On a Property of the Primitive Roots of Unity Leading to the Evaluation of Ramanujan's Sums

Titu Andreescu and Marian Tetiva

1. Introduction. Ramanujan's sums are the sums of powers with the same exponent of the primitive roots of unity of some order. More specifically, let q and m be positive integers, and let $x_1, \dots, x_n$ (with $n = \varphi(q)$, where φ is Euler's totient function) be the roots of the qth cyclotomic polynomial Φ_q, that is, the primitive roots of unity of order q. We denote by

$$c_q(m) = x_1^m + \cdots + x_n^m = \sum_{1\le j\le q,\ (j,q)=1} \left(\cos\frac{2jm\pi}{q} + i\sin\frac{2jm\pi}{q}\right)$$

and call this expression *Ramanujan's sum.* The formula

$$c_q(m) = \sum_{d|(q,m)} \mu\left(\frac{q}{d}\right) d$$

holds–see [2] for a proof. Here μ is the usual Möbius function defined on positive integers by $\mu(1) = 1$, $\mu(t) = (-1)^k$ when t is a product of k distinct prime factors, and $\mu(t) = 0$ in any other case. The resemblance of the above identity with the well-known expression of φ,

$$\varphi(q) = \sum_{d|q} \mu\left(\frac{q}{d}\right) d$$

is, probably, not just a coincidence, as long as $c_q(m) = \varphi(q)$ whenever $q \mid m$ (it is easy to see that, in that case, $c_q(m) = \sum_{1\le j\le q,\ (j,q)=1} 1 = \varphi(q)$). Thus, Ramanujan's sums generalize Euler's totient function. They also represent a generalization of the Möbius function, because, for $(q,m) = 1$ we have

$$c_q(m) = c_q(1) = x_1 + \cdots + x_n = \mu(q),$$

according to a well-known result about the sum of primitive qth roots of unity, which we will mention again (and we will use) immediately.

Ramanujan expanded the usual arithmetic functions in terms of his sums. Also, Ramanujan's sums were used in the proof of Vinogradov's theorem stating that every sufficiently large odd positive integer is the sum of three primes.

2. The main result. We have seen the formula

$$c_q(m) = \sum_{d|(q,m)} \mu\left(\frac{q}{d}\right) d.$$

Let us denote here $D = (q,m)$, and let q' be such that $q = Dq'$. Then let us rewrite the above equation as

$$c_q(m) = \sum_{d|D} \mu\left(\frac{D}{d}q'\right) d = D\sum_{a|D} \frac{\mu(aq')}{a}.$$

Because the values of the Möbius function for integers that are not square-free are zero, and due to its multiplicativity ($\mu(xy) = \mu(x)\mu(y)$ for relatively prime positive integers x and y) we further have

$$c_q(m) = D \sum_{a|D,\ (a,q')=1} \frac{\mu(a)\mu(q')}{a} = D\mu(q') \sum_{a|D,\ (a,q')=1} \frac{\mu(a)}{a}.$$

Notice that only for a a product of distinct primes we get non-zero terms in this sum (and do not forget $q = Dq'$), so we have

$$c_q(m) = D\mu(q') \prod_{p|q,\, p\nmid q'} \left(1 - \frac{1}{p}\right)$$

where the product is over all primes p that divide q, but do not divide q'. Finally we get

$$c_q(m) = \mu(q') \frac{q \displaystyle\prod_{p|q} \left(1 - \frac{1}{p}\right)}{q' \displaystyle\prod_{p|q'} \left(1 - \frac{1}{p}\right)} = \mu(q') \frac{\varphi(q)}{\varphi(q')},$$

hence we have the following result (that gives a closed form expression for the Ramanujan sums):

Proposition 1. For positive integers q and m we have

$$c_q(m) = \frac{\varphi(q)}{\varphi\left(\dfrac{q}{(m,q)}\right)} \mu\left(\frac{q}{(m,q)}\right).$$

The interested reader can find another proof of proposition 1 (in a more general context) in [2].

3. How do we prove the main result. It is time to see what is the purpose of this note. Namely, we intend to give yet another proof of proposition 1, which avoids the usual calculations with arithmetic functions (and is not very complicated, either). It relies on lemmas 1 and 3 below (lemma 2 helps proving lemma 3).

Lemma 1. Let $x_1, \ldots, x_n$ (with $n = \varphi(q))$) be the qth primitive roots of unity. Then their sum is $x_1 + \cdots + x_n = \mu(q)$.

