NNTDM 4 (1998) 3, 93-100

NAGELL'S TOTIENT REVISITED

Pentti Haukkanen[1] and R. Sivaramakrishnan[2]
[1] Department of Mathematical Sciences, University of Tampere, P.O.Box 607, FIN-33101 Tampere, Finland
[2] Department of Studies in Mathematics, Mangalore University, Dk 574199, India

ABSTRACT: Nagell's totient $\theta(n,r)$ counts the number of solutions of the congruence $(*)$ $n \equiv x+y \pmod r$ under the restriction $(x,r)=(y,r)=1$. In this paper we evaluate the number $\theta(n,r,q)$ of solutions of the congruence $(*)$ under the restriction $(x,r)=(y,r)=q$, where $q|r$, via Ramanathan's approach to class-division of integers $\pmod r$.

1 Introduction

Paul J. McCarthy [5, 6] has made an interesting study of obtaining the number of solutions of the linear congruence

$$n \equiv x_1 + x_2 + \cdots + x_s \pmod r \tag{1.1}$$

under various specified restrictions on x_i, $i=1,2,\ldots,s$. Here, r denotes a positive integer and n is any integer.

If $N(n,r,s)$ denotes the number of solutions of (1.1) under the restriction $(x_i,r)=1$, $i=1,2,\ldots,s$ ((x_i,r) denotes the g.c.d of x_i and r), it is known [3] that

$$N(n,r,s) = \frac{1}{r}\sum_{d|r} c\Big(\frac{r}{d}, r\Big)^s c(n,d). \tag{1.2}$$

The function $c(n,r)$ is the trigonometric sum due to Ramanujan given by

$$c(n,r) = \sum_{\substack{h \pmod r \\ (h,r)=1}} \exp\Big(\frac{2\pi inh}{r}\Big). \tag{1.3}$$

The expression for $N(n,r,s)$ given in (1.2) has also been obtained by K. G. Ramanathan [9], C. A. Nicol and H. S. Vandiver [8] and David Rearick [10]. The simplified expression for $N(n,r,s)$ is given by

$$N(n,r,s) = r^{s-1}\prod_{p|(n,r)} \frac{(p-1)\{(p-1)^{s-1}-(-1)^{s-1}\}}{p^s} \prod_{\substack{p|r \\ p\nmid n}} \frac{(p-1)^s-(-1)^s}{p^s}, \tag{1.4}$$

where p is a prime with the specified property. The form of $N(n,r,s)$ given in (1.4) is due to H. Rademacher. See [5].

The evaluation of $N(n,r,2)$, the case $s=2$ of (1.2), is due to T. Nagell [7]. It is easy to note from (1.4) that $N(n,r,2)$ referred to as Nagell's totient is given by

$$N(n,r,2) = r \prod_{p|(n,r)} \Big(1-\frac{1}{p}\Big) \prod_{p|r, p\nmid n} \Big(1-\frac{2}{p}\Big). \tag{1.5}$$

We attempt a generalization of $N(n,r,2)$ in the following manner. We consider the number of solutions of the congruence

$$n \equiv x+y \pmod{r} \tag{1.6}$$

under the restriction $(x,r)=(y,r)=q$, where q is an arbitrary but fixed divisor of r. The number of solutions of (1.6) with $(x,r)=(y,r)=q$ is denoted by $\theta(n,r,q)$.

When $(x,r)=(y,r)=q$, writing $x=qx'$, $y=qy'$ we get

$$n \equiv qx' + qy' \pmod{r} \tag{1.7}$$

under the restriction $(x',\frac{r}{q})=(y',\frac{r}{q})=1$. It is easy to see that if $q \nmid n$, then $\theta(n,r,q)=0$. We also note that

$$\theta(n,r,q) = N\Big(\frac{n}{q},\frac{r}{q},2\Big) \quad \text{if } q \mid n. \tag{1.8}$$

So, from (1.5), we obtain the evaluation of $\theta(n,r,q)$ in the case where $q \mid n$. When $q=r$, we note that $\theta(n,r,r)>0$ if and only if $r \mid n$. Really, $\theta(n,r,r)=1$ and $x=y=0$ is the only solution.

The purpose of this note is to evaluate $\theta(n,r,q)$ in closed form via Ramanathan's [9] approach to class-division of integers $\pmod{r}$, see Theorem 3.2. We also evaluate $\theta(n,r,q)$ in terms of Euler's and Alder's [11, Section V.6] totient functions, see Theorem 4.1.

