Notes on primitive lambda-roots

Peter J. Cameron and D. A. Preece

Draft

This version of July 17, 2009 is on the Web at the address
http://www.maths.qmul.ac.uk/~pjc/csgnotes/lambda.pdf

Abstract

Euler's totient function ϕ has the property that $\phi(n)$ is the order of the group $U(n)$ of units in $\mathbb{Z}_n$ (the integers mod n). In the early years of the twentieth century, Carmichael defined a similar function λ, where $\lambda(n)$ is the exponent of $U(n)$. He called an element of $U(n)$ with order $\lambda(n)$ a primitive λ-root of n.

Subsequently, primitive λ-roots have not received much attention until recently, when they have been used in the construction of terraces and difference sets, and in cryptography.

The purpose of these notes is to outline the theory of primitive λ-roots and to describe some recent developments motivated by the design-theoretic applications.

1 Motivation

Consider the following sequence of the elements of $\mathbb{Z}_{35}$:

START
10 15 5 3 9 27 11 33 29 17 16 13 4 12 1 21 7 ↘
0
25 20 30 32 26 8 24 2 6 18 19 22 31 23 34 14 28 ↙
FINISH

The last 17 entries, in reverse order, are the negatives of the first 17, which, with the zero, can also be written

$$5^5 \;\; 5^6 \;\; 5^7 \mid 3^1 \;\; 3^2 \;\; 3^3 \;\; 3^4 \;\; 3^5 \;\; 3^6 \;\; 3^7 \;\; 3^8 \;\; 3^9 \;\; 3^{10} \;\; 3^{11} \;\; 3^{12} \mid 7^4 \;\; 7^5 \mid 0.$$

If we write the respective entries here as x_i ($i = 1,2,\ldots,18$), then the successive differences $x_{i+1} - x_i$ ($i = 1,2,\ldots,17$) are

$$5 \quad -10 \quad -2 \quad 6 \quad -17 \quad -16 \quad -13 \quad -4 \quad -12 \quad -1 \quad -3 \quad -9 \quad 8 \quad -11 \quad -15 \quad -14 \quad -7.$$

Ignoring minus signs, these differences consist of each of the values $1,2,\ldots,17$ exactly once. Thus the initial sequence of 35 elements is a special type of *terrace*. Indeed, it is a *narcissistic half-and-half power-sequence terrace* – see [2, 3] for the explanation of these terms. Its construction depends in particular on the sequence $3^1\ 3^2\ \ldots\ 3^{11}\ 3^{12}$ (with $3^{12} = 3^0 = 1$) consisting of the successive powers of 3, which is a *primitive* λ*-root* of 35.

Consider now the following sequence of the elements of $\mathbb{Z}_{15}$:

$$6 \quad 3 \,|\, 2 \quad 4 \quad 8 \quad 1 \,|\, 10 \,|\, 0 \,|\, 5 \,|\, 14 \quad 7 \quad 11 \quad 3 \,|\, 12 \quad 9.$$

This too is a terrace, and is of the same special type as before. Its construction depends in particular on the segment $|\ 2\ 4\ 8\ 1\ |$ which is $|\ 2^1\ 2^2\ 2^3\ 2^4\ |$ (with $2^4 = 2^0 = 1$); this consists of the successive powers of 2, which is a primitive λ-root of 15. The second, third, fourth and fifth segments of the terrace make up a *Whiteman difference set* [17, Theorem 1, p. 112], with unsigned differences (written under the difference set, with the element in the ith row being the unsigned difference of the two elements i steps apart in the 0th row symmetrically above it) as follows:

2		4		8		1		10		0		5
	2		4		7		6		5		5	
		6		3		2		1		5		
			1		6		7		4			
				7		4		3				
					2		1					
						3						

Thus primitive λ-roots are important in the construction of both terraces and difference sets.

We have written these notes in expository style. Basic results on number theory and on finite abelian groups can be found in any standard text, for example Hardy and Wright [10] or LeVeque [12], and Hartley and Hawkes [11], respectively. We are grateful to Donald Keedwell, Matt Ollis and David Rees for their comments.

2 Finite abelian groups

In these notes, C_n denotes a cyclic group of order n (which is usually written multiplicatively), and $\mathbb{Z}_n$ denotes the integers modulo n (which is additively a cyclic group of order n but has a multiplicative structure as well).

The *Fundamental Theorem of Finite Abelian Groups* asserts that every such group can be written as a direct product of cyclic groups. This statement, however, needs refining, since the same group may be expressed in several different ways: for example, $C_6 \cong C_2 \times C_3$.

There are two commonly used *canonical forms* for finite abelian groups. Each of them has the property that any finite abelian group is isomorphic to exactly one group in canonical form, so that we can test the isomorphism of two groups by putting each into canonical form and checking whether the results are the same. We refer to Chapter 10 of Hartley and Hawkes [11] for further details.

2.1 Smith canonical form

Definition The expression

$$C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}$$

is in *Smith canonical form* if n_i divides n_{i+1} for $i = 1, \ldots, r-1$. Without loss of generality, we can assume that $n_1 > 1$; with this proviso, the form is unique; that is, if

$$C_{n_1} \times \cdots \times C_{n_r} \cong C_{m_1} \times \cdots \times C_{m_s}$$

where also m_j divides m_{j+1} for $j = 1, \ldots, s-1$, then $r = s$ and $n_i = m_i$ for $i = 1, \ldots, r$.

The numbers $n_1, \ldots, n_r$ are called the *invariant factors*, or *torsion invariants*, of the abelian group.

The algorithm for putting an arbitrary direct product of cyclic groups into Smith canonical form is as follows. Suppose that we are given the group $C_{l_1} \times \cdots \times C_{l_q}$, where $l_1, \ldots, l_q$ are arbitrary integers greater than 1. Define, for $i > 0$,

$$\prod_{j=1}^{i} n'_j = \mathrm{lcm}\left(\prod_{j=1}^{i} l_{k_j} : 1 \le k_1 < \cdots < k_i \le q \right).$$

If r is the least value such that $n'_{r+1} = 1$, then write the numbers $n'_1, \ldots, n'_r$ in reverse order:

$$n_i = n'_{r+1-i} \text{ for } i = 1, \ldots, r.$$

Then the Smith canonical form is

$$C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}.$$

For example, suppose that we are given $C_2 \times C_4 \times C_6$. We have

$$\begin{aligned} n'_1 &= \text{lcm}(2,4,6) = 12, \\ n'_1 n'_2 &= \text{lcm}(8,12,24) = 24, \\ n'_1 n'_2 n'_3 &= \text{lcm}(48) = 48, \end{aligned}$$

so that the Smith canonical form is $C_2 \times C_2 \times C_{12}$.

One feature of the Smith canonical form is that we can read off the *exponent* of an abelian group A, the least number m such that $x^m = 1$ for all $x \in A$; this is simply the number n_r, the largest invariant factor.

2.2 Primary canonical form

Using the fact that, if $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where $p_1, \ldots, p_r$ are distinct primes, then

$$C_n = C_{p_1^{a_1}} \times C_{p_2^{a_2}} \times \cdots \times C_{p_r^{a_r}},$$

we see that any finite abelian group can be written as a direct product of cyclic groups each of prime power order.

If we order the primes in increasing order, and then order the factors first by the prime involved and then by the exponent, the resulting expression is unique: this is the *primary canonical form*.

For example, the primary canonical form of $C_2 \times C_4 \times C_6$ is

$$C_2 \times C_2 \times C_4 \times C_3.$$

The exponent is given by taking the orders of the largest cyclic factors for each prime dividing the group order and multiplying these.

The orders of the factors in the primary canonical form are called the *elementary divisors* of the abelian group.

3 Möbius inversion

We sketch here the definition of the Möbius function and the Möbius inversion formula. These will be used several times without comment below. See Chapter 16 of Hardy and Wright [10].

Definition The *Möbius function* is the function μ defined on the positive integers by the rule

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1; \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes;} \\ 0 & \text{if } n \text{ has a square factor greater than 1.} \end{cases}$$

The Möbius inversion formula is the following statement.

Theorem 3.1 *Let f and g be functions on the natural numbers. Then the following conditions are equivalent:*

(a) $g(n) = \sum_{m|n} f(m)$;

(b) $f(n) = \sum_{m|n} \mu(n/m)g(m)$.

For example, Euler's totient ϕ is the function on the natural numbers given by the rule that $\phi(n)$ is the number of integers $m \in [0, n-1]$ for which $\gcd(m,n) = 1$. (In other words, it is the order of the group $U(n)$ of units of $\mathbb{Z}_n$: see the next section.) Now, if $\gcd(m,n) = d$, then $\gcd(m/d, n/d) = 1$; there are $\phi(n/d)$ such integers m, for each divisor d of n. Thus we have

$$n = \sum_{d|n} \phi(n/d) = \sum_{m|n} \phi(m),$$

and so by Möbius inversion,

$$\phi(n) = \sum_{m|n} \mu(n/m)m = \sum_{d|n} \mu(d)n/d.$$

From here it is an exercise to derive the more familiar formula

$$\phi(n) = n \prod_{\substack{p \text{ prime} \\ p|n}} \left(1 - \frac{1}{p}\right).$$

4 The units modulo n

If x is an element of $\mathbb{Z}_n$ (that is, a residue class modulo n), and m is a divisor of n, then we may regard x also as a residue class modulo m. We usually denote this new residue class by the same symbol x. But really, we have a map from $\mathbb{Z}_n$ to $\mathbb{Z}_m$. This map θ is a ring homomorphism: that is, $\theta(x+y) = \theta(x) + \theta(y)$ and $\theta(xy) = \theta(x)\theta(y)$. We call this the *natural map* from $\mathbb{Z}_n$ to $\mathbb{Z}_m$.

The *Chinese remainder theorem* is crucial for what follows. It asserts that, if $n = n_1 \cdots n_r$, where $n_1, \ldots, n_r$ are pairwise coprime, and θ_i is the natural map from $\mathbb{Z}_n$ to $\mathbb{Z}_{n_i}$ for $i = 1, \ldots, r$, then the map

$$x \mapsto (\theta_1(x), \ldots, \theta_r(x))$$

from $\mathbb{Z}_n$ to $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$ is a bijection: indeed, it is an isomorphism from $\mathbb{Z}_n$ to the direct sum of the rings $\mathbb{Z}_{n_i}$.

Let $U(n)$ denote the group (under multiplication mod n) of units of $\mathbb{Z}_n$ (the integers mod n). The units are the non-zero elements of $\mathbb{Z}_n$ which are coprime to n. The number of them is $\phi(n)$, where ϕ is Euler's totient function, defined in the preceding section.

The structure of the group $U(n)$ is given by the following well-known result. The first part follows immediately from the Chinese remainder theorem.

Theorem 4.1 *(a) Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where $p_1, \ldots, p_r$ are distinct primes and $a_1, \ldots, a_r > 0$. Then*

$$U(n) \cong U(p_1^{a_1}) \times U(p_2^{a_2}) \times \cdots \times U(p_r^{a_r}).$$

(b) If p is an odd prime and $a > 0$, then $U(p^a)$ is a cyclic group of order $p^{a-1}(p-1)$.