Proof. This is a well-known property of the primitive roots of unity. In order to prove it, let $f(t)$ be the sum of the primitive roots of unity of order t (for any positive integer t). We then see that

$$\sum_{d|t} f(d)$$

is the sum of *all* roots of unity of order t, that is,

$$\sum_{d|t} f(d) = \begin{cases} 1, & t = 1 \\ 0, & t > 1. \end{cases}$$

However, it is well-known again that

$$\sum_{d|t} \mu(d) = \begin{cases} 1, & t = 1 \\ 0, & t > 1, \end{cases}$$

therefore

$$\sum_{d|t} f(d) = \sum_{d|t} \mu(d),$$

for any positive integer t. We also have $f(1) = \mu(1) = 1$, thus $f(t) = \mu(t)$ follows for any t. Indeed, if the two functions f and μ differ, there exists a minimal $t_0 > 1$ such that $f(t_0) \neq \mu(t_0)$. But then we would also have

$$\sum_{d|t_0} f(d) \neq \sum_{d|t_0} \mu(d),$$

(as $f(d)=\mu(d)$ for $d \mid t_0$, $d<t_0$, while $f(t_0)\neq\mu(t_0)$), a contradiction. It remains that f and μ coincide, thus $x_1+\cdots+x_n=f(q)=\mu(q)$, as desired.

One can note that the result of lemma 1 also represents a particular case of proposition 1 (for relatively prime q and m). Nevertheless, we will use it in our proof for proposition 1.

Lemma 2. Let a, b, and c be positive integers such that a and b are relatively prime. For any positive integer u denote by

$$M_u=\{v\in\{0,1,\dots,u-1\}\mid (v,u)=1\}.$$

Then the numbers at with $t\in M_{bc}$ leave when divided by b all possible remainders from M_b, and each such remainder is obtained the same number of times, that is, each remainder from M_b appears

$$\frac{\varphi(bc)}{\varphi(b)}$$

times when $at \pmod b$ (with $t\in M_{bc}$) are listed.

First proof. Since a is relatively prime to b, for two numbers $t_1,t_2\in M_{bc}$ (actually, for any integers t_1 and t_2) we have that $at_1\equiv at_2 \pmod b$ if and only if $t_1\equiv t_2 \pmod b$. Thus the remainders of the numbers at, $t\in M_{bc}$ appear with the same multiplicities as the remainders leaved by the numbers from M_{bc} themselves–thus it is enough to prove the statement for $a=1$.

That is, we need to prove that the remainders left by the numbers from M_{bc} at division by b can be organized into groups of

$$\frac{\varphi(bc)}{\varphi(b)}$$

equal numbers, and they cover all the remainders from M_b. Any number from M_{bc} is relatively prime to bc, hence it is relatively prime to b, too, consequently the remainder it leaves when divided by b is also relatively prime to b, that is, it belongs to M_b. Also, we note that remainder 1 is surely obtained. Thus if we denote, for any $r\in M_b$, by

$$N_r=\{x\in M_{bc}\mid x\equiv r \pmod b\}$$

we have $N_1\neq\emptyset$ (since $1\in M_{bc}$). Moreover, every N_r is nonempty. Indeed, let $p_1,\dots,p_s$ be the primes that divide c but do not divide b. By the Chinese remainder theorem, the system of congruences

$$x\equiv r \pmod b,\quad x\equiv 1 \pmod{p_i},\quad 1\le i\le s$$

has a solution in the set $\{0,1,\dots,bp_1\cdots p_s-1\}$. Of course $bp_1\cdots p_s\le bc$ and the solution of the system of congruences is relatively prime to any of $b,p_1,\dots,p_s$, hence to bc. Thus this solution is a number from M_{bc} which leaves remainder r when divided by b, and its existence shows that N_r is nonempty.

Now let r be any element from M_b, and let y_0 be one fixed element from N_r. We define the function $f:N_1\to N_r$ by letting $f(x)$ to be the remainder of y_0x at division by bc. Since $f(x)\equiv y_0x \pmod{bc}$, we also have $f(x)\equiv y_0x \pmod b$, and $x\equiv 1 \pmod b$, $y_0\equiv r \pmod b$ imply $f(x)\equiv r \pmod b$. Thus, indeed, $f(x)\in N_r$ and f is well defined. Also, it is clear that f is a bijection, and this shows that N_r and N_1 have the same number of elements, that is every N_r has the same number of the elements. Also, the sets N_r, with $r\in M_b$ partition M_{bc}, hence

$$|N_r|=\frac{|M_{bc}|}{|M_b|}=\frac{\varphi(bc)}{\varphi(b)}$$

for each $r\in M_b$, as we intended to prove.