2 Preliminaries

An arithmetic function f of two variables n, r denoted by $f(n,r)$ is said to be periodic $\pmod{r}$ if $f(n+r,r)=f(n,r)$, where r is fixed and ≥ 1 (see [1]). An arithmetic function $f(n,r)$ is called an even function $\pmod{r}$ if $f(n,r)=f((n,r),r)$ (see [6, 11]). It is clear that every even function $\pmod{r}$ is periodic $\pmod{r}$. Ramanujan's sum $c(n,r)$ (1.3) is an interesting example of an even function $\pmod{r}$. Further,

$$c(n,r) = \sum_{d|(n,r)} \mu\Big(\frac{r}{d}\Big) d, \tag{2.1}$$

where μ is the Möbius function given by

$$\mu(r) = \begin{cases} 1 & r=1, \\ (-1)^t & \text{if } r=p_1p_2\cdots p_t;\ p_i \text{ being distinct primes}, \\ 0 & \text{if } a^2 \mid r,\ a>1. \end{cases} \tag{2.2}$$

Clearly $c(0,r)=\phi(r)$, the Euler ϕ-function. The Hölder relation for $c(n,r)$ is given by

$$c(n,r) = \frac{\mu(\delta)\phi(r)}{\phi(\delta)}, \quad \delta = \frac{r}{(n,r)}. \tag{2.3}$$

Let $e_r(n)$ denote $\exp(2\pi i n/r)$.

Lemma 2.1 Given r complex numbers $w_0, w_1, \ldots, w_{r-1}$, there exist r uniquely determined complex numbers $a_0, a_1, \ldots, a_{r-1}$ such that

$$w_n = \sum_{m=0}^{r-1} a_m e_r(nm), \quad n = 0, 1, 2, \ldots, r-1. \tag{2.4}$$

Moreover, the coefficients a_n are given by

$$a_n = \frac{1}{r} \sum_{m=0}^{r-1} w_m e_r(-nm), \quad n = 0, 1, 2, \ldots, r-1. \tag{2.5}$$

For proof, see Theorem 8.3 in [1]. From Lemma 2.1 we deduce

Lemma 2.2 Let f, g be periodic functions $\pmod r$. If

$$g(n, r) = \sum_{m=0}^{r-1} f(m, r) e_r(nm), \tag{2.6}$$

then

$$f(n, r) = \frac{1}{r} \sum_{m=0}^{r-1} g(m, r) e_r(-nm). \tag{2.7}$$

For proof, see Theorem 8.4 in [1]. The equivalent form of Lemma 2.2 for even functions $\pmod r$ in terms of Ramanujan sums $c(n, r)$ is stated in

Lemma 2.3 Let f, g be even functions $\pmod r$. If

$$g(n, r) = \sum_{d|r} f\Big(\frac{r}{d}, r\Big) c(n, d), \tag{2.8}$$

then

$$f(n, r) = \frac{1}{r} \sum_{d|r} g\Big(\frac{r}{d}, r\Big) c(n, d). \tag{2.9}$$

Proof of Lemma 2.3 using the orthogonality relation for $c(n, r)$ is given in [3].

Lemma 2.4 Let f be a periodic function $\pmod r$ and let g be an even function $\pmod r$ such that (2.6) holds. Then f is an even function $\pmod r$ and g, f possess the relations (2.8) and (2.9) respectively.

Lemma 2.4 can be deduced using Lemma C of K. G. Ramanathan [9].

3 Class-division of integers $\pmod r$

We now proceed to the class-division of integers $\pmod r$. Let $t_1 (= 1), t_2, \ldots, t_s (= r)$ be the distinct divisors of n, where $s = d(r)$, the number of divisors of r. The integers through r fall into s mutually disjoint classes

$$C_1, C_2, \ldots, C_s,$$

where

$$C_i = \{x : 1 \le x \le r, \quad (x, r) = t_i\}. \tag{3.1}$$

Suppose that

$$C_i = \{y_{1i}, y_{2i}, \ldots, y_{ui}\}, \quad \text{where } ui = \phi\Big(\frac{r}{t_i}\Big) \tag{3.2}$$

and

$$C_j = \{y_{1j}, y_{2j}, \ldots, y_{u'j}\}, \quad \text{where } u'j = \phi\Big(\frac{r}{t_j}\Big). \tag{3.3}$$

