Modular Exponentiations and the Identity Map on Z_n

Richard Alan Winton, Ph.D. †

Abstract

Several known results concerning modular exponentiations and important related special cases are presented. These results are generalized in the main theorem, which extends the result a corollary to Fermat's Theorem. The main theorem is also a modified version of a corresponding corollary to Euler's Theorem. An equivalence is established between the specific types of modular exponentiations addressed in the paper and the identity map on $\mathbf{Z}_n$. The final result provides an application which improves the computational efficiency in previously published cryptosystems.

Introduction

Fermat and Euler both produced remarkable results in number theory. Some of their work involved modular exponentiations. In certain cases, these exponentiations had important applications due to the fact that they produced the identity map on $\mathbf{Z}_n$ for some positive integer n. However, the calculations associated with such exponentiations can become quite large. Consequently, results for making these calculations more computationally efficient are critical. We will develop such a result for a type of modular exponentiation which is used in applications to cryptology. First we present some historical aspects of the problem.

Fermat's Theorem

Among the many great achievements in number theory is the famous result known as Fermat's Theorem, also known as Fermat's Little Theorem or Fermat's Lesser Theorem ([1, p. 89, Theorem 5.1],[4, p. 136, Theorem 4.9], [7, p. 43, Theorem 2.36]). Pierre de Fermat conjectured this result in a letter dated October 18, 1640. The earliest completed proof was found in manuscripts written by Leibniz before 1683 which are located in the Hanover, Germany Library. However, an official proof was not published until Euler's proof in 1736 in the Proceedings of the Saint Petersburg Academy [2, p. 514].

Theorem 1. (Fermat's Theorem) Suppose p is a prime, b is an integer, and $p \nmid b$. Then $b^{p-1} \equiv 1 \pmod{p}$.

Several corollaries are immediate from Theorem 1. Corollary 2 is frequently presented in conjunction with or immediately following Fermat's Theorem ([4, p. 136, Theorem 4.10],[7, p. 43, Theorem 2.37]).

Corollary 2. (Fermat's Corollary) Suppose p is a prime and b is an integer. Then $b^p \equiv b \pmod p$.

Proof: If p|b, then $b \equiv 0 \pmod p$. Therefore $b^p \equiv 0^p \pmod p = 0 \pmod p \equiv b \pmod p$.

On the other hand, if $p \nmid b$, then $b^{p-1} \equiv 1 \pmod p$ by Theorem 1. Thus $b^p = b\, b^{p-1} \equiv b \cdot 1 \pmod p = b \pmod p$.

Hence in either case we have $b^p \equiv b \pmod p$.

Corollaries 3 and 4 follow immediately from Theorem 1. They have important applications to basic exponential cryptosystems.

Corollary 3. Suppose p is a prime, b is an integer, e is a positive integer, $\gcd\{e,p-1\} = 1$, and $d = e^{-1} \pmod{p-1}$. Then $b^{ed} \equiv b \pmod p$.

Proof: If p|b then $b \equiv 0 \pmod p$. Therefore $b^{ed} \equiv 0^{ed} \pmod p = 0 \pmod p \equiv b \pmod p$.

On the other hand, if $p \nmid b$ then $b^{p-1} \equiv 1 \pmod p$ by Theorem 1. Since $d = e^{-1} \pmod{p-1}$, then $ed \equiv 1 \pmod{p-1}$. Thus $ed = 1 + t(p-1)$ for some integer t. Therefore $b^{ed} = b^{1+t(p-1)} = b\left(b^{p-1}\right)^t \equiv b \cdot 1^t \pmod p = b \pmod p$.

Hence in either case we have $b^{ed} \equiv b \pmod p$.

We now present an important special case of Corollary 3 in which the arbitrary integer b is replaced with an element of $\mathbf{Z}_p$. Thus b has the additional restriction that $0 \le b \le p-1$. Therefore Corollary 4 establishes the relationship between the type of modular exponentiation specified in Corollary 3 and the identity map $1_{\mathbf{Z}_p}$ on $\mathbf{Z}_p$.

