Proofs of correctness [edit]

Proof using Fermat's little theorem [edit]

The proof of the correctness of RSA is based on Fermat's little theorem. This theorem states that if p is prime and p does not divide an integer a then

$$a^{p-1} \equiv 1 \pmod{p}$$

We want to show that $m^{ed} \equiv m \pmod{pq}$ for every integer m when p and q are distinct prime numbers and e and d are positive integers satisfying

$$ed \equiv 1 \pmod{\lambda(pq)}.$$

Since $\lambda(pq) = \operatorname{lcm}(p-1, q-1)$ is, by construction, divisible by both $p - 1$ and $q - 1$, we can write

$$ed - 1 = h(p-1) = k(q-1)$$

for some nonnegative integers h and k.

(Note: In particular, the statement above holds for any e and d that satisfy $ed \equiv 1 \pmod{(p-1)(q-1)}$, since $(p-1)(q-1)$ is divisible by $\lambda(pq)$, and thus trivially also by $p - 1$ and $q - 1$. However, in modern implementations of RSA, it is common to use a reduced private exponent d that only satisfies the weaker but sufficient condition $ed \equiv 1 \pmod{\lambda(pq)}$.)

To check whether two numbers, like m^{ed} and m, are congruent mod pq it suffices (and in fact is equivalent) to check they are congruent mod p and mod q separately. (This is part of the Chinese remainder theorem, although it is not the significant part of that theorem.) To show $m^{ed} \equiv m \pmod{p}$, we consider two cases: $m \equiv 0 \pmod{p}$ and $m \not\equiv 0 \pmod{p}$.

In the first case, m is a multiple of p, thus m^{ed} is a multiple of p, so $m^{ed} \equiv 0 \equiv m \pmod{p}$. In the second case

$$m^{ed} = m^{ed-1}m = m^{h(p-1)}m = (m^{p-1})^h m \equiv 1^h m \equiv m \pmod{p}$$

where we used Fermat's little theorem to replace $m^{p-1} \bmod p$ with 1.

The verification that $m^{ed} \equiv m \pmod{q}$ proceeds in a similar way, treating separately the cases $m \equiv 0 \pmod{q}$ and $m \not\equiv 0 \pmod{q}$.

In the first case m^{ed} is a multiple of q, so $m^{ed} \equiv 0 \equiv m \pmod{q}$. In the second case

$$m^{ed} = m^{ed-1}m = m^{k(q-1)}m = (m^{q-1})^k m \equiv 1^k m \equiv m \pmod{q}$$

This completes the proof that, for any integer m, and integers e, d such that $ed \equiv 1 \pmod{\lambda(pq)}$,

$$(m^e)^d \equiv m \pmod{pq}.$$