Addition of C_i and C_j denoted by $C_i \oplus C_j$ is possible, where $C_i \oplus C_j$ is the set of numbers obtained by adding $\pmod r$ each number of C_i to each number of C_j. It is known that in $C_i \oplus C_j$ elements of a class C_k occur the same number $M(i,j,k)$ of times, see R. Vaidyanathaswamy [12]. For a concrete example, see [11, Chapter XV] or [12]. The coefficients $M(i,j,k)$ can be evaluated in terms of Ramanujan sums, see K. G. Ramanathan [9]. These results are given in the following theorem. The proof is adapted from that given in [9].

Theorem 3.1 *If C_i and C_j are two classes* $\pmod r$, *then*

$$C_i \oplus C_j = \sum_{k=1}^{s} M(i,j,k) C_k, \tag{3.4}$$

where

$$M(i,j,k) = \frac{1}{r} \sum_{d|r} c\Big(d, \frac{r}{t_i}\Big) c\Big(d, \frac{r}{t_j}\Big) c\Big(t_k, \frac{r}{d}\Big). \tag{3.5}$$

Proof Using elements of C_i (3.2) and C_j (3.3), we form the product

$$\left(\sum_{h=1}^{u} e_r(n y_{hi})\right) \left(\sum_{l=1}^{u'} e_r(n y_{lj})\right). \tag{3.6}$$

If $f(m,r)$ denotes the number of ways of expressing m as the sum

$$y_{vi} + y_{wj} \pmod r,$$

where $y_{vi} \in C_i$, $y_{wj} \in C_j$, we can write the product in (3.6) as

$$\sum_{m=0}^{r-1} f(m,r) e_r(nm). \tag{3.7}$$

But every element of C_i has g.c.d t_i with r. Therefore,

$$\sum_{h=1}^{u} e_r(n y_{hi}) = c\Big(n, \frac{r}{t_i}\Big)$$

and, similarly,

$$\sum_{l=1}^{u'} e_r(n y_{lj}) = c\Big(n, \frac{r}{t_j}\Big).$$

Thus, from (3.6) and (3.7), we have

$$c\Big(n, \frac{r}{t_i}\Big) c\Big(n, \frac{r}{t_j}\Big) = \sum_{m=0}^{r-1} f(m,r) e_r(nm). \tag{3.8}$$

But, the left-hand side of (3.8) is even $\pmod r$, f is periodic $\pmod r$ and (3.8) is compared with (2.6). Then, by virtue of Lemma 2.4, $f(n,r)$ is even $\pmod r$, and utilizing (2.8) and (2.9), we get

$$c\Big(n,\frac{r}{t_i}\Big)c\Big(n,\frac{r}{t_j}\Big)=\sum_{d|r} f(d,r)c\Big(n,\frac{r}{d}\Big) \tag{3.9}$$

or

$$f(n,r)=\frac{1}{r}\sum_{d|r} c\Big(d,\frac{r}{t_i}\Big)c\Big(d,\frac{r}{t_j}\Big)c\Big(n,\frac{r}{d}\Big). \tag{3.10}$$

Therefore, by the definition of $f(n,r)$, (3.4) holds with $M(i,j,k)=f(t_k,r)$. Taking $n=t_k$ in (3.10), we obtain the evaluation of $M(i,j,k)$ as given in (3.5). This completes the proof of Theorem 3.1. □

Remark 1 We observe that $\theta(n,r,q)$ is the value of $M(i,j,k)$ (3.5) when $t_i=t_j=q$ and $t_k=(n,r)$, or the value of $f(n,r)$ (3.10) with $t_i=t_j=q$.

We now give the evaluation of $\theta(n,r,q)$ obtained via Ramanathan's approach to class-division of integers $\pmod r$.

Theorem 3.2 *The expression for* $\theta(n,r,q)$ *is given by*

$$\theta(n,r,q)=\frac{1}{r}\sum_{d|r} c^2\Big(\frac{r}{d},\frac{r}{q}\Big)c(n,d). \tag{3.11}$$

Proof follows from Remark 1.