(c) $U(2)$ is the trivial group and, for $a > 1$, we have $U(2^a) \cong C_2 \times C_{2^{a-2}}$, where the generators of the two cyclic factors are -1 and 5.

Thus, if $n = p^a$ or $n = 2p^a$, where p is an odd prime, then $U(n)$ is a cyclic group. A generator of this group is called a *primitive root* of n.

For example,

$$U(18) = \{1, 5, 7, 11, 13, 17\}.$$

The successive powers $5^0, 5^1, \ldots \pmod{18}$ are

$$1, 5, 7, 17, 13, 11,$$

with $5^6 = 5^0 = 1$; so 5 is a primitive root of 18.

For $n > 4$, the converse is also true: if there is a primitive root of n, then n is an odd prime power or twice an odd prime power. This is because all the non-trivial cyclic factors given by Theorem 4.1 have even order, so if there are at least two of them, then $C_2 \times C_2$ is a subgroup of $U(n)$; this happens if n has two odd prime divisors, or if n is divisible by 4 and an odd prime, or if n is divisible by 8.

The elements of $U(n)$ can be divided into subsets called *power classes*: these are the equivalence classes of the relation $\sim$, where $x \sim y$ if $y = x^d$ for some d with $\gcd(d, \phi(n)) = 1$. (This relation is symmetric because, if $\gcd(d, \phi(n)) = 1$, then there exists e with $de \equiv 1 \pmod{\phi(n)}$; then $y^e = x^{de} = x$. It is easily seen to be reflexive and transitive.) Said otherwise, $x \sim y$ if and only if x and y generate the same cyclic subgroup of $U(n)$. If x has order m (a divisor of $\phi(n)$), then the size of the power class containing x is $\phi(m)$.

Note that all elements of a power class have the same multiplicative order mod n.

It follows from Theorem 5.2 (and is easy to prove directly) that, given any finite abelian group A, there are only a finite number of positive integers n such that $U(n) \cong A$.

Problem 1 Is it true that, in general, arbitrarily many values of n can be found for which the groups $U(n)$ are all isomorphic to one another?

For example, the groups $U(n)$ for $n = 35$, 39, 45, 52, 70, 78 and 90 are all isomorphic to $C_2 \times C_{12}$. There are ten values of n less than 1 000 000 for which $U(n) \cong U(n+1)$, namely 3, 15, 104, 495, 975, 22 935, 32 864, 57 584, 131 144 and 491 535. This is sequence A003276 in the *On-Line Encyclopedia of Integer Sequences* [15], where further references appear.

Problem 2 (a) Are there infinitely many values of n for which $U(n) \cong U(n+1)$?

(b) All the above examples except for $n = 3$ satisfy $n \equiv 4$ or 5 mod 10. Does this hold in general?

5 Carmichael's lambda-function

Euler's function ϕ has the property that $\phi(n)$ is the order of the group $U(n)$ of units of $\mathbb{Z}_n$. R. D. Carmichael [6] introduced the function λ:

Definition For a positive integer n, let $\lambda(n)$ be the exponent of $U(n)$ (the least m such that $a^m = 1$ for all $a \in U(n)$).

From the structure theorem for $U(n)$ (Theorem 4.1), we obtain the formula for $\lambda(n)$:

Proposition 5.1 *(a) If $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where $p_1, p_2, \ldots, p_r$ are distinct primes and $a_1, a_2, \ldots, a_r > 0$, then*

$$\lambda(n) = \mathrm{lcm}(\lambda(p_1^{a_1}), \lambda(p_2^{a_2}), \ldots, \lambda(p_r^{a_r})).$$

(b) If p is an odd prime and $a > 0$, then $\lambda(p^a) = \phi(p^a) = p^{a-1}(p-1)$.

(c) $\lambda(2) = 1$, $\lambda(4) = 2$, and, for $a \geq 3$, we have $\lambda(2^a) = 2^{a-2} = \phi(2^a)/2$.

The values of $\lambda(n)$ appear as sequence A002322 in the *On-Line Encyclopedia of Integer Sequences* [15]. The computer system GAP [9] has the function λ built-in, with the name `Lambda`.

Given m, what can be said about the values of n for which $\lambda(n) = m$? There may be no such values: this occurs, for example, for any odd number $m > 1$. (If $n > 2$, then the unit $-1 \in U(n)$ has order 2, so $\lambda(n)$ is even.) Also, there is no n with $\lambda(n) = 14$, as we shall see.

To get around this problem, we proceed as follows.

Theorem 5.2 *(a) If n_1 divides n_2, then $\lambda(n_1)$ divides $\lambda(n_2)$.*

(b) For any positive integer m, there is a largest n such that $\lambda(n)$ divides m. Denoting this value by $\lambda^*(m)$, we have that

(i) if $n \mid \lambda^*(m)$, then $\lambda(n) \mid m$;

(ii) $\lambda(n) = m$ if and only if n divides $\lambda^*(m)$ but n does not divide $\lambda^*(l)$ for any proper divisor l of m.

(c) The number of n such that $\lambda(n) = m$ is given by the formula

$$\sum_{l \mid m} \mu\left(\frac{m}{l}\right) d(\lambda^*(l)),$$

where $d(n)$ is the number of divisors of n.

Proof (a) Suppose that n_1 divides n_2. The natural map θ from $\mathbb{Z}_{n_2}$ to $\mathbb{Z}_{n_1}$ induces a group homomorphism from $U(n_2)$ to $U(n_1)$. We claim that θ is onto. It is enough to prove this in the case where n_2/n_1 is a prime p.

If p does not divide n_1, then $U(n_2) \cong U(n_1) \times U(p)$, and the conclusion is obvious. Suppose that $p \mid n_1$. Then if $0 < a < n_1$, we have $\gcd(a,n_1) = 1$ if and only if $\gcd(a,n_2) = 1$; so these elements of $U(n_2)$ are inverse images of the corresponding elements of $U(n_1)$.

Now, if $a^m = 1$ for all $a \in U(n_2)$, then $b^m = 1$ for all $b \in U(n_1)$ (since every such b has the form $\theta(a)$ for some $a \in U(n_2)$). So the exponent of $U(n_1)$ divides that of $U(n_2)$, as required.

(b) Suppose that m is given. If $\lambda(n)$ divides m, then $\lambda(p^a)$ divides m for each prime power factor p^a of n. In particular, if p is odd, then $p-1$ must divide m, so there are only finitely many possible prime divisors of n; and for each prime p, the exponent a is also bounded, since p^{a-1} or p^{a-2} must divide m. Hence there are only finitely many possible values of n, and so there is a largest value $\lambda^*(m)$.

By part (a), if $n \mid \lambda^*(m)$, then

$$\lambda(n) \mid \lambda(\lambda^*(m)) \mid m.$$

Conversely, the construction of $\lambda^*(m)$ shows that it is divisible by every n for which $\lambda(n)$ divides m.

(c) This follows from (b) by Möbius inversion.

Remark If $m > 2$ and m is even, then the summation in part (c) can be restricted to even values of l. For, if m is divisible by 4, then $\mu(m/l) = 0$ for odd l; and if m is divisible by 2 but not 4 and $m > 2$, then each odd value of l has $d(\lambda^*(l)) = 2$, and the contributions from such values cancel out.

The calculation of $\lambda^*(m)$ is implicit in the proof of the theorem. Explicitly, the algorithm is as follows. If m is odd, then $\lambda^*(m) = 2$. If m is even, then $\lambda^*(m)$ is the product of the following numbers:

(a) 2^{a+2}, where $2^a \mid\mid m$;

(b) p^{a+1}, for each odd prime p such that $p-1 \mid m$, where $p^a \mid\mid m$.

(Here the notation $p^a \mid\mid m$ means that p^a is the exact power of p dividing m.)

For example, when $m = 12$, the odd primes p such that $p-1 \mid 12$ are $3, 5, 7, 13$; and so

$$\lambda^*(12) = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 = 65\,520.$$

For another example, let $m = 2q$, where q is a prime congruent to 1 mod 6. Then $2q+1$ is not prime, so the only odd prime p for which $p-1$ divides $2q$ is $p = 3$, and we have

$$\lambda^*(2q) = 2^3 \cdot 3 = 24 = \lambda^*(2).$$

Thus, there is no number n with $\lambda(n) = 2q$.

Other numbers which do not occur as values of the function λ include:

(a) $m = 2q_1q_2\cdots q_r$, where $q_1, q_2, \ldots, q_r$ are primes congruent to 1 mod 6 (they may be equal or distinct); for example, 98, 182, 266, ... ;

(b) $m = 2q^2$, where q is any prime greater than 3; for example, 50, 98, 242, ...

We do not have a complete description of such numbers.

Another observation is that, if q is a Sophie Germain prime (a prime such that $2q+1$ is also prime, see [5]), and q is greater than 3, then there are just eight values of n for which $\lambda(n) = 2q$, namely $n = (2q+1)f$, where f is a divisor of 24. We do not know whether other numbers m also occur just eight times as values of λ.

Sierpiński [14] remarks that the only numbers $n < 100$ which satisfy the equation $\lambda(n) = \lambda(n+1)$ are $n = 3$, 15 and 90. But this is not a rare property: a short GAP computation reveals that there are 143 numbers $n < 1\,000\,000$ for which the equation holds.

The formulae show up a couple of errors on p. 236 of [6], giving values of n for prescribed $\lambda(n)$. The entry 136 for $\lambda(n) = 6$ should read 126, and the value 528 is missing for $\lambda(n) = 20$.

Note that, for a fixed even exponent $m = \lambda(n)$, the maximum value $\lambda^*(m)$ of n also maximises the value of $\phi(n)$. For it is easily checked that, if n_1 is a proper divisor of n_2, then $\phi(n_1) \le \phi(n_2)$, with equality only if n_1 is odd and $n_2 = 2n_1$; but if m is even, then $\lambda^*(m)$ is divisible by 8.

For example, the numbers n with $\lambda(n) = 6$, and the corresponding values of $\phi(n)$, are given in the following table. (The function $\xi(n)$ is defined to be

$\phi(n)/\lambda(n)$.)

n	$\phi(n)$	$\xi(n)$
$7,9,14,18$	6	1
$21,28,36,42$	12	2
$56,72,84$	24	4
$63,126$	36	6
168	48	8
252	72	12
504	144	24

Note that the values of $\phi(n)$ are not monotonic in n for fixed $\lambda(n)$.

The order of magnitude of Carmichael's lambda-function was investigated by Erdős, Pomerance and Schmutz [8]. They showed, among other things, that for $x \geq 16$,

$$\frac{1}{x}\sum_{n\leq x}\lambda(n) = \frac{x}{\log x}\exp\left(\frac{B\log\log x}{\log\log\log x}(1+o(1))\right)$$

for some explicit constant B.

A composite positive integer m is called a *Carmichael number* if $\lambda(m)$ divides $m-1$. (For such numbers, a converse of the little Fermat theorem holds: $x^{m-1} \equiv 1 \pmod{m}$ for all residues x coprime to m.) The smallest Carmichael number is 561, with $\lambda(561) = 80$.

5.1 Denominators of Bernoulli numbers

The sequence $(24,240,504,480,264,\ldots)$ of values of $\lambda^*(2m)$ agrees with sequence A006863 in the *Encyclopedia of Integer Sequences* [15]. It is is described as "denominator of $B_{2m}/(-4m)$, where B_m are Bernoulli numbers".

