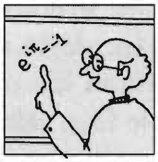

In this section of* Resonance, *we invite readers to pose questions likely to be raised in a classroom situation. We may suggest strategies for dealing with them, or invite responses, or both. "Classroom" is equally a forum for raising broader issues and sharing personal experiences and viewpoints on matters related to teaching and learning science.

Abhishek Saha
B. Math. Hons. Ist year
Indian Statistical Institute
8th Mile Mysore Road
Bangalore 560 059, India.

Sums of Powers of the Primitive Roots of a Prime

In [1], the construction of regular polygons by a ruler and a compass is discussed. In the last section of the article, the notion of cyclotomic polynomials is employed to evaluate the sum of the primitive roots of a prime p. This turns out to be $\mu(p-1)$ where μ is the Möbius function. The general question of evaluating the sum of the m-th powers of the primitive roots is also raised. Here, we answer this question in an elementary manner. Recall that a natural number a is a primitive root of a prime p if $p-1$ is the smallest natural number for which $a^{p-1} \equiv 1 \bmod p$. Let $1 \leq r_1, r_2, \quad, r_k \leq p-1$ be the integers that are co-prime to $p-1$. Then if w is a primitive root of p, we know that $w^{r_1}, w^{r_2}, \quad, w^{r_k}$ are all the primitive roots.

We wish to evaluate the sum $S = \sum_{i=1}^{k} (w^{r_i})^m$. Let us note that as primitive roots are defined only modulo p, this sum will be evaluated only modulo p.

Keywords
Primitive roots, inclusion-exclusion principle.

Here and elsewhere in this proof, we write $a = b$ to mean $a \equiv b \bmod p$. Thus S is simply the congruence class modulo p to which $\sum_{i=1}^{k}(w^{r_i})^m$ belongs.

Let us start with the useful observation (here and elsewhere (a,b) denotes the GCD of two natural numbers):

Lemma. *For an integer q, let $(p-1,q) = d$. Then, if t divides $p-1$,*

$$\sum_{\ell=1}^{(p-1)/t} w^{tq\ell} = \begin{cases} 0 & \text{if } \frac{p-1}{d} \nmid t \\ \frac{p-1}{t} & \text{if } \frac{p-1}{d} | t \end{cases}$$

Proof.

$$w^{tq} = 1 \Leftrightarrow p-1 | tq \Leftrightarrow \frac{p-1}{d} | t$$

In this case $\sum_{\ell=1}^{(p-1)/t} w^{tq\ell} = 1 + 1 + \quad + 1 = \frac{p-1}{t}$.

If $w^{tq} \neq 1$, then

$$\begin{aligned} \sum_{\ell=1}^{(p-1)/t} w^{tq\ell} &= w^{tq} + w^{2tq} + \quad + w^{(p-1)q} \\ &= \frac{w^{tq}(w^{(tq)\cdot\frac{p-1}{t}} - 1)}{w^{tq} - 1} \\ &= 0. \end{aligned}$$

We shall prove:

Theorem. *The sum S of m-th powers of primitive roots for p is given by $S = \mu(g)\frac{\phi(p-1)}{\phi(g)}$ where $g = \frac{p-1}{(m,p-1)}$.*

Here ϕ and μ are Euler's phi function and the Möbius function respectively. We shall evaluate S by using the inclusion-exclusion principle.

Proof. Let $p_1, p_2, \quad , p_s$ be the various distinct prime divisors of $p-1$. Thus

$$S = \sum_{i=1}^{k}(w^{r_i})^m = \sum_{i=1}^{p-1} w^{im} - \sum_{j=1}^{s}\sum_{i=1}^{\frac{p-1}{p_j}}(w^{ip_j})^m$$

$$+\sum_{j_1<j_2}\sum_{i=1}^{(p-1)/(p_{j_1}p_{j_2})}(w^{ip_{j_1}p_{j_2}})^m$$

$$-\quad +(-1)^u\sum_{j_1<\ldots<j_u}\sum_{i=1}^{(p-1)/(p_{j_1}p_{j_2}\cdots p_{j_u})}(w^{ip_{j_1}p_{j_2}\cdots p_{j_u}})^m$$

$$\pm\quad +(-1)^s\sum_{i=1}^{(p-1)/(p_1p_2\cdots p_s)}(w^{ip_1p_2\cdots p_s})^m \qquad \spadesuit$$

The above equality is deduced as follows. Let $T = \{1, 2, \quad, p-1\}$ and let T_f denote the subset of T consisting of those integers from T which are divisible by f. Then by the inclusion-exclusion principle, one gets:

$$S = \sum_{(x,p-1)=1}(w^x)^m = \sum_{x\in T}(w^x)^m - \{\sum_{x\in T_{p_1}}(w^x)^m +$$

$$+\sum_{x\in T_{p_s}}(w^x)^m\} + \sum_{i<j}\sum_{x\in(T_{p_i}\cap T_{p_j})}(w^x)^m -$$

$$+(-1)^s\sum_{x\in(T_{p_1}\cap T_{p_2}\cap\ldots\cap T_{p_s})}(w^x)^m$$

Finally, as it is clear that

$$\sum_{x\in(T_{p_{j_1}}\cap T_{p_{j_2}}\cap\ldots\cap T_{p_{j_u}})}(w^x)^m = \sum_{i=1}^{(p-1)/(p_{j_1}p_{j_2}\cdots p_{j_u})}(w^{ip_{j_1}p_{j_2}\cdots p_{j_u}})^n$$

we obtain the expression $\spadesuit$ for S.