Second proof. We know now that it is enough to consider the case $a = 1$. Let r be any element from M_b, and let

$$N_r = \{x \in M_{bc} \mid x \equiv r \pmod{b}\},$$

which is obviously the same as

$$N_r = \{r + by \mid y \in \{0, 1, \ldots, c-1\},\ (r + by, bc) = 1\}.$$

Let P be the set of primes that divide c, but do not divide b. For any prime $p \in P$ that divides c, let

$$A_p = \{y \in \{0, 1, \ldots, c-1\} \mid r + by \text{ is divisible by } p\}.$$

We see that an element $r + by$, $y \in \{0, 1, \ldots, c-1\}$ is relatively prime to bc (that is, it belongs to N_r) if and only if there is no prime $p \in P$ such that $p | r + by$. This means that N_r has the same number of elements as the set

$$\{0, 1, \ldots, c-1\} \setminus \left(\bigcup_{p \in P} A_p \right),$$

that is,

$$|N_r| = c - \left| \bigcup_{p \in P} A_p \right|.$$

The cardinality of the union of the A_ps is easily obtained by inclusion-exclusion principle. By noting that for any nonempty subset P' of P we have

$$\left| \bigcap_{p \in P'} A_p \right| = \frac{c}{\prod_{p \in P'} p}$$

we immediately get

$$|N_r| = c \prod_{p \in P} \left(1 - \frac{1}{p}\right),$$

or

$$|N_r| = \frac{bc \prod_{p|bc} \left(1 - \frac{1}{p}\right)}{b \prod_{p|b} \left(1 - \frac{1}{p}\right)} = \frac{\varphi(bc)}{\varphi(b)},$$

as desired.

Lemma 3. Keep the same notations from lemma 1, and let m be a positive integer, let $D = (m, q)$, and $q' = \frac{q}{D}$. Then $x_1^m, \ldots, x_n^m$ can be partitioned into groups consisting of $\frac{\varphi(q)}{\varphi(q')}$ equal values each, the values corresponding to different groups being precisely the primitive q'th roots of unity.

Proof. We will use lemma 2. Note that $x_1, \ldots, x_n$ are actually the numbers

$$\cos \frac{2j\pi}{q} + i \sin \frac{2j\pi}{q},$$

with j running over the set M_q (same notation from lemma 2). Therefore $x_1^m, \ldots, x_n^m$ are

$$\cos \frac{2mj\pi}{q} + i \sin \frac{2mj\pi}{q} = \cos \frac{2m'j\pi}{q'} + i \sin \frac{2m'j\pi}{q'},$$

where, if $D = (m, q)$, we define q' and m' by $q = Dq'$ and $m = Dm'$. Of course, q' and m' are relatively prime. Then lemma 2 (with $a = m'$, $b = q'$ and $c = D$) tells us that the numbers $m'j$, with j running over $M_{Dq'}$ leave, when divided by q', remainders that take every value from $M_{q'}$ precisely

$$\frac{\varphi(Dq')}{\varphi(q')} = \frac{\varphi(q)}{\varphi(q')}$$

times. For $x_1^m, \ldots, x_n^m$ this means that they repeat each value

$$\cos\frac{2r\pi}{q'} + i\sin\frac{2r\pi}{q'},$$

with $r \in M_{q'}$ (that is, every primitive root of unity of order q') precisely

$$\frac{\varphi(q)}{\varphi(q')}$$

times, and that is what we intended to prove.

With these tools in our hands we can now provide another

Proof of Proposition 1. Lemma 2 tells us that the numbers $x_1^m, \ldots, x_n^m$ can be split into k groups of l equal numbers in each group, where

$$k = \varphi(q') = \varphi\left(\frac{q}{(m, q)}\right)$$

and

$$l = \frac{n}{k} = \frac{\varphi(q)}{\varphi\left(\dfrac{q}{(m, q)}\right)}.$$

Thus, the sum $c_q(m)$ actually equals l times the sum of the distinct values among $x_1^m, \ldots, x_n^m$, which is precisely the sum of primitive roots of unity of order $\dfrac{q}{(m, q)}$. As the sum of these roots is $\mu\left(\dfrac{q}{(m, q)}\right)$, by lemma 1, the formula for $c_q(m)$ follows once again.

4. Final remarks: how did we find lemma 3. Surprisingly, maybe, we first came across with the result of lemma 3 (rather than with that from lemma 2) to which we gave the following

Second proof of lemma 3. The order of any of $x_1, \ldots, x_n$ as an element of the multiplicative group of nonzero complex numbers is precisely q; then the order of any of $x_1^m, \ldots, x_n^m$ is $q' = \dfrac{q}{(m, q)}$, so that $x_1^m, \ldots, x_n^m$ are roots of unity of order q'. Each of $x_1, \ldots, x_n$ has the form

$$\cos\frac{2s\pi}{q} + i\sin\frac{2s\pi}{q}$$

where $1 \le s \le q$ and s is relatively prime to q. Thus, if we still denote $m' = \dfrac{m}{D}$, we have any of $x_1^m, \ldots, x_n^m$ of the form

$$\cos\frac{2ms\pi}{q} + i\sin\frac{2ms\pi}{q} = \cos\frac{2m's\pi}{q'} + i\sin\frac{2m's\pi}{q'},$$

where $m's$ and q' are relatively prime. This shows that, in fact, $x_1^m, \ldots, x_n^m$ are *primitive* q'th roots of unity, thus they are roots of $\Phi_{q'}$, which is an irreducible polynomial, hence it is the minimal polynomial of any of $x_1^m, \ldots, x_n^m$.