Corollary 4. Suppose p is a prime, $b \in \mathbf{Z}_p$, e is a positive integer, $\gcd\{e,p-1\} = 1$, and $d = e^{-1} \pmod{p-1}$. Then $b^{ed} \pmod p = b$. In other words, the function defined on $\mathbf{Z}_p$ by $f(b) = b^{ed} \pmod p$ is the identity map $1_{\mathbf{Z}_p}$ on $\mathbf{Z}_p$.

Proof: $b^{ed} \equiv b \pmod p$ by Corollary 3, so that $b^{ed} \pmod p = b \pmod p$. Furthermore, $b \pmod p = b$ since $b \in \mathbf{Z}_p$. Hence $f(b) = b^{ed} \pmod p = b = 1_{\mathbf{Z}_p}(b)$.

Having presented Fermat's Theorem and the resulting corollaries, we continue now with the historical development of this paper. The next stage is attributed to the work of Euler.

Euler's Theorem

In 1760 Leonhard Euler produced Euler's Theorem [2, p. 534]. This result extends Fermat's Theorem by replacing the prime modulus with an arbitrary positive integer ([8, p. 23, Theorem 2.8],[9, p. 21, Theorem 12]). Note that for the prime modulus p in the hypothesis of Fermat's Theorem, $p \nmid b$ is equivalent to $\gcd\{b,p\} = 1$. Furthermore, $p-1 = \phi(p)$. Thus Fermat's Theorem can alternately be stated as follows.

Alternate form of Fermat's Theorem: Suppose p is a prime, b is an integer, and $\gcd\{b,p\} = 1$. Then $b^{\phi(p)} \equiv 1 \pmod{p}$.

Euler's Theorem then follows by replacing the prime p in the alternate form of Fermat's Theorem with an arbitrary positive integer n.

Theroem 5. (Euler's Theorem) Suppose n is a positive integer, b is an integer, and $\gcd\{b,n\} = 1$. Then $b^{\phi(n)} \equiv 1 \pmod{n}$.

Euler's Theorem produced related results which generalized those yielded by Fermat's Theorem. Corollaries 6 and 7 are immediate from Euler's Theorem. These results correspond in their relationship with Euler's Theorem to Corollaries 3 and 4, respectively, relative to their relationship with Fermat's Theorem.

Corollary 6. Suppose n and e are positive integers, b is an integer, $\gcd\{b,n\} = 1$, $\gcd\{e,\phi(n)\} = 1$, and $d = e^{-1} \pmod{\phi(n)}$. Then $b^{ed} \equiv b \pmod{n}$.

Proof: Since $\gcd\{b,n\} = 1$, then $b^{\phi(n)} \equiv 1 \pmod{n}$ by Theorem 5. Furthermore, since $d = e^{-1} \pmod{\phi(n)}$, then $ed \equiv 1 \pmod{\phi(n)}$. Thus $ed = 1 + t\cdot\phi(n)$ for some integer t. Therefore $b^{ed} = b^{1+t\cdot\phi(n)} = b\left(b^{\phi(n)}\right)^t \equiv b\cdot 1^t \pmod{n} = b \pmod{n}$.

We now present an important special case of Corollary 6. Corollary 7 establishes the relationship between the type of modular exponentiation specified in Corollary 6 and the identity map $1_{\mathbf{Z}_n}$ on $\mathbf{Z}_n$.

Corollary 7. Suppose n and e are positive integers, $b \in \mathbf{Z}_n$, $\gcd\{b,n\} = 1$, $\gcd\{e,\phi(n)\} = 1$, and $d = e^{-1} \pmod{\phi(n)}$. Then $b^{ed} \pmod{n} = b$. In other words, the function defined on $\mathbf{Z}_n$ by $f(b) = b^{ed} \pmod{n}$ is the identity map $1_{\mathbf{Z}_n}$ on $\mathbf{Z}_n$.

Proof: $b^{ed} \equiv b \pmod{n}$ by Corollary 6, so that $b^{ed} \pmod{n} = b \pmod{n}$. Furthermore, $b \pmod{n} = b$ since $b \in \mathbf{Z}_n$. Hence $f(b) = b^{ed} \pmod{n} = b = 1_{\mathbf{Z}_n}(b)$.