The Bernoulli numbers arise in many parts of mathematics, including modular forms and topology as well as number theory. We won't try to give an account of all the connections here (but see the entry for "Eisenstein series" in MathWorld [16] for some of these); we simply prove that the formula given in the Encyclopedia agrees with the definition of $\lambda^*(2m)$.

The mth term a_m of the *Encyclopedia* sequence is the gcd of $k^L(k^{2m}-1)$, where k ranges over all natural numbers and L is "as large as necessary". To see how this works, consider the case $m = 3$. Taking $k = 2$, we see that a_3 divides $2^L(2^6-1)$, so a_3 is a power of 2 times a divisor of 63. Similarly, with $k = 3$, we find that a_3 is a power of 3 times divisor of 728. We conclude that a_3 divides

504. It is not yet clear, however, that 504 is the final answer, since in principle all values of k must be checked.

We show that a_m (as defined by this formula) is equal to $\lambda^*(2m)$. First, let $n = a_m$, and choose any k with $\gcd(k,n) = 1$. Then n divides $k^L(k^{2m}-1)$. Since k is coprime to n, we have $k^{2m} \equiv 1 \pmod{n}$. So the exponent of $U(n)$ divides $2m$, and n divides $\lambda^*(2m)$.

In the other direction, let $n = \lambda^*(2m)$; we must show that n divides $k^L(k^{2m}-1)$ for all k (with large enough L). Since

$$(k_1k_2)^L((k_1k_2)^{2m}-1) = (k_1k_2)^L k_1^{2m}(k_2^{2m}-1) + (k_1k_2)^L(k_1^{2m}-1),$$

it is enough to prove this when $k = p$ is prime. Write $n = p^a n_1$, where p does not divide n_1. Then $n_1 \mid \lambda^*(2m)$, so $\lambda(n_1) \mid 2m$ by Theorem 5.2; that is, $n_1 \mid p^{2m}-1$. So $n \mid p^a(p^{2m}-1)$, as required.

5.2 p-rank and p-exponent

Definition Let p be a prime. The *p-rank* of an abelian group A is the number of its elementary divisors which are powers of p, and the *p-exponent* is the largest of these elementary divisors.

The 2-rank and 2-exponent of the group of units mod n can be calculated as follows.

Suppose that $n = 2^a p_1^{a_1} \cdots p_r^{a_r}$, where $p_1, \ldots, p_r$ are odd primes, $a_1, \ldots, a_r > 0$, and $a \geq 0$. Then the 2-rank of $U(n)$ is equal to

$$\begin{cases} r & \text{if } a \leq 1, \\ r+1 & \text{if } a = 2, \\ r+2 & \text{if } a \geq 3. \end{cases}$$

The 2-exponent of $U(n)$ is the 2-part of $\lambda(n)$. It is the maximum of 2^b and the powers of 2 dividing $p_i - 1$ for $i = 1, \ldots, r$, where

$$b = \begin{cases} 0 & \text{if } a \leq 1, \\ 1 & \text{if } a = 2, \\ a-2 & \text{if } a \geq 3. \end{cases}$$

In particular, the 2-exponent of $U(n)$ is 2 if and only if

(a) the power of 2 dividing n is at most 2^3;

(b) all odd primes dividing n are congruent to 3 mod 4.

We leave as an exercise the description of the p-rank and p-exponent of $U(n)$ for odd p.

6 Primitive lambda-roots

Carmichael [6] defined primitive λ-roots as a generalisation of primitive roots, to cover cases where the latter do not exist.

Definition A primitive λ-root of n is an element of largest possible order (namely, $\lambda(n)$) in $U(n)$.

We also put $\xi(n) = \phi(n)/\lambda(n)$, where (as noted) $\phi(n)$ is the order of $U(n)$; thus there is a primitive root of n if and only if $\xi(n) = 1$. (Carmichael calls a primitive root a *primitive ϕ-root*.)

Since elements of a power class all have the same order, we see:

Proposition 6.1 *Every element in the power class of a primitive λ-root is a primitive λ-root.*

Proposition 6.2 *For any n, either $\xi(n) = 1$ or $\xi(n)$ is even.*

Proof Theorem 4.1 shows that $\xi(n) = 1$ if and only if $n = p^a$ or $n = 2p^a$, where p is an odd prime. Suppose that this is not the case. Then n is divisible by either two odd primes or a multiple of 4. In the first case, let $n = p^a q^b m$ where p and q are distinct odd primes not dividing m. Then $\phi(n) = \phi(p^a)\phi(q^b)\phi(m)$ and $\lambda(n) = \mathrm{lcm}\{\phi(p^a), \phi(q^b), \lambda(m)\}$; since $\phi(p^a)$ and $\phi(q^b)$ are both even, $\phi(n)/\lambda(n)$ is even. In the second case, if $a \geq 2$ then $\phi(2^a) = 2\lambda(2^a)$, and so $\phi(2^a m)/\lambda(2^a m)$ is even for any odd m.

For example, consider the case $n = 15$. We have $\phi(15) = \phi(3)\phi(5) = 8$, while $\lambda(15) = \mathrm{lcm}(\phi(3), \phi(5)) = 4$, and $\xi(15) = 2$. The group $U(15)$ consists of the elements $1, 2, 4, 7, 8, 11, 13, 14$, and their powers are given in the following table:

element x	powers of x
1	1
2	1, 2, 4, 8
4	1, 4
7	1, 7, 4, 13
8	1, 8, 4, 2
11	1, 11
13	1, 13, 4, 7
14	1, 14

The primitive λ-roots are thus $2, 7, 8, 13$, falling into two power classes $\{2, 8\}$ and $\{7, 13\}$.

Corollary 6.3 *If $\lambda(n) > 2$, then the number of primitive λ-roots of n is even.*

Proof The number of PLRs in a power class is $\phi(\lambda(n))$; and $\phi(m)$ is even for $m > 2$.

Proposition 6.4 *The group $U(n)$ of units mod n is generated by primitive lambda-roots; the least number of PLRs required to generate the group is equal to the number of invariant factors.*

Proof We can write $U(n) = A \times B$, where A is a cyclic group of order $\lambda(n)$ generated by a primitive lambda-root a. Clearly every element of A lies in the subgroup generated by the primitive lambda-roots. For any $b \in B$, the element ab is a primitive lambda-root; for if m is a proper divisor of $\lambda(n)$, then $(ab)^m = a^m b^m$ and $a^m \neq 1$. So b is the product of the primitive lambda-roots a^{-1} and ab.

The number of generators of $U(n)$ is not less than the number of invariant factors. Suppose that $a_1, \ldots, a_r$ are generators of the invariant factors of $U(n)$, where a_1 is a PLR. Then the elements $a_1, a_1a_2, \ldots, a_1a_r$ are all PLRs and clearly generate $U(n)$.

How many primitive λ-roots of n are there? The answer is obtained by putting $m = \lambda(n)$ in the following result:

Theorem 6.5 *Let $A = C_{m_1} \times C_{m_2} \times \cdots \times C_{m_r}$ be an abelian group. Then, for any m, the number of elements of order m in A is*

$$\sum_{l|m} \mu\left(\frac{m}{l}\right) \prod_{i=1}^{r} \gcd(l, m_i).$$

Proof Let $a = (a_1, a_2, \ldots, a_r) \in A$. Then $a^m = 1$ if and only if $a_i^m = 1$ for $i = 1, \ldots, r$. The number of elements $x \in C_{m_i}$ satisfying $x^m = 1$ is $\gcd(m, m_i)$, so the number of elements $a \in A$ satisfying $a^m = 1$ is $g(m) = \prod_{i=1}^{r} \gcd(m, m_i)$. Now $a^m = 1$ if and only if the order of a divides m; so $g(m) = \sum_{l|m} f(l)$, where $f(l)$ is the number of elements of order l in A. Now the result follows by Möbius inversion.

For example, $U(65) \cong U(5) \times U(13) \cong C_4 \times C_{12}$, so that $\lambda(65) = 12$; and the number of primitive λ-roots is

$$\sum_{l|12} \mu(12/l) \gcd(4, l) \gcd(12, l).$$

The only non-zero terms in the sum occur for $l = 12, 6, 4, 2$, and the required number is

$$4 \cdot 12 - 2 \cdot 6 - 4 \cdot 4 + 2 \cdot 2 = 24.$$

Since $\phi(12) = 4$, there are $24/4 = 6$ power classes of primitive λ-roots; these are $\{2, 32, 33, 63\}$, $\{3, 22, 42, 48\}$, $\{6, 11, 41, 46\}$, $\{7, 28, 37, 58\}$, $\{17, 23, 43, 62\}$ and $\{19, 24, 54, 59\}$.

The following table gives the number of primitive λ-roots, and the smallest primitive λ-root, for certain values of n.

n	$\phi(n)$	$\lambda(n)$	# PLRs	Smallest PLR
15	8	4	4	2
24	8	2	7	5
30	8	4	4	7
35	24	12	8	2
63	36	6	24	2
65	48	12	24	2
91	72	12	32	2
105	48	12	16	2
117	72	12	32	2
143	120	60	32	2
168	48	6	20	5
189	108	18	54	2
275	200	20	96	2

We have $U(15) \cong U(30) \cong C_2 \times C_4$, and $U(91) \cong U(117) \cong C_6 \times C_{12}$, explaining the equal numbers and orders of primitive λ-roots in these cases. On the other hand, $\phi(65) = \phi(105)$, but $U(65) \cong C_4 \times C_{12}$, while $U(105) \cong C_2 \times C_4 \times C_6$; these groups are not isomorphic (the Smith canonical form of $U(105)$ is $C_2 \times C_2 \times C_{12}$). Note that, for $n = 143$, the proportion of units that are PLRs is less than $1/3$. In this connection, we have the following result and problem:

Proposition 6.6 *The proportion of units which are primitive λ-roots can be arbitrarily close to* 0.

Proof If $n = p$ is prime, then the proportion of units which are PLRs is

$$\phi(p-1)/(p-1) = \prod_{\substack{r \text{ prime} \\ r \mid p-1}} \left(1 - \frac{1}{r}\right).$$

Choosing p to be congruent to 1 modulo the product of the first k primes (this is possible, by Dirichlet's Theorem) ensures that the product on the right is arbitrarily small. In order to obtain proper PLRs, also choose $p \equiv 1 \pmod 4$; then the proportion for $4p$ is the same as for p.

Problem 3 Can the proportion of units which are primitive λ-roots be arbitrarily close to 1? Numbers n which are of the form $\lambda^*(m)$ seem to be particularly good for this problem. For example, if

$$\begin{aligned} n &= \lambda^*(53\,130) \\ &= 460\,765\,909\,369\,981\,425\,841\,156\,813\,418\,098\,240\,135\,472\,867\,831\,112, \end{aligned}$$

then the proportion of PLRs in the group of units differs from 1 by less than one part in two million.

Li [13] has considered the analogue for PLRs of Artin's conjecture for primitive roots, that is, the function $N_a(x)$ whose value is the number of positive integers $n \le x$ such that a is a PLR of n. This function is more erratic than the corresponding function for primitive roots: the lim inf of $\left(\sum_{1\le a\le x} N_a(x)\right)/x^2$ is zero, while the lim sup of this expression is positive.

