7-1-2001

The totient function of composite integers. N= pq.

Nelson A. Carella

SCHOOL OF COMPUTER SCIENCE AND INFORMATION SYSTEMS

TECHNICAL REPORT

Number 165, July 2001

The Totient Function of Composite Integers $n = pq$

Nelson A. Carella

PACE UNIVERSITY

The present manuscript is currently under review for publication by the Journal of Cryptography. It is the first part of a larger study.

Nelson A. Carella, a mathematician who hails from the City University of New York, adjuncts in the Information Systems Department at Pace University in Manhattan. Most recently he has taught Data Communications.

The Totient Function of Composite Integers $n = pq$

Nelson A. Carella

Abstract: In this paper it will be shown that the totient $\varphi(n)$ can be evaluated in terms of divisor function $\sigma_s(n)$, the counting function $r_s(n)$, and the modular form $G_s(\tau)$. These results lead to several analytical, and number theoretical algorithms for computing the values of the function $\varphi(n)$ at composite arguments $n = pq$, p, q primes. These techniques provide potential new tools for the factorization of $n = pq$, and the analysis of cryptosystems based on the ring of integers $\mathbf{Z}_n$.

1 Introduction

In the last decades very extensive research and resources has been devoted to the factorization of large integers of the form $n = pq$, and the equivalent problem of determining the values of $\varphi(n)$. These efforts have resulted in a variety of factorization algorithms, but no effective solution yet. Several elementary methods of transforming this problem into different problems will be considered in this paper. Some of the techniques considered here are of theoretical interest and probably are not practical.

Each of the remaining sections will treat a different technique of dealing with this problem.

2 The Number Theoretical Formulae

The divisor function is the usual $\sigma_s(n) = \sum_{d|n} d^s$. The recursive formula

$$\sigma(n) = \begin{cases} \dfrac{(-1)^{d+1} d(d+1)(2d+1)}{6} + \sum_{k\geq 1} (-1)^{k+1}(2k+1)\sigma(n-k(k+1)/2), & \text{if } n = d(d+1)/2, \\ \sum_{k\geq 1} (-1)^{k+1}(2k+1)\sigma(n-k(k+1)/2), & \text{if } n \neq d(d+1)/2, \end{cases} \tag{1}$$

can be used to determine $\sigma(n) = \sigma_1(n)$. A profusion of other identities for computing $\sigma_s(n)$, recursively, or in terms of other divisors functions are also available in the literature. Some recent convolution identities are given in [ML].

The counting function $r_s(n)$ enumerates all the integer solutions $x_s, \ldots, x_2, x_1$ of the quadratic form $x_1^2 + x_2^2 + \cdots + x_s^2 = n$. The function $r_s(n)$ can be written in term of divisor functions and other functions. For the parameters $s = 2, 4, 6$, and 8, the two functions $r_s(n)$ and $\sigma_s(n)$ have a simple linear relationship:

$$r_2(n) = 4\sum_{d|n} (-1)^{(d-1)/2}, \qquad r_4(n) = 8[2 + (-1)^n] \sum_{\text{odd } d|n} d, \tag{2}$$

$$r_6(n) = 4\sum_{d|n}(-1)^{(d-1)/2}\left(\left(\frac{4n}{d}\right)-d^2\right), \qquad r_8(n) = 16\sum_{d|n}(-1)^{n-d}d^3.$$

These are given in [GR, p.121], and [IW, p.187], see also [RA, p.372]. In general, the function $r_{2s}(n) = \delta_{2s}(n) + e_{2s}(n)$, where $\delta_{2s}(n)$ consists of divisor functions and $e_{2s}(n)$ is a function of lower order. The exact formulae for $2s \le 32$, appears in Acta Arith. LIV (1989), pp. 9-36, and other sources in the literature. Recently infinite sequences of formulae have been determined for $s = 4k^2$ or $4k(k + 1)$, $k \ge 1$, see [MN]. The function $r_s(n)$ can be computed via the convolution and the quadratic step recursion formulae