Main Results

We now present the main results of the paper. Theorem 8 is a modified version of Corollary 6. The requirement that $\gcd\{b,n\} = 1$ in the hypothesis of Corollary 6 is omitted. However, there is a price for this improvement. The modulus n, which is an arbitrary positive integer in Corollary 6, must be restricted to a positive integer which is the product of distinct primes. Thus Theorem 8 generalizes Corollary 3 by extending the result for a prime modulus p to any modulus which is the product of distinct primes. In other words, Corollary 3 is a special case of Theorem 8 in which $r = 1$.

Theorem 8. Suppose $\{p_i\}_{i=1}^{r}$ is a collection of distinct primes, $n = \prod_{i=1}^{r} p_i$, b is an integer, e is a positive integer, $\gcd\{e,\phi(n)\} = 1$, and $d = e^{-1} \pmod{\phi(n)}$. Then $b^{ed} \equiv b \pmod{n}$.

Proof: Case 1. If $n|b$ then $b \equiv 0 \pmod{n}$. Therefore $b^{ed} \equiv 0^{ed} \pmod{n} = 0 \pmod{n} \equiv b \pmod{n}$.

On the other hand, suppose that $n \nmid b$. Since $d = e^{-1} \pmod{\phi(n)}$, then $ed \equiv 1 \pmod{\phi(n)}$. Thus $ed = 1 + t\cdot\phi(n)$ for some integer t.

Case 2. If $r = 1$, then $n = p_1$ is prime. Since $n \nmid b$, then $\gcd\{b,n\} = 1$. Therefore $b^{ed} \equiv b \pmod{n}$ by Corollary 6 (or Corollary 3).

Case 3. Now suppose $r > 1$ and $\gcd\{b,n\} = 1$. Therefore $b^{\phi(n)} \equiv 1 \pmod{n}$ by Theorem 5. Then $b^{ed} = b^{1+t\cdot\phi(n)} = b\left(b^{\phi(n)}\right)^t \equiv b\cdot 1^t \pmod{n} = b \pmod{n}$.

Case 4. Finally, suppose $r > 1$ and $\gcd\{b,n\} > 1$. Then $p_u|b$ for some u, $1 \le u \le r$. However, since $n \nmid b$, then $p_v \nmid b$ for some v, $1 \le v \le r$. Without loss of generality, suppose k is an integer, $1 \le k \le r-1$, $p_i|b$ for $1 \le i \le k$, and $p_i \nmid b$ for $k+1 \le i \le r$.

If $1 \le i \le k$, then $p_i|b$, so that $b \equiv 0 \pmod{p_i}$. Then $b^{ed} \equiv 0^{ed} \pmod{p_i} = 0 \pmod{p_i}$. However, if $k+1 \le i \le r$, then $p_i \nmid b$, so that $b^{p_i-1} \equiv 1 \pmod{p_i}$ by

Theorem 1. Define $s = \prod_{j \neq i} (p_j - 1)$. Then $b^{ed} = b^{1+t\cdot\phi(n)} = b^{1+t(p_1-1)\cdots(p_r-1)} = b\left(b^{p_i-1}\right)^{ts} \equiv b \cdot 1^{ts} \pmod{p_i} = b \pmod{p_i}$.

Therefore $b^{ed} \equiv 0 \pmod{p_i}$ for $1 \le i \le k$ and $b^{ed} \equiv b \pmod{p_i}$ for $k+1 \le i \le r$. However, since $p_i | b$ for $1 \le i \le k$, then $b \equiv 0 \pmod{p_i}$ for $1 \le i \le k$. Furthermore, it is clear that $b \equiv b \pmod{p_i}$ for $k+1 \le i \le r$. Thus both b^{ed} and b are solutions of the linear system

$$x \equiv 0 \pmod{p_i} \text{ for } 1 \le i \le k;$$
$$x \equiv b \pmod{p_i} \text{ for } k+1 \le i \le r.$$

Since $\{p_i\}_{i=1}^{r}$ is a collection of distinct primes, then $b^{ed} \equiv b \pmod{n}$ by the Chinese Remainder Theorem ([3, p. 39, Theorem 2],[5, p. 19, Theorem I.3.3], [6, p. 118, Theorem 5.4]).

Hence in all possible cases we have $b^{ed} \equiv b \pmod{n}$. The result follows.

