mathbb{Z} : x\%n = a\%n\}$.
The set $\mathbb{Z}_n = \{[x]_n : x = 0, 1, 2, ...n-1\}$. *The set* $\mathbb{Z}_n^\times = \{[x]_n \in \mathbb{Z}_n : [x]_n^{-1} exists\}$.

Definition. *The order* $O([a]_n) = \min\{b : b \in \mathbb{N}\backslash\{0\}$ *and* $[a]_n^b = [1]_n\}$

Theorem. *A congruence class* $[a]_n$ *has finite order if and only if* $\gcd(a, n) = 1$.

Corollary. *A congruence class has finite order if and only if it is invertible.*

Theorem. *If* $[a]_n$ *has finite order* k *and* $k|r - s$, *then* $[a]_n^r = [a]_n^s$.

Theorem. *If* $[a]_n$ *has finite order* k *and* $[a]_n^r = [a]_n^s$, *then* $k|r - s$.

Corollary. *If* $[a]_n$ *has finite order* k *and* $[a]_n^r = [1]_n$, *then* $k|r$.

Theorem (Fermat's little theorem)**.** *If* p *is a prime number and* a *is relatively prime to* p, *then* $[a]_p^{p-1} = [1]_p$.

Corollary. *If* p *is a prime number and* a *is relatively prime to* p, *then* $p|a^p - a$.

Definition (Totient)**.** *The totient function* $\phi(n)$ *is the number of invertible congruence classes modulo* n.

Theorem (Euler's theorem)**.** *If* $[a]_n$ *has finite order, then* $[a]_n^{\phi(n)} = [1]_n$.

Corollary. *If* $[a]_n$ *has finite order, then* $n|a^{\phi(n)} - 1$

Theorem 1. *If* p *is prime,* $\phi(p^n) = p^n - p^{n-1}$.

Lemma. *If* $\gcd(p, q) = 1$, *then* $\gcd(xp + yq, pq) = 1$ *if and only if* $\gcd(x, q) = \gcd(y, p) = 1$.

Lemma (Generalized Division Theorem)**.** *If* $\gcd(p, q) = 1$, *then for any integer* x, *there is a unique triple of integers* (a, b, c) *such that* $x = aq + bp + cpq$, $0 \leq a < p$, *and* $0 \leq b < q$.

Theorem. *If* p *and* q *are relatively prime, then* $\phi(pq) = \phi(p)\phi(q)$.

Theorem. *If* x *has prime-factorization*

$$x = \prod_{i=0}^{K} p_i^{a_i},$$

in standard form where $a_i > 0$ *for each* i *and* $i < j$ *implies* $p_i < p_j$, *then*

$$\phi(x) = \prod_{i=0}^{K} (p_i - 1)p_i^{a_i - 1}.$$

Orders of congruence classes $[a]_n$ for first 24 values of n.

n	$\phi(n)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	1	∞																								
2	1	∞	1																							
3	2	∞	1	2																						
4	2	∞	1	∞	2																					
5	4	∞	1	4	4	2																				
6	2	∞	1	∞	∞	∞	2																			
7	6	∞	1	3	6	3	6	2																		
8	4	∞	1	∞	2	∞	2	∞	2																	
9	6	∞	1	6	∞	3	6	∞	3	2																
10	4	∞	1	∞	4	∞	∞	∞	4	∞	2															
11	10	∞	1	10	5	5	5	10	10	10	5	2														
12	4	∞	1	∞	∞	∞	2	∞	2	∞	∞	∞	2													
13	12	∞	1	12	3	6	4	12	12	4	3	6	12	2												
14	6	∞	1	∞	6	∞	6	∞	∞	∞	3	∞	3	∞	2											
15	8	∞	1	4	∞	2	∞	∞	4	4	∞	∞	2	∞	4	2										
16	8	∞	1	∞	4	∞	4	∞	2	∞	2	∞	4	∞	4	∞	2									
17	16	∞	1	8	16	4	16	16	16	8	8	16	16	16	4	16	8	2								
18	6	∞	1	∞	∞	∞	6	∞	3	∞	∞	∞	6	∞	3	∞	∞	∞	2							
19	18	∞	1	18	18	9	9	9	3	6	9	18	3	6	18	18	18	9	9	2						
20	8	∞	1	∞	4	∞	∞	∞	4	∞	2	∞	2	∞	4	∞	∞	∞	4	∞	2					
21	12	∞	1	6	∞	3	6	∞	∞	2	∞	6	6	∞	2	∞	∞	3	6	∞	6	2				
22	10	∞	1	∞	5	∞	5	∞	10	∞	5	∞	∞	∞	10	∞	5	∞	10	∞	10	∞	2			
23	22	∞	1	11	11	11	22	11	22	11	11	22	22	11	11	22	22	11	22	11	22	22	22	2		
24	8	∞	1	∞	∞	∞	2	∞	2	∞	∞	∞	2	∞	2	∞	∞	∞	2	∞	2	∞	∞	∞	2	