6.1 Another formula

Here is another, completely different, method for calculating the number of primitive lambda-roots of n. This depends on knowing the elementary divisors of $U(n)$.

Theorem 6.7 *Let n be a positive integer. For any prime p dividing $\phi(n)$, let $p^{a(p)}$ be the largest p-power elementary divisor of $U(n)$, and let $m(p)$ be the number of elementary divisors of $U(n)$ which are equal to $p^{a(p)}$. Then the number of primitive lambda-roots of n is*

$$\phi(n) \prod_{p\mid\phi(n)} \left(1 - \frac{1}{p^{m(p)}}\right).$$

Proof Write $U(n) = P_1 \times \cdots \times P_r$, where P_i is the p_i-primary part of $U(n)$ (the product of all the cyclic factors of p_i-power order in the primary decomposition of $U(n)$). Now an element of $U(n)$ is a primitive lambda-root if and only if, for each

i with $1 \leq i \leq r$, its projection into P_i is of maximum possible order $p_i^{a(p_i)}$. So we have to work out the fraction of elements of P which are of maximum possible order.

Dropping the subscripts, let $P = C_{p^a} \times \cdots \times C_{p^a} \times Q$, where there are m factors p^a, and Q is a product of cyclic p-groups of orders smaller than p^a. Then an element of P has order p^a if and only if its projection into $(C_{p^a})^m$ has order p^a. So the fraction of elements of maximal order in P is the same as in $(C_{p^a})^m$. Now the elements of the latter group of order less than p^a are precisely those lying in the subgroup $(C_{p^{a-1}})^m$, a fraction $1/p^m$ of the group. So a fraction $1 - 1/p^m$ have order equal to p^a.

This result has a curious corollary. If n is such that primitive roots of n exist (that is, if n is an odd prime power, or twice an odd prime power, or 4), then the number of primitive roots of n is $\phi(\phi(n))$. Now for any n, compare the formula in the theorem with the formula from page 5:

$$\phi(\phi(n)) = \phi(n) \prod_{p|\phi(n)} \left(1 - \frac{1}{p}\right).$$

We see that the number of PLRs is at least $\phi(\phi(n))$, with equality if and only if $m(p) = 1$ for all p dividing $\phi(n)$. In other words:

Corollary 6.8 *For any n, the number of primitive lambda-roots of n is at least $\phi(\phi(n))$. Equality holds if and only if, for each prime p which divides $\phi(m)$, the largest p-power elementary divisor of $U(n)$ is strictly greater than all the other p-power elementary divisors of n. An equivalent condition is that the second largest invariant factor of $U(n)$ divides $\lambda(n)/\sigma(\lambda(n))$, where $\sigma(m)$ is the product of the distinct prime divisors of m.*

Proof The first part follows from the prefatory remarks. The equivalence of the last condition with the condition involving the elementary divisors is clear.

This raises a curious number-theoretic problem.

Problem 4 What proportion of numbers n have the property that the number of PLRs of n is equal to $\phi(\phi(n))$?

A computer search shows that over half of all numbers below ten million have this property (to be precise, 5 309 906 of them do).

The condition in this proposition comes up in a completely different context, namely, a relationship between the number of power classes of PLRs and the function $\xi(n) = \phi(n)/\lambda(n)$.

Proposition 6.9 *For any positive integer n, the number of power classes of PLRs of n is at least* $\xi(n)$. *Equality holds if and only if, for any prime divisor p of* $\phi(n)$, *the largest p-power elementary divisor is strictly greater than any other p-power elementary divisor.*

Proof We can write $U(n) = A \times B$, where A is a cyclic group of order $\lambda(n)$, generated by a (which is a PLR). Now, for each element $b \in B$, the product ab is a PLR. We claim that distinct elements of B give rise to distinct power classes. For suppose that ab_1 and ab_2 lie in the same power class. Then $ab_2 = (ab_1)^m$ for some m with $\gcd(\lambda(n), m) = 1$. This implies that $a = a^m$, so that $m \equiv 1 \pmod{\lambda(n)}$, from which it follows that $b_2 = b_1^m = b_1$. So there are at least as many power classes as elements of B. Since $|B| = \phi(n)/\lambda(n) = \xi(n)$, the inequality is proved.

Equality holds if and only if, whenever $a \in A$, $b \in B$, and ab is a PLR, it follows that a is a PLR. Suppose that the condition on elementary divisors holds. For any p dividing $\lambda(n)$, the p-elementary divisors of B divide $\lambda(n)/p$, and so $b^{\lambda(n)/p} = 1$. Hence $a^{\lambda(n)/p} = (ab)^{\lambda(n)/p} \neq 1$. Since this holds for all p, the order of a is $\lambda(n)$, and so a is a PLR. Conversely, suppose that the condition on elementary divisors fails, and suppose that the largest p-elementary divisor of B is p^r and is the p-part of $\lambda(n)$. Choose an element $b \in B$ of order p^r. Then $a^{p^r}b$ is a PLR, but a^{p^r} is not.

For another proof that the cases of equality in the two results coincide, note that $\phi(n)$ and $\lambda(n)$ have the same prime divisors, and so

$$\frac{\phi(\phi(n))}{\phi(n)} = \frac{\phi(\lambda(n))}{\lambda(n)},$$

so that $\xi(n) = \phi(\phi(n))/\phi(\lambda(n))$, whereas the number of power classes is the number of PLRs divided by $\phi(\lambda(n))$.

Example For $n = 360 = 2^3 \cdot 3^2 \cdot 5$, we have

$$U(n) \cong C_2 \times C_2 \times C_6 \times C_4 \cong C_4 \times C_2^3 \times C_3,$$

so

$$\begin{aligned} \#\text{PLRs} = \phi(\phi(n)) &= 32, \\ \#\text{PCs} = \xi(n) &= 8. \end{aligned}$$

For $n = 720 = 2^4 \cdot 3^2 \cdot 5$, we have

$$U(n) \cong C_2 \times C_4 \times C_6 \times C_4 \cong C_4^2 \times C_2^2 \times C_3,$$

so

$$\begin{aligned} \#\text{PLRs} &= 96, & \phi(\phi(n)) &= 64, \\ \#\text{PCs} &= 24 & \xi(n) &= 16. \end{aligned}$$

6.2 Fraternities

Definition Two PLRs x and y of n are said to be *fraternal* if $x^2 \equiv y^2 \pmod{n}$. This is an equivalence relation on the set of PLRs; its equivalence classes are called *fraternities*.

Recall the definition of 2-rank and 2-exponent from Subsection 5.2.

Proposition 6.10 *Suppose that $n \geq 2$. Let the 2-rank and 2-exponent of $U(n)$ be s and 2^e respectively. Then the size of a fraternity of PLRs of n is equal to*

$$\begin{cases} 2^s & \text{if } e > 1, \\ 2^s - 1 & \text{if } e = 1. \end{cases}$$

Proof Let $A = \{u \in U(n) : u^2 \equiv 1 \pmod{n}\}$. Clearly $|A| = 2^s$. Since $x^2 \equiv y^2$ if and only if $x = yu$ for some $u \in A$, each fraternity is the intersection of the set of PLRs with a coset of A.

Let a coset C of A contain an element of even order $2m$. If m is even, then every element of C has order $2m$. Suppose that m is odd. Then, for $u \in C$, $u^m \in A$, and $u \cdot u^m$ has order m; all other elements of C have order $2m$.

In particular, the number of PLRs in a coset of A is 2^r if $e > 1$, and is $2^r - 1$ if $e = 1$.

Remark We worked out in Subsection 5.2 the necesary and sufficient conditions for $e = 1$.

Proposition 6.11 *Suppose that $n > 2$, and let $\lambda(n) = 2m$. The intersection of the power class and the fraternity containing a PLR x of n is equal to $\{x\}$ if m is odd, and is $\{x, x^{m+1}\}$ if m is even. The number of fraternities is divisible by $\phi(\lambda(n))$ if m is odd, and by $\phi(\lambda(n))/2$ if m is even.*

Proof The elements of the power class of x have the form x^d, where $\gcd(d, \lambda(n)) = 1$. Now x and x^d are fraternal if and only if $x^{2(d-1)} \equiv 1$, which holds if and only if $d = 1 + \lambda(n)/2 = m + 1$. Now $\gcd(m+1, 2m) = 1$ if and only if m is even.

The last part follows from the fact that each power class has cardinality $\phi(\lambda(n))$.

Corollary 6.12 *The number of fraternities of PLRs is even, unless n divides 240, in which case there are three fraternities if $n = 80$ or $n = 240$, and 1 otherwise.*

Proof Suppose first that $\lambda(n) \equiv 2 \pmod 4$. Then either $\lambda(n) = 2$, or $\phi(\lambda(n))$ is even. In the first case, n divides 24, and every PLR satisfies $x^2 \equiv 1$, so there is just one fraternity. In the second, the number of fraternities meeting each power class is even.

Now suppose that $\lambda(n) \equiv 0 \pmod 4$. Then either $\lambda(n) = 4$, or $\phi(\lambda(n))$ is also divisible by 4. In the first case, n divides 240, and a finite amount of checking establishes the result. In the second, the number of fraternities meeting every power class is even.

Examples For $n = 40$ we have $s = 3$ and $e = 2$, so the size of a fraternity is $2^3 = 8$; all PLRs belong to a single fraternity

For $n = 56$, we have $s = 3$ and $e = 1$, so the size of a fraternity is $2^3 - 1 = 7$; the 14 PLRs fall into two fraternities. Since $\lambda(n) = 6$, one fraternity contains the inverses of the elements of the other.

For $n = 75$, we have $s = 2$ and $e = 2$, so the size of a fraternity is 4; the 16 PLRs fall into four fraternities.

7 Some special structures for the units

Theorem 7.1 *Suppose that the Smith canonical form of $U(n)$ is*

$$U(n) \cong C_{\lambda(n)} \times \cdots \times C_{\lambda(n)} \qquad (r \text{ factors}),$$

with $r > 1$. Then either

(a) $n = 8$, 12 or 24; or

(b) $n = p^a(p^a - p^{a-1} + 1)$ or $2p^a(p^a - p^{a-1} + 1)$, where p and $p^a - p^{a-1} + 1$ are odd primes.

In particular, $r \leq 3$, and $r = 3$ only in the case $n = 24$.

Proof Suppose first that $\phi(n)$ is a power of 2. Then $n = 2^a p_1 \cdots p_s$, where $p_1, \ldots, p_s$ are distinct Fermat primes, and $U(n) \cong U(2^a) \times C_{p_1-1} \times \cdots \times C_{p_s-1}$. Since all the cyclic factors have the same order, either $s = 0$, or $s = 1$, $p_1 = 3$; the cases where there are more than one cyclic factor are $n = 8$, 12 and 24.

Now suppose that $\phi(n)$ is not a power of 2; let n have s odd prime factors. The number of 2-power cyclic factors of $U(n)$ is s, plus one or two if the power of 2 dividing n is 4 or at least 8, respectively; the number of cyclic factors of odd prime power order is at most s. So n must be odd or twice odd; we may assume that n is odd. We have $s = r$.

