References

[1] G. Birkhoff and S. Mac Lane, A Survey of Modern Algebra, 4th ed., Macmillan, 1977.
[2] R. Bronson, Matrix Algebra: An Introduction, Academic Press, 1970.
[3] Daniel T. Finkbeiner, Introduction to Matrices and Linear Transformations, 3rd ed., Freeman, 1978.
[4] Felix R. Gantmacher, Theory of Matrices, Chelsea, 1959.
[5] D. C. Murdoch, Linear Algebra, John Wiley and Sons, New York, 1970.

A Number-Theoretic Sum

JOHN D. BAUM
Oberlin College
Oberlin, OH 44074

A topic which comes up in many elementary number theory texts, and one which I like to cover in a first course in number theory, is the Möbius inversion formula. Recall that the Möbius function $\mu(n)$ assigns -1, 0, or 1 to each positive integer n by the rule

$$\mu(n)=\begin{cases}1 & \text{if } n=1\\ 0 & \text{if } a^2\mid n, \text{ for some integer } a>1\\ (-1)^r & \text{if } n=p_1p_2\cdots p_r,\ p_i \text{ distinct primes.}\end{cases}$$

The Möbius inversion formula asserts that if $F(n)$ and $f(n)$ are functions with domain the set of positive integers, and range in the set of complex numbers, (i.e., number-theoretic functions), with $F(n)=\Sigma_{d|n}f(d)$ for every positive integer n, then $f(n)=\Sigma_{d|n}\mu(d)F(n/d)$, where $\Sigma_{d|n}$ indicates that the sum is to be taken over all divisors d of n [**1**, p. 245], [**2**, p. 88].

The number of exercises which use this formula and which are interesting is small, and it was in an attempt to add to this small number that I discovered the theorem of this note. First a bit of notation. As usual, (m,n) designates the greatest common divisor of integers m and n. If T is a set of positive integers, ΣT designates the sum of the elements of T (for example, $\Sigma\{2,4,7\}=13$). For positive integers n and k, define the following sets of positive integers:

$$R_k(n)=\{x^k \mid 1\leqslant x\leqslant n,\ (x,n)=1\},$$
$$R'_k(n)=\left\{x^k \mid 1\leqslant x\leqslant \frac{n}{2},\ (x,n)=1\right\},$$

where we write $R(n)$ for $R_1(n)$ and $R'(n)$ for $R'_1(n)$. We are interested in calculating the sum of the elements in these sets; accordingly we let $S_k(n)=\Sigma R_k(n)$ and $S'_k(n)=\Sigma R'_k(n)$. (We write $S(n)$ for $S_1(n)$ and $S'(n)$ for $S'_1(n)$.)

It is a nice exercise in the use of the Möbius inversion formula to calculate $S_2(n)$, and this calculation is the content of Exercises 9–14 on page 90 of [**2**]. It is not a difficult matter to extend these ideas to calculate $S_3(n)$, $S_4(n)$ and so on. Note that the number of elements in $R(n)$ is $\phi(n)$, the Euler ϕ-function, and that it is a simple matter to compute $S(n)$. For if $(x,n)=1$, then also $(n-x,n)=1$, and since the sum of x and $n-x$ is n, it follows that

$$S(n)=\frac{n\phi(n)}{2} \tag{1}$$

(see also [**1**, p. 150] or [**2**, p. 36]). It is natural to wonder if the calculation of $S'(n)$ might also be interesting. My first conjecture was that

$$S'(n)=\left(\frac{n}{2}\right)\phi\left(\frac{n}{2}\right)/2=\frac{1}{8}n\phi(n).$$

Indeed, $S'(4)=1=\frac{1}{8}4\phi(4)$ gave confirmation for one example. But I found to my surprise, in trying other values of n, that although the sums $S(n)$, $S_2(n)$, and in general, $S_k(n)$, do not depend upon the form of n, the sum $S'(n)$ does. The residue modulo 4 of n determines the value of $S'(n)$. The method of calculation of $S'(n)$ is the content of the theorem below.

Several well-known facts that we shall use are collected in the following lemma. In this, and in the theorem, the function $\psi(n)$ is defined

$$\psi(n)=\Pi_{p|n}(1-p).$$

LEMMA. 1. $\phi(n)=n\cdot\Pi_{p|n}\left(1-\frac{1}{p}\right)$, *the product being taken over all primes which divide n* [**1**, p. 139].

If $\mu(n)$ is the Möbius function, then

2. $\Sigma_{d|n}\mu(d)d=\psi(n)$ [**1**, p. 125]

3. $\Sigma_{d|n}\frac{\mu(d)}{d}=\frac{\phi(n)}{n}$ [**1**, p. 151].

Furthermore we take it as well known that $\Sigma_{i=1}^{n}i=n(n+1)/2$ and that $\Sigma_{i=1}^{n}(2i-1)=n^2$.