Now $\{p_1, p_2, \quad, p_s\}$ is the set of all prime divisors of $p-1$. Consider its subset $\{p_1, p_2, \quad, p_t\}$, the set of prime divisors of $g = \frac{p-1}{(m,p-1)}$. Then, by the lemma, a sum of the form $\sum_{i=1}^{(p-1)/(p_{j_1}p_{j_2}\cdots p_{j_u})}(w^{ip_{j_1}p_{j_2}\cdots p_{j_u}})^m$ is not equal to 0 if and only if $g|p_{j_1}p_{j_2}\quad . p_{j_k}$. Clearly this happens only if g is squarefree. Assume g is squarefree; then $g = p_1p_2\quad . p_t$. So, in evaluating S, we only have to find the sum of all terms of the form

$$(-1)^u\sum_{i=1}^{(p-1)/(p_{j_1}p_{j_2}\cdots p_{j_u})}(w^{ip_{j_1}p_{j_2}\cdots p_{j_u}})^m$$

where $\{1, 2, \quad, t\} \subseteq \{j_1, j_2, \quad, j_u\}$. But, the lemma gives us

$$\sum_{i=1}^{(p-1)/(p_{j_1}p_{j_2}\cdots p_{j_u})} (w^{ip_{j_1}p_{j_2}\cdots p_{j_u}})^m = \frac{p-1}{p_{j_1}p_{j_2} \quad \cdot p_{j_u}}$$

whenever $\{1, 2, \quad t\} \subseteq \{j_1, j_2, \quad . j_u\}$. Hence, we have

$$S = (-1)^t \frac{p-1}{p_1p_2 \quad \cdot p_t} +$$

$$(-1)^{t+1}\left[\frac{p-1}{p_1p_2 \quad \cdot p_tp_{t+1}} + \quad + \frac{p-1}{p_1p_2 \quad \cdot p_tp_s}\right]$$

$$+(-1)^{t+2}\left[\frac{p-1}{p_1p_2 \quad \cdot p_t}\left(\frac{1}{p_{t+1}p_{t+2}} + \frac{1}{p_{t+1}p_{t+3}} + \quad + \frac{1}{p_{s-1}p_s}\right)\right]$$

$$\pm \quad + (-1)^s \frac{p-1}{p_1p_2 \quad \cdot p_s}$$

$$= (-1)^t \frac{p-1}{p_1p_2 \quad \cdot p_t}\left[1 - \left(\frac{1}{p_{t+1}} + \quad + \frac{1}{p_s}\right)\right.$$

$$\left. + \left(\frac{1}{p_{t+1}p_{t+2}} + \quad + \frac{1}{p_{s-1}p_s}\right) + \quad + \frac{(-1)^{s-t}}{p_{t+1}p_{t+2} \quad \cdot p_s}\right]$$

$$= (-1)^t \frac{p-1}{p_1p_2 \quad \cdot p_t}\left(1 - \frac{1}{p_{t+1}}\right)\left(1 - \frac{1}{p_{t+2}}\right) \quad \left(1 - \frac{1}{p_s}\right)$$

$$= (-1)^t \left(\frac{p-1}{p_1p_2 \quad \cdot p_t}\right) \frac{(1-\frac{1}{p_1})(1-\frac{1}{p_2}) \quad (1-\frac{1}{p_s})}{(1-\frac{1}{p_1})(1-\frac{1}{p_2}) \quad (1-\frac{1}{p_t})}$$

$$= (-1)^t \left(\frac{p-1}{p_1p_2 \quad \cdot p_t}\right) \frac{\phi(p-1)/(p-1)}{\phi(g)/g} = \mu(g)\frac{\phi(p-1)}{\phi(g)}$$

since $g = p_1 \quad \cdot p_t$ and $(-1)^t = \mu(g)$).

Thus whenever g is squarefree, $S = \frac{\mu(g)\phi(p-1)}{\phi(g)}$. But, if g is not squarefree, g cannot divide $p_{j_1}p_{j_2} \quad \cdot p_{j_u}$; so each term of $\spadesuit$ is 0 and $S = 0$. Also $\mu(g)\frac{\phi(p-1)}{\phi(g)} = 0$ if g is not squarefree. Therefore, in all cases $S = \mu(g)\frac{\phi(p-1)}{\phi(g)}$.

Suggested Reading

[1] B Sury, Cyclotomy and cyclotomic polynomials, *Resonance*, Vol.4, No.12, 1999.