Let $n = p_1^{a_1} \cdots p_r^{a_r}$. The decomposition

$$U(n) \cong U(p_1^{a_1}) \times \cdots \times U(p_r^{a_r})$$

must coincide with the Smith normal form of $U(n)$, so we must have

$$p_1^{a_1-1}(p_1-1) = \cdots = p_r^{a_r-1}(p_r-1).$$

Clearly $a_i = 1$ can hold for at most one value of i. But, if $a_i > 1$, then p_i is the largest prime divisor of $p_i^{a_i-1}(p_i-1)$. We conclude that $r = 2$ and that (assuming $p = p_1 < p_2$ and $a = a_1$) we have $p_2 = p^{a-1}(p-1)+1$ and $a_2 = 1$.

The odd numbers $n < 1\,000\,000$ occurring in case (b) of the theorem are

$$\begin{aligned} 63 &= 9 \cdot 7, \\ 513 &= 27 \cdot 19, \\ 2\,107 &= 49 \cdot 43, \\ 12\,625 &= 125 \cdot 101, \\ 26\,533 &= 169 \cdot 157, \\ 39\,609 &= 243 \cdot 163, \text{ and} \\ 355\,023 &= 729 \cdot 487. \end{aligned}$$

There are various possibilities for the structure $U(n) \cong C_a \times C_{\lambda(n)} \times C_{\lambda(n)}$ with $a \mid \lambda(n)$; for example, for odd n, we have

$$\begin{aligned} n = 3 \cdot 7^2 \cdot 43, &\quad U(n) \cong C_2 \times C_{42} \times C_{42}; \\ n = 3^2 \cdot 7^2 \cdot 43, &\quad U(n) \cong C_6 \times C_{42} \times C_{42}; \\ n = 3 \cdot 5^3 \cdot 101, &\quad U(n) \cong C_2 \times C_{100} \times C_{100}; \\ n = 11 \cdot 5^3 \cdot 101, &\quad U(n) \cong C_{10} \times C_{100} \times C_{100}. \end{aligned}$$

For even n, the values $n = 4 \cdot p^j \cdot (p^{j-1}(p-1)+1)$, where p and $p^{j-1}(p-1)+1$ are odd primes, give examples.

Problem 5 Can the multiplicity of $\lambda(n)$ as the order of an invariant factor of $U(n)$ be arbitrarily large? Again, numbers of the form $n = \lambda^*(m)$ are particularly fruitful here: for $n = \lambda^*(157\,080)$, a number with 122 digits, the multiplicity of $C_{157\,080}$ in the Smith normal form of $U(n)$ is 16.

This problem is related to Problem 3 as follows:

Proposition 7.2 *Suppose that the multiplicity of $\lambda(n)$ as an invariant factor of $U(n)$ is $d > 1$. Then the number $F(n)$ of primitive lambda-roots of n saatisfies*

$$F(n)/\phi(n) \geq \zeta(d)^{-1} \geq 1 - 1/2^{d-1},$$

where ζ is the Riemann zeta-function.

Proof We use the formula of Theorem 6.7. The number $m(p)$ is at least d for each prime dividing $\phi(n)$, so we have:

$$\begin{aligned}
F(n)/\phi(n) &= \prod_{p|\phi(n)} (1 - 1/p^{m(p)}) \\
&\geq \prod_{p|\phi(n)} (1 - 1/p^{d}) \\
&\geq \prod_{p} (1 - 1/p^{d}) \\
&= \zeta(d)^{-1} \\
&\geq \left(1 + \frac{1}{2^d} + \frac{1}{2^d} + \frac{1}{4^d} + \frac{1}{4^d} + \frac{1}{4^d} + \frac{1}{4^d} + \frac{1}{8^d} + \cdots\right)^{-1} \\
&= \left(\frac{1}{1 - 1/2^{d-1}}\right)^{-1} \\
&= 1 - 1/2^{d-1}.
\end{aligned}$$

(In the third line we have the product over all prime numbers p. In the fourth line we have used the Euler product formula for the Riemann zeta function.)

8 Negating and non-negating PLRs

Suppose that x is a primitive λ-root. We can ask:

(a) Is $-x$ also a primitive λ-root?

(b) If so, is $-x$ in the same power class as x?

In an abelian group, the order of the product of two elements divides the lcm of the orders of the factors. Since $x = (-1)(-x)$, we see that, if x is a PLR, then the order of $-x$ must be either $\lambda(n)$ or $\lambda(n)/2$, and the latter holds only if $\lambda(n)/2$ is odd. Thus, we have:

Proposition 8.1 *Let x be a primitive λ-root of n, where $n > 2$. Then $-x$ is also a primitive λ-root if either n has a prime factor congruent to $1 \pmod 4$, or n is divisible by 16.*

Note that, if $-x$ has order $\lambda(n)/2$, then we have

$$\langle x \rangle = \langle -1 \rangle \times \langle -x \rangle,$$

so that -1 and $-x$ are both powers of x in this case. Conversely, if $\lambda(n)/2$ is odd and -1 is a power of x, then $-x$ is an even power of x and so has order $\lambda(n)/2$. Thus, in the cases excluded in the above Proposition, we see that $-x$ is a primitive λ-root if and only if -1 is not a power of x. Necessary and sufficient conditions for this are given in Subsection 8.3 below.

Definition The PLR x of n is *negating* if -1 is a power of x, and *non-negating* otherwise.

Now clearly $-x$ is a power of x if and only if x is negating.

Corollary 8.2 *Suppose that $\lambda(n)$ is twice an odd number (so that n is not divisible by 16 or by any prime congruent to $1 \pmod 4$).*

(a) If $n = 4$ or $n = 2p^a$ for some prime $p \equiv 3 \pmod 4$, then for every primitive λ-root x, we have that $-x$ is not a primitive λ-root.

(b) Otherwise, some primitive λ-roots x have the property that $-x$ is a primitive λ-root, and some have the property that it is not.

The PLR x is negating if and only if -1 belongs to the cyclic group generated by x; so we see:

Proposition 8.3 *If a primitive λ-root is negating, then so is every element of its power class.*

In the next two sections, after a technical result, we will determine for which n there exist negating PLRs, and count them. We conclude this section with some open problems.

Problem 6 Is it possible for -1 to be the only unit which is not a power of a PLR? More generally, which units can fail to be powers of PLRs?

Problem 7 For which values of n is it true that the product of two PLRs is never a PLR? (This holds for $n = 105$, for example.) For other values of n, can we characterise (or count) the number of pairs (x_1, x_2) of PLRs whose product is a PLR?

8.1 A refined canonical form

While the invariant factors and the elementary divisors of a finite abelian group are uniquely determined, the actual cyclic factors are not in general. This freedom is used in the following result, which is useful in the construction of terraces. This result lies at the opposite extreme from the negating PLRs we have considered; it shows that there is a unit generating a cyclic factor of $U(n)$ of smallest possible 2-power order which has -1 as a power.

Theorem 8.4 *Let 2^m be the smallest elementary divisor of $U(n)$ for the prime 2. Then $U(n) = A \times B$, where $A \cong C_{2^m}$ and $-1 \in A$. In particular,*

(a) $U(n)$ can be written in Smith canonical form so that the smallest cyclic factor contains -1;

(b) $U(n)$ can be written in primary canonical form so that the smallest cyclic factor of 2-power order contains -1.

Proof The case where n is divisible by 4 can be dealt with by a simple constructive argument. In this case, we have $2^m = 2$; all units are odd, and those congruent to 1 mod 4 form the subgroup B, while A is generated by -1.

Next, suppose that n is odd. In the decomposition of $U(n)$ into cyclic groups given by Theorem 4.1, the element -1 has order 2 in every factor. So, if we refine this decomposition to the primary canonical form, the element -1 has order 2 in every 2-power factor.

Let $C_{2^{m_1}} \times \cdots \times C_{2^{m_r}}$ be the 2-part of $U(n)$, where $m = m_1$. Let x_i be the generator of the ith factor. Then

$$-1 = x_1^{2^{m_1-1}} \cdots x_r^{2^{m_r-1}}.$$

Now replace x_1 by

$$y_1 = x_1 x_2^{2^{m_2-m_1}} \cdots x_r^{2^{m_r-m_1}}.$$

Then $y_1, x_2, \cdots x_r$ generate cyclic groups also forming the 2-part of the primary decomposition of $U(n)$; and we have

$$-1 = y_1^{2^{m_1-1}},$$

as required.

Finally, if n is odd, then $U(2n) \cong U(n)$, and the natural isomorphism maps -1 to -1. So the case where n is twice an odd number follows from the case where n is odd.

8.2 Generators differing by 1

As an example of the preceding result, consider $n = 275 = 5^2 \cdot 11$. The Smith canonical form of $U(n)$ is $C_{10} \times C_{20}$. If we take 139 and 138 as generators of the respective cyclic factors, then $139^5 = -1$. Is it just coincidence that the two generators differ by 1 in this case?

We cannot answer this question completely, but in some cases where $U(n)$ has just two cyclic factors, we can show that generators differing by 1 must exist, keeping the property that -1 lies in the smaller cyclic group.

We consider the case where $n = pq$, with p and q distinct odd primes. Then $U(n) \cong C_{\xi(n)} \times C_{\lambda(n)}$, where $\lambda(n)$ and $\xi(n)$ are the least common multiple and greatest common divisor, respectively, of $p-1$ and $q-1$. We have seen that it is possible to choose a generator x of the first factor such that -1 is a power of x (necessarily $-1 = x^{\xi(n)/2}$). Under suitable hypotheses, we can assume also that $x+1$ generates the second factor.

We consider first the case where $\xi(n) = 4$. In this case, both p and q must be congruent to 1 mod 4, and at least one must be congruent to 5 mod 8. Moreover, we have $x^2 \equiv -1 \pmod{pq}$.

Theorem 8.5 *Let p and q be primes congruent to $5 \pmod 8$, such that $\gcd(p-1, q-1) = 4$. Suppose that 2 is a primitive root of both p and q. Then there exists*

a number x such that

$$U(pq) = \langle x \rangle \times \langle x+1 \rangle = \langle x \rangle \times \langle x-1 \rangle,$$

where the cyclic factors have orders $\xi(pq) = 4$ and $\lambda(pq) = (p-1)(q-1)/4$, and the first factor contains -1. There are two such values, one the negative of the other modulo pq.

Proof We have

$$2^{(p-1)(q-1)/8} = \left(2^{(p-1)/2}\right)^{(q-1)/4} \equiv (-1)^{\text{odd}} = -1 \pmod{p},$$

and similarly mod q; so

$$2^{(p-1)(q-1)/8} \equiv -1 \pmod{pq}.$$

Now there are four solutions of $x^2 \equiv -1 \pmod{pq}$, namely $\pm x_1$ and $\pm x_2$, where

$$\begin{aligned} x_1 &\equiv a \pmod{p}, & x_1 &\equiv b \pmod{q}, \\ x_2 &\equiv a \pmod{p}, & x_2 &\equiv -b \pmod{q}, \\ a^2 &\equiv -1 \pmod{p}, & b^2 &\equiv -1 \pmod{q}. \end{aligned}$$

So we can choose x such that $x^2 \equiv -1$ and $x \not\equiv \pm y \pmod{pq}$, where $y = 2^{(p-1)(q-1)/16}$.

