# A Generalisation of the RSA Congruence

**Henry O. Omokaro**
**Department of Mathematics,**
**University of Benin, Benin City.**

**Abstract**

*The RSA congruence* [5] *states that: If p, q are prime numbers and e, d positive integers such that* $m < pq$ *and* $ed \equiv 1 \bmod (p-1)(q-1)$ *then* $m^{ed} \equiv m \bmod pq$. *In this work the RSA congruence is extended to a wider class of integers. It is proved to be true for a finite number of primes* $p_1, p_2, \cdots, p_n$ *instead of just two primes p and q.*

**pp 27 – 28**

## 1.0 Introduction

Let p and q be prime numbers, clearly their greatest common divisor, (p, q) = 1 since the Euler – phi function $\phi$ is multiplicative [6], $\phi(p) = p-1$, $\phi(q) = q-1$ so that: $(p-1)(q-1) = \phi(p)\,\phi(q) = \phi(pq)$.

We can now therefore rewrite the RSA congruence which we stated above as follows:

## 2.0 Theorem: The RSA Congruence

*If p,q are primes and e,d positive integers such that* $m < pq$ *and* $ed \equiv 1 \bmod \phi(pq)$. *Then* $m^{ed} \equiv m \bmod pq$.[5]

## 3.0 Proposition

Let *e,d,m,n be positive integers such that* $(m,n) = 1$ *and* $ed \equiv 1 \bmod \phi(n)$. *Then* $m^{ed} \equiv m \bmod n$.

**Proof**

Now, $ed \equiv 1 \bmod \phi(n) \Rightarrow \exists$ an integer k such that $ed - 1 = k\phi(n)$. $\therefore ed = k\phi(n) + 1$

$$\therefore m^{ed} = m^{k\phi(n)+1} = m^{k\phi(n)}\, m = 1^k .m \bmod n$$

and the proof is complete.

## 4.0 Theorem [2]

*Let a, b be integers and* $m_1, m_2, \ldots, m_r$ *be positive integers pairwise relatively prime such that:* $a \equiv b \bmod m_1$, $a \equiv b \bmod m_2$, ..., $a \equiv \bmod m_r$ *then* $a \equiv b \bmod m_1 m_2 \ldots m_r$.[2],[4].

## 5.0 Theorem [1]

*Every integer* $n > 1$ *can be written as a product of primes* $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ *where* $p_1 < p_2 < \ldots < p_k$ *are primes.*[1],[3].

## 6.0 Definition

If $a_1 = a_2 = \ldots = a_k = 1$ in the above representation, we say n is a simple product of primes.

## 7.0 Lemma

If *p* is prime then for any integer a and any positive integers, *k, r* $a^{kp(r-1)}(p-1) + 1 \equiv a \bmod p$

**Proof**

We will consider 2 cases:

**Case 1:** If (a, p) = 1. Euler's theorem $\Rightarrow$ $a^{p-1} \equiv 1 \bmod p$ $= (a^{p-1})^{kp^{(r-1)}} .a = (1)^{kp^{(r-1)}} .a \bmod p$. Therefore

$a^{kp^{(r-1)}}(p-1) + 1 \equiv a \bmod p.$

**Case 2:** $(a, p) > 1$
If $(a, p) > 1$ then p is a divisor of a and the identity holds trivially.

## 8.0 Theorem

*Let n be a simple product of r distinct primes for some r and let e, d be positive integers satisfying* $ed \equiv 1 \bmod \phi(n)$ *then for any positive integer* $m < n$, $m^{ed} \equiv m \bmod n$.

**Proof**

Since n is given to be a simple product of primes, we can write $n = p_1 p_2 \ldots p_k$. Clearly $(p_i, p_j) = 1$, $i \neq j$, from one of our previous lemmas, if we are able to show that $m^{ed} \equiv m \bmod p_i$, $i = 1, 2, \ldots, r$ for any positive integer $m < n$ and e,d satisfying $ed \equiv 1 \bmod \phi(n)$ we will be through. Now $ed \equiv 1 \bmod \phi(n)$ $\Rightarrow ed = k\phi(n) + 1$ for some positive integer k. We consider 2 cases:

**Case 1:**

Suppose $(m, p_i) = 1$ then $m^{ed} = m^{k\phi(n)+1} = m^{k\phi(n)} . m$. Now $\phi(n) = \phi(p_1 p_2 \ldots p_r)$

$$= (p_1 p_2 \ldots p_r)\left[\frac{p_1 - 1}{p_1}\right]\left[\frac{p_2 - 1}{p_2}\right]\ldots\left[\frac{p_r - 1}{p_r}\right]$$

So that $m^{ed} = m^{k(p_1-1)(p_2-1)\ldots(p_r-1)} . m$ and for any $i$, $1 \leq i \leq r$, $m_{ed} = m^{k(p_i-1)(p_1-1)(p_2-1)\ldots(p_{i-1}-1)(p_{i+1}-1)\ldots(p_r-1)} . m$

$$= m^{k(p_i-1)(p_1-1)(p_2-1)\ldots(p_{i-1}-1)(p_{i+1}-1)\ldots(p_r-1)} . m$$

$$\equiv 1.m \bmod p_i$$

**Case 2**

If $(p_i, m) > 1$ then $P_i \mid m$ and so $m^{ed} \equiv m \bmod n$.

## 9.0 Remarks

If we put $n = p_1 p_2$ ( a product of 2 primes) we obtain the original RSA congruence:

## 10.0 Corollary

*If p q are primes and e, d positive integers such that* $ed \equiv 1 \bmod (p-1)(q-1)$ *then for any positive integer* $m < pq$, $m^{ed} \equiv m \bmod pq$.

**Proof**

Put $p_1 = p$ and $p_2 = q$ and $n = p_1 p_2$. The result follows from the last theorem.

### References


[1] Chaum, D., Rivest, R. L., Shermans, A. T., (1983) Advanceds in Cryptology, Proceedings of Crypto 82, Plenum: New York.

[2] Chaum, D., Rivest, R. L., Shermans, A. T., (1984) Advaneeds in Cryptology, Proceedings of Crypto 83, Plenum: New York

[3] Eynden, V. C.(1987) Elementary Number Theory, McGraw hill Inc., New York

[4] Williams, H. C ed. (1986) Advances in Cryptology, Crypto '85, Springer-Verlag, Berlin.

[5] Rivest, R. L.; Shamir, A.; Adleman, L. (1978) A method for obtaining digital signature and public key cruptosystem. Communications of ACM Vol. 21.

[6] Rosen, K. H. (1992) Elementary Number Theory and its Applications, Addison-Wesley Publishing Company, New York.