Corollary 9 is a direct consequence of Theorem 8. Furthermore, its relationship with Theorem 8 corresponds to the relationship of Corollary 7 with Corollary 6, as well as that of Corollary 4 with Corollary 3, respectively. Finally, Corollary 9 establishes the relationship between the type of modular exponentiation specified in Theorem 8 and the identity map $1_{\mathbf{Z}_n}$ on $\mathbf{Z}_n$.

Corollary 9. Suppose $\{p_i\}_{i=1}^{r}$ is a collection of distinct primes, $n = \prod_{i=1}^{r} p_i$, $b \in \mathbf{Z}_n$, e is a positive integer, $\gcd\{e,\phi(n)\} = 1$, and $d = e^{-1} \pmod{\phi(n)}$. Then $b^{ed} \pmod{n} = b$. In other words, the function defined on $\mathbf{Z}_n$ by $f(b) = b^{ed} \pmod{n}$ is the identity map $1_{\mathbf{Z}_n}$ on $\mathbf{Z}_n$.

Proof: $b^{ed} \equiv b \pmod{n}$ by Theorem 8, so that $b^{ed} \pmod{n} = b \pmod{n}$. Furthermore, $b \pmod{n} = b$ since $b \in \mathbf{Z}_n$. Hence $f(b) = b^{ed} \pmod{n} = b = 1_{\mathbf{Z}_n}(b)$.

Corollary 10 is immediate from Corollary 9 and provides an important special case of that result for which the modulus is the product of precisely two distinct primes. Since several well known public and private key cryptosystems are based on moduli which are constructed in this manner, Corollary 10 has useful applications to cryptology.

Corollary 10. Suppose p and q are distinct primes, $n = pq$, $b \in \mathbf{Z}_n$, e is a

positive integer, gcd{e,ϕ(n)} = 1, and d = e^{-1} (mod ϕ(n)). Then b^{ed} (mod n) = b. In other words, the function defined on $\mathbf{Z}_n$ by f(b) = b^{ed} (mod n) is the identity map $1_{\mathbf{Z}_n}$ on $\mathbf{Z}_n$.

Proof: The result is immediate from Corollary 9 with r = 2.

Concluding Remarks

In 2007 Winton published the EMO-1 and EMO-2 cryptosystems [10]. Both cryptosystems use a system modulus n = pq, where p and q are distinct primes. Furthermore, the selection of p and q depend on the largest integer L which can represent an encrypted message M. In particular, the decryption processes in both these systems are based on Euler's Theorem. Consequently, the system modulus used in both cases requires that p > L and q > L in order to guarantee that gcd{M,n} = 1. Therefore n = pq > L^2.

However, Corollary 10 allows for significantly smaller values of p and q to satisfy n = pq > L, reducing the size of the system modulus n. Hence the same decryption capability is achieved with greater computational efficiency.

† *Richard Alan Winton*, *Ph.D.*, Tarleton State University, TX, USA

References

1. Burton, D. M., *Elementary Number Theory*, 4th edition, McGraw-Hill, New York, 1998.
2. Burton, D. M., *The History of Mathematics, An Introduction*, 6th edition, McGraw-Hill, Boston, 2007.
3. Dudley, U., *Elementary Number Theory*, 2nd edition, W. H. Freeman and Company, New York, 1978.
4. Eynden, C. V., *Elementary Number Theory*, 2nd edition, Waveland Press, Inc., Long Grove, Illinois, 2001.
5. Koblitz, N., *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 1987.
6. Long, C. T., *Elementary Introduction to Number Theory*, 3rd edition, Prentice-Hall, Inc., New Jersey, 1987.
7. McCoy, N. H., *The Theory of Numbers*, Macmillan Company, New York, 1965.
8. Niven, I. and Zuckerman, H. S., *An Introduction to the Theory of Numbers*, 3rd edition, John Wiley and Sons, Inc., New York, 1972.
9. Rademacher, H., *Lectures on Elementary Number Theory*, Blaisdell Publishing Company, New York, 1964.
10. Winton, R. A., *Enhancing the Massey-Omura Cryptosystem*, Journal of Mathematical Sciences and Mathematics Education, Vol. 2, No. 1, (2007) pp. 21-29.