Certainly x has order 4. Also we have

$$(x+1)^2 = x^2 + 2x + 1 \equiv 2x \pmod{pq},$$

and

$$(2x)^{(p-1)(q-1)/16} \equiv (\pm y)(\pm x) \pmod{pq},$$

whence $(2x)^{(p-1)(q-1)/8} \equiv 1 \pmod{pq}$. Clearly every odd divisor of $p-1$ or $q-1$ divides the order of $2x$, so $2x$ has order $(p-1)(q-1)/8$, and $x+1$ has order $(p-1)(q-1)/16$. Moreover, the subgroup generated by $x+1$ does not contain -1 (since its unique element of order 2 is $\pm xy$), so it is disjoint from the subgroup generated by x. Thus, these two subgroups generate their direct product, which (by considering order) is the whole of $U(pq)$.

The argument for $x-1$ is the same. Alternatively, note that we can replace x by $-x$ in the argument, giving

$$U(pq) = \langle -x \rangle \times \langle -x+1 \rangle = \langle x \rangle \times \langle x-1 \rangle.$$

The final statement in the theorem holds because if we chose $x = \pm y$, then $(2x)^{(p-1)(q-1)/16} \equiv \pm 1$, so that either the order of $x+1$ is too small, or $-1 \in \langle x \rangle \cap \langle x+1 \rangle$.

For example, 2 is a primitive root modulo 5, 13, 29, 37 and 53, so we can use any two of these primes in the Theorem. The table gives all instances with $pq < 300$.

n	x
$65 = 5 \cdot 13$	± 18
$145 = 5 \cdot 29$	± 12
$185 = 5 \cdot 37$	± 68
$265 = 5 \cdot 53$	± 83

A similar argument works in other cases, with some modification. If $q \equiv 1 \pmod 8$, then 2 is a quadratic residue mod q, and cannot be a primitive root: its order is at most $(q-1)/2$. For $q = 17, 41, \ldots$, it happens that the order of 2 mod q is $(q-1)/2$.

Consider, for example, the case $p = 5$, $q = 17$. Now 2 has order 4 mod 5 and 8 mod 17, so $2^8 \equiv 1 \pmod{85}$ but $2^4 \equiv 16 \pmod{85}$. So $2x$ has order 8, and $(x+1)$ has order 16, if x is any solution of $x^2 \equiv -1 \pmod{85}$. Thus all four such solutions $x = \pm 13, \pm 38$ have the required property.

On the other hand, 2 has order 20 mod 41, and so $2^{10} \equiv -1 \pmod{205}$. Thus $(2x)^{10} \equiv 1 \pmod{205}$, so in this case $x+1$ has order 20, rather than 40, and the construction fails.

In general, we have the following result, whose proof follows the same lines as the case $pq = 85$.

Theorem 8.6 *Let p and q be primes with $p \equiv 5 \pmod 8$ and $q \equiv 1 \pmod{16}$, such that $\gcd(p-1, q-1) = 4$. Suppose that 2 is a primitive root of p and has order $(q-1)/2$ modulo q. Then there exists a number x such that*

$$U(pq) = \langle x \rangle \times \langle x+1 \rangle = \langle x \rangle \times \langle x-1 \rangle,$$

where the cyclic factors have orders 4 and $\lambda(pq) = (p-1)(q-1)/4$, and the first factor contains -1. There are four such values of x modulo pq, falling into two pairs $\pm x$.

Examples with $pq < 300$ are given in the next table.

n	x
$85 = 5 \cdot 17$	$\pm 13, \pm 38$
$221 = 13 \cdot 17$	$\pm 21, \pm 47$

Similar results hold in the case where $\xi(pq) = 6$. In this case our condition is $x^3 \equiv -1$. This condition permits the possibility that $x \equiv -1$ modulo one of the

primes; we exclude this, since then $x+1$ would not be a unit. Since $x^3+1 = (x+1)(x^2-x+1)$, this means that we require $x^2-x+1 \equiv 0$ modulo both p and q, so that this congruence holds modulo pq. Conversely, if $x^2 \equiv x-1 \pmod{pq}$, then x has order 6 and $-1 \in \langle x \rangle$. The following theorem is a corrected version of a theorem stated in the previous draft.

Theorem 8.7 *Let p and q be primes congruent to $7 \pmod{12}$. Assume that 3 is a negating PLR of pq. (This holds, in particular, if 3 is a primitive root of both p and q.) Assume further that there is a number x satisfying $x^2 = x-1$ such that*

1. *x is not a power of 3;*
2. *$x+1$ has even order;*
3. *$-1 \notin \langle x+1 \rangle$.*

Then $\mathbb{U}(pq) = \langle x \rangle \times \langle x+1 \rangle$, where the cyclic factors have orders $\xi(pq) = 6$ and $\lambda(pq) = (p-1)(q-1)/6$, and the first factor contains -1.

Proof The proof is similar to the proof of the preceding two results. To begin, we note that the equation $x^2 = x-1$ has four solutions in $\mathbb{Z}_{pq}$. (For, in $\mathbb{Z}_p$, it asserts that $x^2-x+1 = 0$, or x has order 6; there are two such elements, and similarly two in $\mathbb{Z}_q$, whence the conclusion follows from the Chinese Remainder Theorem.) The four elements fall into two inverse pairs.

Let $\lambda = \lambda(pq) = (p-1)(q-1)/6$, so $\lambda \equiv 6 \pmod{12}$. We note that our assumptions on 3 imply that $3^{\lambda/6}$ is an element of order 6 whose cube is -1, and is not x or x^{-1}. (Note that at least two solutions of $x^2 = x-1$ will satisfy the first condition.)

Now if x is a solution of this equation, then $x+x^{-1} = xx^{-1} = 1$, so that $(1+x)(1+x^{-1}) = 1+1+1 = 3$. Thus, $(1+x)(1+x^{-1})$ has even order, so at least one of $1+x$ and $1+x^{-1}$ has even order. So at least one element satisfies the first and second conditions.

As before, $3^{\lambda/2} = -1 = x^{\lambda/2}$, so $(3x)^{\lambda/2} = 1$. By assumption, $(3x)^{\lambda/6} \neq 1$, so $3x$ has order $\lambda/2$. Since $(x+1)^2 = 3x$, it follows that $x+1$ has order λ or $\lambda/2$. Our choice of x ensures that the order is λ. Also, we cannot have a non-identity power of $1+x$ in the subgroup $\langle x \rangle$, by assumption.

So we have the required decomposition.

Examples of the Theorem include

$$\begin{aligned}\mathbb{U}(133) &= \langle 103\rangle \times \langle 104\rangle = \langle 31\rangle \times \langle 32\rangle \\ \mathbb{U}(217) &= \langle 68\rangle \times \langle 69\rangle = \langle 150\rangle \times \langle 151\rangle \\ \mathbb{U}(301) &= \langle 136\rangle \times \langle 137\rangle = \langle 166\rangle \times \langle 167\rangle\end{aligned}$$

Remark We saw in the above proof that, with the given assumptions on p, q and 3, there is at least one element x satisfying $x^2 = x-1$ and the first and second conditions of the theorem. However, there may be no element satisfying all three.

For example, let $n = 973 = 7 \times 139$. Then 3 is a primitive root of both primes. The four solutions of $x^2 = x-1$ are 236, 738, 460, and 514; the orders of the elements $x+1$ are λ, $\lambda/2$, $\lambda/3$ and λ respectively, but each of the elements of order λ has the property that $x^{\lambda/2} = -1$.

Problem 8 Is there a more direct way of identifying numbers pq for which the conditions of the Theorem hold?

Problem 9 Find an analogous result in the case where $q \equiv 1 \pmod{12}$. We note that the conclusions of the theorem hold in several further cases, as in the next table.

n	x
$91 = 7 \cdot 13$	$17, 75$
$247 = 13 \cdot 19$	$69, 88, 160, 179$

There are also cases where the second factor is generated by $x-1$ rather than $x+1$:

n	x
$91 = 7 \cdot 13$	$12, 38$
$259 = 7 \cdot 37$	$73, 110$

Problem 10 (a) What happens for larger values of $\xi(pq)$?

(b) What happens for larger numbers of prime factors of n?

8.3 Existence of negating PLRs

The existence and number of negating PLRs of n depend on the structure of the *Sylow 2-subgroup* S of $U(n)$, the group of all units of 2-power order.

Definition An abelian group is *homocyclic* if it is the direct product of cyclic groups of the same order. The *rank* of a homocyclic abelian group is the number of cyclic factors in such a decomposition.

Theorem 8.8 *Let $n > 1$. There exists a negating PLR of n if and only if the Sylow 2-subgroup S of $U(n)$ is homocyclic. In this case, the proportion of PLRs which are negating is $1/(2^s - 1)$, where s is the rank of S.*

Proof Suppose first that S is not homocyclic. By Theorem 8.4, $U(n) = A \times B$, where A is cyclic and $-1 \in A$; and $\lambda(n)/|A|$ is even, so $a^{\lambda(n)/2} = 1$ for all $a \in A$. Thus no element of $U(n)$ has the property that its $\lambda(n)/2$ power is -1.

In the other direction, suppose that S is homocyclic. Then $U(n) = S \times T$, where T consists of the elements of odd order in $U(n)$; and a PLR of n is a product of elements of maximal order in S and T. In this case, the automorphism group of S acts transitively on the set of $2^s - 1$ elements of order 2 in S, so that each of them (and in particular, -1) occurs equally often as a power of an element of maximal order.

As a result, we see that every PLR is negating if and only if S is cyclic; this occurs if and only if $n = p^a$, $2p^a$ (for some odd prime p) or 4.

The next result, which follows immediately from the structure theorem for $U(n)$ (Theorem 4.1), thus describes when negating PLRs exist.

Theorem 8.9 *Let $n = 2^a m$ where m is odd, and let r be the number of distinct prime divisors of m. Then the Sylow 2-subgroup S of $U(n)$ is homocyclic if and only if one of the following holds:*

(a) $a \leq 1$ and, for any two primes p and q dividing m, the powers of 2 dividing $p-1$ and $q-1$ are equal. In this case the rank of S is r.

(b) $a = 2$ or $a = 3$, and every prime divisor of m is congruent to $3 \pmod 4$. In this case the rank of S is $r + a - 1$.

9 Inward and outward PLRs

Definition The PLR x of n is *inward* if $x - 1$ is a unit, and *outward* otherwise.

Like the previous property, this one is a property of power classes. This follows from a more general observation.

Proposition 9.1 *Let $x, y \in U(n)$, and suppose that x and y belong to the same power class. Then $x-1 \in U(n)$ if and only if $y-1 \in U(n)$.*

Proof Let $y = x^d$. Since $\gcd(d, \phi(n)) = 1$, there exists e such that $x = y^e$. Now

$$y - 1 = x^d - 1 = (x-1)(x^{d-1} + \cdots + 1) = (x-1)a$$

for some $a \in \mathbb{Z}_n$. Similarly, $x - 1 = (y-1)b$ for some $b \in \mathbb{Z}_n$. Thus $(x-1)ab = x - 1$. If $x-1$ is a unit, this implies that $ab = 1$, so that a is a unit and $y - 1 = (x-1)a$ is a unit; and conversely.