THEOREM. *Let n be an integer greater than* 2. *If* $n\equiv r$ mod 4, *where r is one of the residues*: -1, 0, 1, *or* 2, *then*

$$S'(n)=\frac{1}{8}\left[n\phi(n)-|r|\psi(n)\right].$$

Proof. CASE I. $n\equiv 0$ mod 4. Observe that if $(x,n)=1$, then also $\left(x,\frac{n}{2}\right)=1$ and conversely. $S'(n)$ therefore equals $S'\left(\frac{n}{2}\right)$, which by (1), equals $\frac{1}{2}\left(\frac{n}{2}\phi\left(\frac{n}{2}\right)\right)$. Since $n\equiv 0$ mod 4 it is easily seen that $\phi\left(\frac{n}{2}\right)=\frac{1}{2}\phi(n)$, so that $S'(n)=\frac{1}{8}n\phi(n)$.

CASE II. $n\equiv\pm 1$ mod 4. Let $N_d=\{x\,|\,1\leqslant x\leqslant(n-1)/2,\ (x,n)=d\}$. Now

$$\sum_{i=1}^{\frac{n-1}{2}} i=\sum_{d|n}\sum N_d. \tag{2}$$

Let x be a summand in ΣN_d; then $(x,n)=d$, whence $\left(\frac{x}{d},\frac{n}{d}\right)=1$. Since $1\leqslant x\leqslant(n-1)/2$, it follows that $1\leqslant x/d\leqslant(n-1)/2d<n/2d$. Thus x/d occurs as a summand in $S'\left(\frac{n}{d}\right)$, or equivalently, x occurs as a summand in $dS'\left(\frac{n}{d}\right)$. The argument works just as well conversely, so that

$$\sum N_d=dS'\left(\frac{n}{d}\right)=\frac{n}{d^*}S'(d^*),\text{ where } d^*=\frac{n}{d}.$$

Thus from (2),

$$n\sum_{d|n}\frac{S'(d)}{d}=\sum_{i=1}^{\frac{n-1}{2}}i=\frac{1}{2}\left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right)=\frac{n^2-1}{8}$$

or

$$\frac{n-\frac{1}{n}}{8}=\sum_{d|n}\frac{S'(d)}{d}.$$

Note that this last result holds only if n is odd, but that is guaranteed by the hypothesis of this case. Applying the Möbius inversion formula to this last sum, we see that

$$\begin{aligned}\frac{S'(n)}{n} &= \frac{1}{8}\sum_{d|n}\mu(d)\left(\frac{n}{d}-\frac{d}{n}\right)\\ &= \frac{1}{8}\left(n\sum_{d|n}\frac{\mu(d)}{d}-\frac{1}{n}\sum_{d|n}d\mu(d)\right)\\ &= \frac{1}{8}\left(\phi(n)-\frac{\psi(n)}{n}\right),\end{aligned}$$

by 2. and 3. of the Lemma. Thus, $S'(n)=\frac{1}{8}(n\phi(n)-\psi(n))$.

CASE III. $n\equiv 2 \bmod 4$. In this case $n=2m$, where m is odd. Thus $(x,n)=1$ is equivalent to $(x,m)=1$ and x is odd. From this observation, we have

$$\begin{aligned}S'(n) &= \sum\{x\,|\,1\leqslant x\leqslant m,\,(x,m)=1,\,x\text{ odd}\}\\ &= \sum\{x\,|\,1\leqslant x\leqslant m,\,(x,m)=1\}-\{2x\,|\,1\leqslant 2x\leqslant m,\,(x,m)=1\}.\end{aligned}$$

In this case, $\phi(n)=\phi(m)$ and $\psi(n)=-\psi(m)$, and since m is odd we may apply Case II and (1) to our last equation to obtain

$$\begin{aligned}S'(n) &= \frac{m\phi(m)}{2}-2\left(\frac{1}{8}[m\phi(m)-\psi(m)]\right)\\ &= \frac{n\phi(n)}{4}-\frac{1}{4}\left(\frac{n}{2}\phi(n)+\psi(n)\right)\\ &= \frac{1}{8}(n\phi(n)-2\psi(n)).\end{aligned}$$

This completes the proof.

As an exercise, the reader may verify that computations similar to those in the above proof lead to the following formulae for $S_2'(n)$:

$$S_2'(n)=\begin{cases}\dfrac{n^2\phi(n)+2n\psi(n)}{24} & \text{if } n\equiv 0 \bmod 4\\[2ex] \dfrac{n^2\phi(n)-4n\psi(n)}{24} & \text{if } n\equiv 2 \bmod 4\\[2ex] \dfrac{n^2\phi(n)-n\psi(n)}{24} & \text{if } n\equiv \pm 1 \bmod 4.\end{cases}$$

We note by way of contrast the formula for $S_2(n)$ [**2**, p. 91]:

$$S_2(n)=\frac{2n^2\phi(n)+n\psi(n)}{6}.$$

Finally, it is interesting to observe that $S'(n)/S(n)$ tends to the limit $(1/2)^2$ as n tends to infinity and that $S_2'(n)/S_2(n)$ tends to $(1/2)^3$. This is what one might expect if the elements of $R(n)$ were uniformly distributed in the interval $0\leqslant x\leqslant n$.

The author wishes to thank both the editor and the referee for many helpful suggestions.

References

[1] David M. Burton, Elementary Number Theory, Allyn-Bacon, Boston, 1976.

[2] I. Niven and H. S. Zuckerman, An Introduction to the Theory of Numbers, 3rd ed., Wiley, New York, 1972.