Remark 2 One could also obtain (3.11) considering the congruence (1.6) under the restriction $(x,r)\in S_1$, $(y,r)\in S_2$ and applying the Cauchy product of even functions $\pmod r$, where S_1 and S_2 are subsets of the set of positive integers. We do not apply this method here, as the object of this paper is to evaluate $\theta(n,r,q)$ via Ramanathan's approach [9] to class-division of integers $\pmod r$. For application of this method, see [4, 6].

4 The evaluation of $\theta(n,r,q)$ in terms of Euler's and Alder's totients

Euler's totient $\phi(r)$ is the number of integers $a \pmod r$ such that $(a,r)=1$, see also §2. It is well known that

$$\phi(r)=r\prod_{p|r}\Big(1-\frac{1}{p}\Big). \tag{4.1}$$

We denote by $\phi_2(r)$ the number of integers $a \pmod r$ such that $(a,r)=(a+1,r)=1$. The function ϕ_2 is a special case of Alder's totient. It is known that

$$\phi_2(r)=r\prod_{p|r}\Big(1-\frac{2}{p}\Big). \tag{4.2}$$

The derivation of (4.2) is shown in [11].

The function $\theta(n,r,q)$ is a multiplicative function in the sense that if $(r,r')=1$, $q\mid r$, $q'\mid r'$, then $(qr,q'r')=1$ and

$$\theta(n,r,q)\theta(n,r',q')=\theta(n,rr',qq'). \tag{4.3}$$

We see that it suffices to evaluate $\theta(n,p^a,p^b)$, where p is a prime and $a \geq b$. In evaluation of $\theta(n,p^a,p^b)$ we use the expression for $\theta(n,r,q)$ given in (3.11) in the form

$$\theta(n,r,q) = \frac{\phi^2(\frac{r}{q})}{r} \sum_{d|r} \frac{\mu^2(\frac{d}{(q,d)})}{\phi^2(\frac{d}{(q,d)})} c(n,d), \tag{4.4}$$

which comes out using (2.3). We also use the concept of a unitary divisor of r which is defined as a divisor δ for which $(\delta, r/\delta) = 1$.

We recall that $\theta(n,r,q)$ vanishes whenever q does not divide n. Therefore, it suffices to evaluate $\theta(n,r,q)$ when $q \mid r$ and $q \mid n$. We now obtain the evaluation of $\theta(n,r,q)$ in the following manner.

Notation We write $r = r_1 r_2$, where r_1 is the greatest unitary divisor of r containing precisely those prime factors which are common to r and n. Then r_2 is the greatest unitary divisor of r such that $(r_2, n) = 1$. We write $q = q_1 q_2$, where q_1 is the greatest unitary divisor of q such that no prime factor of q_1 occurs to the same power as that in n. Then q_2 is the greatest common unitary divisor of q and n. Note that q_2 is such that every prime factor of q_2 occurs to the same power as that in n and $(q_2, n/q_2) = 1$. We write $r_1 = s_1 s_2$, where s_1 is the greatest unitary divisor of r_1 such that $(s_1, q_2) = 1$ and s_2, q_2 contain the same distinct prime factors. Note that $(r_1, r_2) = (q_1, q_2) = (s_1, s_2) = 1$.

Theorem 4.1 *With the above notation, one has*

$$\theta(n,r,q) = \phi\Big(\frac{s_1}{q_1}\Big)\phi_2\Big(\frac{r_2 s_2}{q_2}\Big). \tag{4.5}$$

Proof By virtue of (4.3) we have

$$\begin{aligned} \theta(n,r,q) &= \theta(n,r_1,q)\theta(n,r_2,1) \\ &= \theta(n,s_1,q_1)\theta(n,s_2,q_2)\theta(n,r_2,1). \end{aligned} \tag{4.6}$$

Since $(r_2, n) = 1$, we obtain

$$\theta(n,r_2,1) = N(n,r_2,2) = \phi_2(r_2), \tag{4.7}$$

see (1.5) and (4.2). Again, by virtue of (4.3), it suffices to evaluate $\theta(n,s_1,q_1)$ and $\theta(n,s_2,q_2)$ when the arguments are prime powers. The evaluations are given in Cases (i) and (ii).