Now consider the polynomial

$$h = (X - x_1^m) \cdots (X - x_n^m)$$

(which has integer coefficients, by the fundamental theorem of symmetric polynomials) and notice that each irreducible factor of it has to be the minimal polynomial of some x_j^m. But $x_1^m, \dots, x_n^m$ have all the same minimal polynomial, hence any irreducible factor of h is this minimal polynomial, namely $\Phi_{q'}$. As both h and $\Phi_{q'}$ are monic, we have

$$h = (\Phi_{q'})^l$$

for some positive integer l that verifies $n = \varphi(q')l = kl$, if we denote $k = \varphi(q')$. Thus, we have $l = \dfrac{\varphi(q)}{\varphi(q')}$, and

$$(X - x_1^m) \cdots (X - x_n^m) = (\Phi_{q'})^{\frac{\varphi(q)}{\varphi(q')}}.$$

It is clear now that, if $y_1, \dots, y_k$ are the (distinct) roots of $\Phi_{q'}$, then (after an appropriate indexation) we have $x_1^m = \cdots = x_l^m = y_1$, $x_{l+1}^m = \cdots = x_{2l}^m = y_2$, and so on, until $x_{(k-1)l+1}^m = \cdots = x_{kl}^m = y_k$, and the proof of lemma 2 is complete.

Note that this allows the computation of sums or products as $\sum_{j=1}^n f(x_j^m)$, $\prod_{j=1}^n f(x_j^m)$ (for some function f defined on complex numbers) in terms of the values of f for the primitive roots of unity of order q', namely

$$\sum_{j=1}^n f(x_j^m) = \frac{\varphi(q)}{\varphi(q')} \sum_{s=1}^k f(y_s), \quad \prod_{j=1}^n f(x_j^m) = \left(\prod_{s=1}^k f(y_s) \right)^{\frac{\varphi(q)}{\varphi(q')}}.$$

The proof above actually mimics the proof (as lemma 3 is a particular case) of the following

Proposition 2. If $f \in \mathbb{Q}[X]$ is an irreducible polynomial in $\mathbb{Q}[X]$, of degree n, if $x_1, \dots, x_n$ are its complex roots, and if $g \in \mathbb{Q}[X]$ is any polynomial, then the numbers $g(x_1), \dots, g(x_n)$ can be split into $k \geq 1$ groups of the same size l such that in each group the numbers are all equal, and the common values of the numbers from the k groups are mutually distinct. Of course, we have $kl = n$. More specifically, we have, after a possible re-indexation, $g(x_1) = \cdots = g(x_l) = a_1$, $g(x_{l+1}) = \cdots = g(x_{2l}) = a_2$, and so on, until $g(x_{(k-1)l+1}) = \cdots = g(x_n) = a_k$, with $a_1, \dots, a_k$ mutually distinct.

Moreover, $g(x_1), \dots, g(x_n)$ have the same minimal polynomial, and k is precisely the degree of this minimal polynomial.

This is the main result from [1], and, basically, starting from it we found the property of the primitive roots of unity described in lemma 3, the property that allows the (very direct) evaluation of Ramanujan's sums. Thus proposition 2 lead us to lemma 3, and only after all that we found the arithmetic property from lemma 2, which, clearly, is equivalent to lemma 3. Thus we wrote the note following a more natural order of the results, rather than the order in which we "discovered" them. (We don't have any reference for lemmas 2 and 3 in the literature, but we don't really think that there isn't one.) We thought, however, that it is interesting to find an elementary property starting from (a little bit more) advanced results, that is why we wrote this note.

Finally, we gratefully thank Gabriel Dospinescu for his valuable suggestions which considerably improved the content and the form of this note. Actually, he is the one who found the two elementary proofs of lemma 2.

References

1. T. Andreescu, M. Tetiva: *About an Old Romanian TST Problem*, *Mathematical Reflections*, 5/2018

2. Tom M. Apostol: *Introduction to Analytic Number Theory*, Springer-Verlag, New York Heidelberg Berlin, 1976

Titu Andreescu
University of Texas at Dallas
Richardson, TX, USA
Marian Tetiva
National College "Gheorghe Roşca Codreanu"
Bîrlad, Romania