Corollary 9.2 *If a primitive λ-root is inward, then so is every element of its power class.*

Proposition 9.3 *(a) Every primitive λ-root of n is outward if and only if n is even.*

(b) If a primitive λ-root x is outward and negating, then n is even, and if n is divisible by 4 then $x \equiv 3 \pmod 4$.

Proof (a) If n is even, then every unit is odd, and so $x \in U(n)$ implies $x - 1 \notin U(n)$.

Conversely, suppose that n is odd. Suppose first that n is a prime power, say $n = p^a$. If $x \equiv 1 \pmod p$, then the order of x mod n is a power of p, and x is not a PLR. Thus, every PLR is inward in this case.

In general, choose x congruent to a primitive root modulo every prime power divisor of n. Then x is a PLR, and by the preceding argument, $x - 1$ is coprime to n. Thus, $x - 1 \in U(n)$, and x is inward.

(b) If x is outward and negating, then $x^d = -1$ for some d, and $x - 1$ divides $x^d - 1 = -2$. If n is odd, then -2 is a unit, and hence x is inward; so n is even. If n is divisible by 4, then x cannot be congruent to $1 \pmod 4$, since then 4 divides $x - 1$ but 4 does not divide $x^d - 1$.

We remark that whether a PLR is inward or outward does not depend only on the group-theoretic structure of $U(n)$. For example,

$$U(21) \cong U(28) \cong U(42) \cong C_2 \times C_6;$$

each of these groups has six PLRs, falling into three power classes of size 2, as in the following table.

n	Power class	Type
21	2, 11	inward non-negating
	19, 10	outward non-negating
	5, 17	inward negating
28	11, 23	outward non-negating
	5, 17	outward non-negating
	3, 19	outward negating
42	11, 23	outward non-negating
	19, 31	outward non-negating
	5, 17	outward negating

A PLR x of n is outward if and only if x is congruent to 1 modulo some prime divisor of n. In principle, the number of inward PLRs can be calculated by inclusion-exclusion over the prime divisors of n. However, we do not have a concise formula.

For example, consider the case $n = 275 = 5^2 \cdot 11$. We have $\lambda(n) = 20$ and the number of PLRs of n is 96. A unit congruent to 1 mod 5 has order dividing 5 mod 5^2 and dividing 10 mod 11, and so cannot be a PLR. A unit congruent to 1 mod 11 is a PLR if and only if it is a primitive root of 25: there are 8 such elements. So there are $96 - 8 = 88$ inward PLRs of 275.

For a more complicated example, let $n = 189 = 3^3 \cdot 7$, with $\lambda(n) = 18$. An element congruent to 1 mod 3 has order dividing 9 mod 27; to be a PLR, its order must be 9 mod 27 and 2 or 6 mod 7. An element congruent to 1 mod 7 is a PLR mod 189 if and only if it is a PLR mod 27. So the number of inward PLRs is

$$54 - 6 \cdot 3 - 6 = 30.$$

Again, we end the section with an open problem.

Problem 11 What are necessary and sufficient conditions for n to have only inward PLRs? (If n is odd and squarefree, then a necessary and sufficient condition is that $\lambda(n/p) < \lambda(n)$ for every prime divisor p of n. There are many examples of this: $n = 35, 55, 77, 95, \ldots$)

10 Perfect, imperfect and aberrant PLRs

For convenience, in this section the term "primitive lambda-root" includes "primitive root".

Definition If $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then the PLR x of n is said to be

- *perfect* if x is a PLR of $p_i^{a_i}$ for all $i = 1, \ldots, r$;
- *imperfect* if x is a PLR of $p_i^{a_i}$ for at least one but not all $i = 1, \ldots, r$;
- *aberrant* if x is not a PLR of $p_i^{a_i}$ for any of the values $i = 1, \ldots, r$.

Trivially, if $r = 1$, then any PLR of n is perfect. From now on we assume that $r \geq 2$. Also, of course, if p_i is odd then a PLR of $p_i^{a_i}$ is simply a primitive root of $p_i^{a_i}$.

If n is odd, every unit mod $2n$ is congruent to 1 mod 2 and to a unit mod n, so there is a bijection between the units modulo n and $2n$. This bijection clearly preserves the properties of being a PLR and of being perfect, imperfect or aberrant. So the numbers of PLRs in each of these three categories are the same for $2n$ as for n.

The property of being a perfect PLR is equivalent to the apparently stronger property (b) in the following result.

Theorem 10.1 *Let x be a unit modulo n. Then the following are equivalent:*

(a) x is a perfect PLR of n;

(b) x is a PLR of m, for every divisor m of n;

(c) x is a perfect PLR of m, for every divisor m of n.

Proof Clearly (c) implies (b) and (b) implies (a). So suppose that (a) holds, with $n = p_1^{a_1} \cdots p_r^{a_r}$. Then x is a PLR of $p_i^{a_i}$, for each i.

We claim that x is a PLR of p_i^b, for all i and all b with $0 < b \leq a_i$. This is because the natural homomorphism from $U(p^c)$ to $U(p^{c-1})$ has kernel of order p if $c > 1$, so the order of x mod p^{c-1} is at least a fraction $1/p$ of its order mod p^c. (Compare the proof of Theorem 5.2(a).) Now "downward induction" establishes the claim.

But now, by definition, x is a perfect PLR of m for every divisor m of n, and we are done.

Perfect PLRs always exist: if x_i is a PLR of $p_i^{a_i}$ for $i = 1, \ldots, r$, then the Chinese Remainder Theorem guarantees us a solution of the simultaneous congruences $x \equiv x_i \pmod{p_i^{a_i}}$, and clearly x is a PLR of n. This argument allows us to count the number of perfect PLRs of n: this number is simply the product of the numbers of PLRs of $p_i^{a_i}$ for $i = 1, \ldots, r$.

Theorem 10.2 *Let n be odd. Then any perfect PLR of n is an inward PLR.*

Proof A number congruent to 1 mod p_i cannot be a PLR of $p_i^{a_i}$ for odd p_i, since its order is a power of p_i. Hence, if x is a PLR of n with n odd, then $x \not\equiv 1 \pmod{p_i}$ for $i = 1, \ldots, r$. This shows that $x-1$ is not divisible by any of $p_1, \ldots, p_r$, so that $x-1$ is a unit mod n. (This is the same as the proof of Proposition 9.3(a).)

Theorem 10.3 *If a PLR x of n is perfect, then so is every member of its power class. The same holds with "imperfect" or "aberrant" replacing "perfect".*

Proof Suppose that x is a perfect PLR of n, and let y belong to the power class of x. Then each of x and y is congruent to a power of the other mod n. It follows that each is a power of the other mod $p_i^{a_1}$, so that x and y have the same order mod $p_i^{a_i}$; thus, if one is a PLR of $p_i^{a_i}$, then so is the other.

Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. We say that the prime power $p_i^{a_i}$ is *essential* in n if the following holds: for every prime power q^b such that q^b exactly divides $\lambda(p_i^{a_i})$, and for all $j \neq i$, it holds that q^b does not divide $\lambda(p_j^{a_j})$. If n is twice an odd number, then 2 is (vacuously) essential in n. Apart from this, there can be at most one essential prime power, since, if $p_i^{a_i} > 2$ is essential, then the power of 2 dividing $\lambda(p_i^{a_i})$ is higher than that dividing $\lambda(p_j^{a_j})$ for $j \neq i$.

If $p_i^{a_i}$ is essential in n, then any PLR of n is obviously a PLR of $p_i^{a_i}$, and conversely. Thus, we have the following result:

Theorem 10.4 *Every PLR of n is perfect if and only if n is a prime power or twice a prime power.*

In the following table, PLRs from different power classes are separated by semi-colons, and negating PLRs are asterisked.

n	perfect PLRs	imperfect PLRs	aberrant PLRs
15	2, 8	7, 13	—
21	5^*, 17^*	2, 11; 10, 19	—
35	3, 12, 17, 33	2, 18, 23, 32	—
63	5^*, 38^*; 47^*, 59^*	2, 32; 10, 19; 11, 23; 17^*, 26^*; 20^*, 41^*; 29, 50; 31, 61; 40, 52	13, 34; 44, 53

We turn now to the existence question for aberrant PLRs. The answer is somewhat elaborate and depends on the structure of an auxiliary coloured hypergraph, which we now construct.

Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. The vertices of the hypergraph $H(n)$ are indexed by the primes $p_1, \ldots, p_n$. The edges (to be defined in a moment) are indexed by the prime divisors of $\lambda(n)$.

We say that a prime divisor q of $\lambda(n)$ *occurs maximally* in $\lambda(p_i^{a_i})$ if the largest power of q dividing $\lambda(p_i^{a_i})$ is the same as the largest power of q dividing $\lambda(n)$. Now we colour the vertices p_i with three colours as follows:

- p_i is red if every prime divisor of $\lambda(p_i^{a_i})$ occurs maximally there;
- p_i is green if some but not all prime divisors of $\lambda(p_i^{a_i})$ occurs maximally there;
- p_i is blue if no prime divisor of $\lambda(p_i^{a_i})$ occurs maximally there.

The edge indexed by the prime q is incident with all vertices p_i for which q occurs maximally in $\lambda(p_i^{a_i})$. Thus, the blue vertices are isolated. Note that an edge of the hypergraph may be incident with just one vertex.

For example, let $n = 63 = 9 \cdot 7$. We have $\lambda(63) = \lambda(9) = \lambda(7) = 6$; the graph $H(63)$ has two vertices labelled 3 and 7, both red, and two edges labelled 2 and 3, each incident with both the vertices. Since this graph is a cycle, the following theorem guarantees that aberrant PLRs exist for $n = 63$.

Theorem 10.5 *Let n be a positive integer. Then an aberrant PLR of n exists if and only if every connected component of the hypergraph $H(n)$ contains either a non-red vertex or a cycle.*

Proof Let x be a PLR of n. Then, for every prime q dividing $\lambda(n)$, there exists some p_i such that q occurs maximally in $\lambda(p_i^{a_i})$ and the order of x modulo $p_i^{a_i}$ is divisible by this maximal power of q. Thus, each edge q of the hypergraph must contain at least one representative vertex p_i for which this holds.

Suppose that the vertex p_i is blue. Choosing x to be congruent to a PLR mod $n/p_i^{a_i}$ and to 1 mod $p_i^{a_i}$, we see that x is aberrant mod n if and only if it is aberrant mod $n/p_i^{a_i}$. So we can ignore the blue primes.

Now suppose that a connected component contains either a green prime p_j, or a cycle $(p_{i_1}, q_1, p_{i_2}, \ldots, p_{i_m}, q_m, p_{i_1})$. In the case of the cycle, let p_{i_k} be the representative of q_k for $i = 1, \ldots, m$. Then choose a representative for all other cycles which is at least distance to the green prime or the cycle in the hypergraph. Now choose x so that its order mod $p_i^{a_i}$ is the product of the appropriate powers of q for all edges q represented by p_i. Then the order of x is divisible by the correct

power of each prime q indexing an edge of the component, but x is not a PLR of $p_i^{a_i}$ for any prime p_i in the component.