Case (i). Let $s_1 = p^a$, $q_1 = p^b$ and $n = p^c$. Then $a \geq b \geq 0$ and $c > b$. If $a > b$, then using (4.4)

$$\begin{aligned} \theta(p^c,p^a,p^b) &= \frac{\phi^2(p^{a-b})}{p^a}\Big\{1 + \phi(p) + \cdots + \phi(p^b) + \frac{\phi(p^{b+1})}{\phi^2(p)}\Big\} \\ &= \frac{\phi^2(p^{a-b})}{p^{a-b}}\Big(1 + \frac{1}{\phi(p)}\Big) \end{aligned}$$

or

$$\theta(p^c,p^a,p^b) = \phi(p^{a-b}). \tag{4.8}$$

Also, if $a = b$, (4.8) holds. Since ϕ is multiplicative,

$$\theta(n,s_1,q_1) = \phi\Big(\frac{s_1}{q_1}\Big). \tag{4.9}$$

Case (ii). Let $s_2 = p^a$, $q_2 = p^b$ and $n = p^c$. Then $a \geq b \geq 1$ and $c = b$. If $a > b$, then using (4.4)

$$\begin{aligned} \theta(p^c, p^a, p^b) &= \frac{\phi^2(p^{a-b})}{p^a}\Big\{1 + \phi(p) + \cdots + \phi(p^b) - \frac{p^b}{\phi^2(p)}\Big\} \\ &= \frac{\phi^2(p^{a-b})}{p^{a-b}}\Big(1 - \frac{1}{\phi^2(p)}\Big) = p^{a-b}\Big(1 - \frac{2}{p}\Big) \end{aligned}$$

or

$$\theta(p^c, p^a, p^b) = \phi_2(p^{a-b}). \tag{4.10}$$

Also, if $a = b$, (4.10) holds. Since ϕ_2 is multiplicative,

$$\theta(n, s_2, q_2) = \phi_2\Big(\frac{s_2}{q_2}\Big). \tag{4.11}$$

We note that Cases (i) and (ii) could also be treated with the aid of (1.5) and (1.8). Since we are dealing with class-division of integers $\pmod r$ in this paper, we prefer the use of (4.4).

Now, from (4.6), (4.7), (4.9) and (4.11), we obtain

$$\theta(n, r, q) = \phi\Big(\frac{s_1}{q_1}\Big)\phi_2\Big(\frac{s_1}{q_1}\Big)\phi_2(r_2).$$

Since ϕ_2 is multiplicative, the expression for $\theta(n, r, q)$ is as shown in (4.5). This completes the proof of Theorem 4.1. □

Remark 3 For a discussion of solutions of linear congruency (1.1) in a general setting with application to matrices, see Umberto Cerruti [2].

The authors are grateful to Professor Andrew Granville for valuable comments which improved the original version of the manuscript.

References

[1] Tom M. Apostol: Introduction to Analytic Number Theory, Springer-Verlag UTM (1976).

[2] Umberto Cerruti: Computing the number of restricted solutions of linear congruences by using generalized Ramanujan sums and matrices (Extended Abstract) (1996).

[3] Eckford Cohen: A class of arithmetical functions, Proc. Nat. Acad. Sci. (USA) 41 (1955), 939–944.

[4] P. Haukkanen and Paul J. McCarthy: Sums of values of even functions, Portugal. Math. 48 (1991), 53–66.

[5] Paul J. McCarthy: Counting restricted solutions of a linear congruence, Nieuw Arch. Wisk. (3) XXV (1977), 133–147.

[6] Paul J. McCarthy: Introduction to Arithmetical Functions, Springer-Verlag Universitext (1986).

[7] T. Nagell: Verallgemeinerung eines Satzes von Schemmel, Skr. Norske Vod. Akad. Oslo (Math. Class) I, No. 13 (1923), 23–25.

[8] C. A. Nicol and H. S. Vandiver: A von Sterneck arithmetical function and restricted partitions with respect to a modulus, Proc. Nat. Acad. Sci. (USA) 40 (1954), 825–835.

[9] K. G. Ramanathan: Some applications of Ramanujan's trigonometrical sum $C_m(n)$, Proc. Ind. Acad. Sci. (A) 20 (1944), 62–69.

[10] David Rearick: A linear congruence with side conditions, Amer. Math. Monthly 70 (1963), 837–840.

[11] R. Sivaramakrishnan: Classical Theory of Arithmetic Functions, Marcel Dekker: Monographs and Text Books in Pure and Applied Mathematics No. 126 (1989).

[12] R. Vaidyanathaswamy: A remarkable property of integers (mod N) and its bearing on group theory, Proc. Ind. Acad. Sci. Section A (1937), 63–75.