$$r_s(n) = \sum_{k=0}^{n} r_{s-a}(k)r_a(n-k) \quad \text{and} \quad r_s(n) = 2\sum_{k=1}^{\sqrt{n}}\left(\frac{s+1}{n}k^2 - 1\right)r_s(n-k^2), \tag{3}$$

respectively. In general, the kth-step recursion

$$r_{k,s}(n) = 2\sum_{l=1}^{n^{1/k}}\left(\frac{s+1}{n}l^k - 1\right)r_{k,s}(n-l^k) \tag{4}$$

can be utilized to compute number $r_{k,s}(n)$ of vectors solutions $x_s, \ldots, x_2, x_1$ of the k-form $x_1^k + x_2^k + \cdots + x_s^k = n$ in the integers lattice $\mathbf{Z}^s$, see [NT, p.426]. The dimension $s = g(k)$ of the integers lattice is the smallest s such that every integer $n \ge 0$ can be expressed as a sum of s kth powers (Waring's problem). This is given by $g(k) = 2^k + [(3/2)^k] - 2$, if $3^k = 2^k q + r$, and $q + r \le 2^k$. The values $g(2) = 4$, $g(3) = 9$, $g(4) = 19$, and $g(5) = 37$ are well known.

The number theoretical formulae allow the construction of polynomial relationships between the functions $r_s(n)$, $\sigma_s(n)$, and $\varphi(n)$.

***Lemma* 1.** Let $n = pq$, and $s \ge 1$. Then

$$\varphi(n)^s + a_{s-1}\varphi(n)^{s-1} + \cdots + a_1\varphi(n) + a_0 + \sigma_s(n) = 0, \tag{5}$$

where the coefficients $a_i = a_i(n)$ are polynomials in n. In Particular,

$$(1)\ \varphi(n) = 2(n + 1) - \sigma(n), \tag{6}$$

(2) $\varphi(n) = 2(n + 1) - 2^{-3}r_4(n)$,

(3) $$\varphi(n)^2 - 2(n+1)\varphi(n) + n^2+1 = \begin{cases} 12^{-1}r_6(n) - n^2 - 1 & \text{if } p,q \equiv 1 \bmod 4, \\ n^2 + 1 - 12^{-1}r_6(n) & \text{if } p,q \equiv 3 \bmod 4, \end{cases}$$

(4) $\varphi(n)^3 - 3(n+1)\varphi(n)^2 + 3(n^2+n+1)\varphi(n) - (n + 1)^3 - n^3 - 1 + \sigma_3(n) = 0$,

(5) $\varphi(n)^3 - 3(n+1)\varphi(n)^2 + 3(n^2+n+1)\varphi(n) - (n + 1)^3 - n^3 - 1 + 2^{-4}r_8(n) = 0$.

The new identities immediately lead to new algorithms for computing $\varphi(n)$ recursively, and eventually factoring $n = pq$, at least in theory. Two of these algorithms are given by

$$\varphi(n) = 2(n+1) - \frac{1}{4}\sum_{k=1}^{\sqrt{n}}\left(\frac{5}{n}k^2 - 1\right) r_4(n-k^2), \tag{7}$$

and

$$\varphi(n) = 2(n+1) - \tag{8}$$
$$\begin{cases} \frac{(-1)^{d+1}d(d+1)(2d+1)}{6} + \sum_{k\geq 1}(-1)^{k+1}(2k+1)\sigma(n-k(k+1)/2), & \text{if } n = d(d+1)/2, \\ \sum_{k\geq 1}(-1)^{k+1}(2k+1)\sigma(n-k(k+1)/2), & \text{if } n \neq d(d+1)/2. \end{cases}$$

Although these algorithms are not efficient, it is conceivable that the sequences of numbers $r_4(n-1)$, $r_4(n-4)$, $r_4(n-9)$, $r_4(n-16)$, ..., or $\sigma(n-1)$, $\sigma(n-3)$, $\sigma(n-6)$, $\sigma(n-10)$, ... are easily computable for certain n. A recursive formula for $\sigma(n)$ slightly more efficient than the one employed above is given in [EW].

3 The Analytic Formulae

The change of variable map $\tau \to q = e^{i2\pi\tau}$ appearing in the various equations below identifies the complex upper half plane $\Im = \{ \tau = x + iy : y > 0 \}$ with the open unit disk $D(0,1) = \{ |q| < 1 : q \in \Im \}$.

The divisor function $\sigma_s(n)$ has a power series expansion of the form

$$\sigma_{1-s}(n) = \zeta(s)\sum_{k=1}^{\infty}\frac{c_k(n)}{k^s}, \quad (\Re e(s) > 1), \tag{9}$$

where the kth coefficient is the Ramanujan's sum

$$c_k(n) = \sum_{\gcd(x,k)} e^{i2\pi n x/k} = \sum_{d|k,d|n} d\mu(k/d), \tag{10}$$

see [HR, pp. 140-142]. Further, the kth coefficient $c_k(n) = \mu(k)$ for all $k < p < q$.

The theta function and the sth power of it are defined by the power series

$$\theta(\tau) = \sum_{k=0}^{\infty} q^{k^2} = \sum_{k=0}^{\infty} r_2(k)q^k \quad \text{and} \quad \theta^s(\tau) = \sum_{k=0}^{\infty} r_{2s}(k)q^k. \tag{11}$$

The kth coefficient of the Fourier series expansion of the sth power of the theta function is precisely the number of representations of k as a sum of $2s$ squares. Further, the functional equations $\theta(\tau)=\theta(\tau+2)$, and $\theta^4(-1/\tau)=\tau^2\theta^4(\tau)$ classify it as an automorphic form of weight 1/2 and level 2.

The modular form of weight $2s$ is defined by

$$G_{2s}(\tau)=\sum_{(u,v)\neq(0,0)}\frac{1}{(u\tau+v)^{2s}}, \tag{12}$$

see [AP, p. 69], [CH, p. 83] or similar text. Further, the summation formula below provides a rapidly convergent power series.

***Lemma* 2.** Let $\tau=x+iy:y>0$, and $s>1$. Then

$$\frac{1}{2^s}\sum_{-\infty=v}^{\infty}\frac{1}{(\tau+v)^s}=\frac{\pi^s e^{-i\pi s/2}}{\Gamma(s)}\sum_{k=1}^{\infty}k^{s-1}e^{i2\pi k\tau}. \tag{13}$$

The proof of this result appears in [KN, p. 65]. After some algebraic manipulations, this function can be rewritten in two different ways as power series:

$$G_{2s}(\tau)=2\zeta(2s)+2\frac{(i2\pi)^{2s}}{(2s-1)!}\sum_{k=1}^{\infty}\sigma_{2s-1}(k)q^k=2\zeta(2s)+2\frac{(-1)^s(2\pi)^{2s}}{(2s-1)!}\sum_{u\geq1}\sum_{k=1}^{\infty}k^{2s-1}e^{i2\pi ku\tau}. \tag{14}$$

The analytical formulae bring the representation of $\varphi(n)$ into the realm of modular forms and theta functions.

***Theorem* 3.** Let $n=pq$, and $s\geq1$. Then

$$\text{(1)}\ \sum_{i=0}^{2s-1}a_i\varphi(n)^i=\frac{(2s-1)!}{2(i2\pi)^{2s}}\int_{|q|=r}\sum_{(u,v)\neq(0,0)}\frac{1}{(u\tau+v)^{2s}}\frac{dq}{q^n}, \tag{15}$$

$$\text{(2)}\ \sum_{i=0}^{s-1}a_i\varphi(n)^i=\zeta(s)\sum_{k=1}^{\infty}\frac{c_k(n)}{k^s},$$

where $a_i\in\mathbf{Z}$, $q=e^{i2\pi\tau}$, and $Im(\tau)>0$. In particular,

$$\text{(3)}\ \varphi(n)^3-3(n+1)\varphi(n)^2+3(n^2+n+1)\varphi(n)-(n+1)^3-n^3-1=\frac{-3}{16\pi^4}\int_{|q|=r}\sum_{(u,v)\neq(0,0)}\frac{1}{(u\tau+v)^4}\frac{dq}{q^n},$$

$$\text{(4)}\ \varphi(n)^3-3(n+1)\varphi(n)^2+3(n^2+n+1)\varphi(n)-(n+1)^3-n^3-1=-n^3\zeta(4)\sum_{k=1}^{\infty}\frac{c_k(n)}{k^4},$$

Proof of (1): Since the constant functions are analytic on the open disk $D(0,r) = \{ \mid q \mid < r \}, r > 0$, the integral of the modular form $G_{2s}(\tau)$ times the local uniformizer q^{-n} reduces to the right side of the equation. ■

The elliptic function $\wp$ will be utilized to derive a result in the next proposition. This function is defined by

$$(z) = \frac{1}{z^2} + \sum_{0 \neq \omega \in L} \frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \tag{16}$$

The index set in the summation is the lattice $L = \{ \omega = \omega_1 n + \omega_2 m \}$, $\tau = \omega_2/\omega_1$, a lattice is an additive subgroup of the complex numbers, see [AP, p. 10], [CH, p. 85] or a similar source.

***Theorem* 4.** If $n = pq$ then the followings are equivalent.

$$(1)\ \varphi(n) = 2(n+1) - \frac{\pi^2 n}{6} \sum_{k=1}^{\infty} \frac{c_k(n)}{k^2}. \tag{17}$$

$$(2)\ \varphi(n) = 2(n+1) - \frac{1}{8} \int_{|q|=r} \theta^4(\tau) \frac{dq}{q^n}.$$

$$(3)\ \varphi(n) = 2(n+1) + \frac{\omega_1^2}{2\pi^2} \int_{|q|=r} \wp\left(\frac{\omega_1(1+\tau)}{2}\right) \frac{dq}{q^n}.$$

Proof of (3): The theta function satisfies the identity $e_1 - e_3 = \left(\frac{\pi}{2\omega_1}\right)^2 \theta^4(\tau)$, where the terms $e_1 = \wp\left(\frac{\omega_1}{2}\right)$, $e_2 = \wp\left(\frac{\omega_2}{2}\right)$, and $e_3 = \wp\left(\frac{\omega_1+\omega_2}{2}\right)$ are the roots of the cubic differential equation $\wp'^2(z) = 4\wp^3(z) - g_2\wp(z) - g_3$. Now observe that for a fixed real ω_1, the root $e_1(\omega_1)$ is constant and the corresponding integral vanishes. ■

References:

[AP] A Apostol, Modular Functions and Dirichlet Series in Number theory, GTM 41, Springer-Velag, NY 1990.
[CH] K Chandrasekharan, Elliptic Functions, Springer-Verlag, NY, 1985.
[EW] JA Ewell, *Recursive Determination Of The Sum Of Divisors Function*, Proc. Amer. Math,. Soc. Vol. 73, No. 2 (1979), pp. 169–172.
[GR] E Grosswald, Representations of Integers as Sums of Squares, Springer-Verlag, NY, 1985.
[HR] GH Hardy, Ramanujan: Twelve Lectures On Subjects Suggested By His Life And Works, Cambridge Press, 1990.
[IW] H Iwanec, Topics In Classical Automorphic Forms, GSM Volume 17, AMS 1997.
[KA] Knapp, Elliptic Curves, Princeton Press, 1989.
[KN] MI Knopp, Modular Functions in Analytic Number Theory, Chelsea Publishing Co, NY 1993.
[ML] G Melfi, *On Some Modular Identities*, Number Theory, deGruyer, 1998, p. 371-382.
[MN] SC Milne, New infinite families of exact sums of squares formulas, Jacobi elliptic functions, and Ramanujan's tau function, Proc. National Academy of Sciences, 93 (1996) pp. 15004-15008.
[RA] H Rademacher, Topics in Analyctic Number Theory, Springer-Verlag, NY, 1985.
[RN] RA Rankin, *Sums of Squares: An Elementary Method*, Number Theory Series, RP Bambah et al. Editors, Birkhauser, pp.371-399, 2000.