Now suppose that a component is acyclic and has only red vertices. We claim that, if a representative vertex is chosen for each edge, then some vertex must represent every edge containing it. For suppose we have a minimal counterexample. Choose a vertex lying on a single edge, and remove this vertex (by assumption, it is not the representative of its edge). By minimality, the hypergraph obtained by deleting this edge has a vertex which is the representative of every edge containing it, contrary to assumption.

Thus, if there is a component with this property, then every PLR of n must be a PLR of $p_i^{a_i}$ for some vertex p_i in this component, and x is not aberrant.

This completes the proof.

Corollary 10.6 *If $n = p^j(p^{j-1}(p-1)+1)$, where $j > 1$ and p and $p^{j-1}(p-1)+1$ are odd primes, then n has aberrant PLRs.*

For another example, let $n = 741 = 3 \cdot 13 \cdot 19$. In the graph $G(n)$, the prime 3 is blue while 13 and 19 are green; and the edges labelled 2 and 3 are incident with single vertices 13 and 19 respectively. Choosing x congruent to 1 mod 3, to an element of order 4 mod 13, and to an element of order 13 mod 19, we obtain an aberrant PLR of n.

Problem 12 Find families of integers n for which aberrant PLRs exist.

Problem 13 Count the aberrant PLRs of n. (This problem will not have a simple answer unless our characterisation of the values of n for which aberrant PLRs exist can be substantially improved!)

10.1 Deeply aberrant and nearly perfect PLRs

We can strengthen the concept of an aberrant PLR as follows.

Definition If $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then the PLR x of n is said to be *deeply aberrant* if x is not a PLR of p_i for any of the values $i = 1, \ldots, r$.

Thus, a deeply aberrant PLR is aberrant. Note that deeply aberrant PLRs cannot exist for even n.

Problem 14 Count the deeply aberrant PLRs of n.

We can also refine the notion of an imperfect PLR as follows.

Definition Let $n = p_1^{a_1} \cdots p_r^{a_r}$, and let x be a PLR of n which is not perfect. We say that x is *nearly perfect* if it is a PLR of p_i for all $i = 1, \ldots, r$.

Problem 15 Count the nearly perfect PLRs of n.

We note that, if n is even, then any unit is congruent to 1 mod 2, so the condition for the prime 2 is vacuous. Moreover, if n is squarefree, there are no nearly perfect PLRs of n. The proportion of units mod n which are congruent to primitive roots modulo each prime divisor of n is the product, over all prime divisors p of n, of the proportion of units mod p which are primitive roots. However, these elements may not all be PLRs.

For example, the number of perfect or nearly perfect PLRs of 63 is

$$\phi(63) \times \frac{1}{2} \times \frac{2}{6} = 6;$$

as we have seen, there are four perfect PLRs, and hence two nearly perfect PLRs. (In this case all such elements are PLRs, since $\lambda(63) = \lambda(7) = 6$.)

Proposition 10.7 *A nearly perfect PLR of n cannot be aberrant.*

Proof Suppose that n is a nearly perfect but aberrant PLR of n. Then each prime divisor of n must occur to a power higher than the first, since the requirements "not a PLR of $p_i^{a_i}$" and "a primitive root of p_i" conflict if $a_i = 1$. Let p be the largest prime divisor of n, and suppose that p^a exactly divides n. Suppose first that p is odd. Then p^{a-1} exactly divides $\lambda(n)$, so a PLR of n has order divisible by p^{a-1} mod p^a. But, if it is nearly perfect, then its order mod p^a is also divisible by $p-1$, and hence it is a primitive root mod p^a, and so is not aberrant. On the other hand, if $p = 2$, then n is a power of 2, and any PLR of n is perfect by definition.

Note also that, if n is odd, then any nearly perfect PLR of n is inward; in other words, Theorem 10.2 extends to nearly perfect PLRs, with the same proof.

The following table gives the nearly perfect PLRs of $n = 9p$ where p is prime and $\xi(n) = 6$ (that is, $p \equiv 1 \pmod 6$). They are negating if $p \equiv 3 \pmod 4$ and non-negating if $p \equiv 1 \pmod 4$.

n	nearly perfect PLRs
$63 = 3^2 \cdot 7$	$\{17, 26\}$
$117 = 3^2 \cdot 13$	$\{80, 71, 89, 98\}$
$171 = 3^2 \cdot 19$	$\{53, 116, 89, 98, 143, 71\}$
$279 = 3^2 \cdot 31$	$\{17, 260, 53, 251, 269, 179, 88, 197\}$

11 Further properties of PLRs

If x is an inward PLR of n, then the $2\lambda(n)$ differences

$$\pm(x^i - x^{i-1}), \quad (i = 1, 2, \ldots, \lambda(n)),$$

are all units, and consist of $2\lambda(n)$ different elements if x is non-negating, or $\lambda(n)$ elements each repeated twice if x is negating.

This property shows the importance (for constructions such as the motivating terrace in Section 1) of PLRs that are both inward and non-negating.

Definition The PLR x of n is *strong* if it is inward and non-negating. (Clearly this requires n to be odd, and not a prime power.)

It follows from Proposition 8.3 and Corollary 9.2 that, if a PLR is strong, then so is every PLR in the same power class.

Problem 16 Is it true that strong PLRs exist for all odd n with $\xi(n) > 1$, in other words, all odd numbers which are not prime powers?

This question has an affirmative answer for $n \leq 20\,000$.

Problem 17 Count the strong PLRs of n.

Problem 18 For which odd n such that $U(n) \cong C_{\lambda(n)} \times C_{\lambda(n)}$, can $U(n)$ be generated by two strong PLRs?

Note that the values of n for which $U(n) \cong C_{\lambda(n)} \times C_{\lambda(n)}$ are those given by Theorem 7.1(b), namely $n = p^a(p^a - p^{a-1} + 1)$, where p and $p^a - p^{a-1} + 1$ are odd primes and $a > 1$.

We give some examples. For $n = 63 = 9 \cdot 7$, $U_n \cong C_6 \times C_6$, and this group can be generated by the two PLRs 2 (which is strong) and 13 (which is outward and non-negating). However, it is not possible to choose two strong PLRs which generate the group.

For the next value of n, namely $n = 513 = 27 \cdot 19$, it is also not possible to find two strong PLRs generating $U(n)$, However, for $n = 2107 = 49 \cdot 43$, both 2 and 6 are strong PLRs, and they do generate $U(n)$.

Definition Let x be a strong PLR of n. Then x is called *self-seeking* if $x-1 = \pm x^d$ for some integer d. Note that x is self-seeking if and only if the set $X = \{x^i : i = 0,1,\ldots,\lambda(n)-1\}$ of powers of x is equal to one of the two sets $A = \{x^i - x^{i-1} : i = 1,2,\ldots,\lambda(n)\}$ or its negative $B = \{x^{i-1} - x^i : i = 1,2,\ldots,\lambda(n)\}$. We say that x is *self-avoiding* otherwise.

Proposition 11.1 *If a self-avoiding strong PLR exists then* $\xi(n) > 2$.

Proof If x is strong then each of the sets X, A, B consists of units; X is the subgroup generated by x, and A and B are cosets of X. Clearly, if $\xi(n) = 1$, there are only $\lambda(n)$ units, so all three sets must be equal. Since x is strong, -1 is not a power of x, so the sets A and B are disjoint (for $x^i - x^{i-1} = x^{j-1} - x^j$ implies $x^{i-j} = -1$); so one of them must be equal to X if $\xi(n) = 2$.

Unlike what we have seen for other properties of PLRs, it is possible for all, some, or none of the elements of a power class of PLRs to be self-seeking. For $n = 65$, the powers of the PLRs ± 3 are:

3	1	3	9	27	16	48	14	42	61	53	29	22
-3	1	62	9	38	16	17	14	23	61	12	29	43

Thus the power class $\{3,48,42,22\}$ consists of self-avoiding elements, while the power class $\{62,17,23,43\}$ consists of self-seeking elements. (For example, $61 = 62^8$.)

For $n = 91$, the strong PLRs 2 and 32 come from the same power-class; successive powers are:

2	1	2	4	8	16	32	64	37	74	57	23	46
32	1	32	23	8	74	2	64	46	16	57	4	37

The power class is $\{2,32,37,46\}$; 2 and 46 are self-seeking but the other two are self-avoiding.

Problem 19 What conditions must hold for the product of two strong PLRs of n to be a PLR of n? If $\xi(n) > 2$, is it possible for both, one or neither of the PLRs to be self-seeking?

Problem 20 Under what circumstances can the product of two strong PLRs of n be itself a strong PLR of n? Is it possible for both, one or neither of the PLRs to be self-seeking?

The smallest value of n for which this can occur is $n = 455$, where 18, 19 and $18 \cdot 19 = 342$ are all strong PLRs. None of these three is self-seeking.

For the value $n = 1771$, the numbers 39, 1768 and $39 \cdot 1768 = 1654$ are all self-seeking PLRs. This is the smallest value of n for which this can occur.

12 Tables of PLRs

We conclude with tables giving information about the smallest PLRs.

12.1 PLRs for composite odd multiples of 3

n	$\phi(n)$	$\lambda(n)$	$2 =$ PLR?	$-2 =$ PLR?	minPLR > 3
15	8	4	√	√	7
21	12	6	√	√	5
33	20	10	√	–	5
39	24	12	√	√	7
45	24	12	√	√	7
51	32	16	–	–	5
57	36	18	√	–	5
63	36	6	√	√	5
69	44	22	√	√	5
75	40	20	√	√	8
87	56	28	√	√	8
93	60	30	–	–	11
99	60	30	√	–	5
105	48	12	√	√	17
111	72	36	√	√	5
117	72	12	√	√	5
123	80	40	–	–	7
129	84	42	–	–	5
135	72	36	√	√	7
141	92	46	√	√	5
147	84	42	√	√	5
153	96	48	–	–	5
159	104	52	√	√	5
165	80	20	√	√	7
171	108	18	√	–	5
177	116	58	√	–	5
183	120	60	√	√	7
189	108	18	√	√	5
195	96	12	√	√	7
201	132	66	√	–	7
207	132	66	√	√	5
213	140	70	√	√	7
219	144	72	–	–	5
225	120	60	√	√	13
231	120	30	√	√	5
237	156	78	√	√	5
249	164	82	√	–	5
255	128	16	–	–	7
261	168	84	√	√	11
267	176	88	–	–	7
273	144	12	√	√	5
279	180	30	√	√	11
285	144	36	√	√	13
291	192	96	–	–	5
297	180	90	√	–	5

12.2 PLRs for composite odd non-multiples of 3

n	$\phi(n)$	$\lambda(n)$	PLR?				minPLR
			2	-2	3	-3	>3
35	24	12	√	√	√	√	12
55	40	22	√	√	√	√	7
65	48	12	√	√	√	√	6
77	60	30	√	√	√	√	5
85	64	16	—	—	√	√	6
91	72	12	√	√	—	—	5
95	72	36	√	√	√	√	13
115	88	44	√	√	√	√	7
119	96	48	—	—	√	√	5
133	108	18	√	√	√	—	5
143	120	60	√	√	—	—	6
145	112	28	√	√	√	√	7
155	120	60	—	—	√	√	7
161	132	66	—	√	√	√	5
175	120	60	√	√	√	√	12
185	144	36	√	√	√	√	7
187	160	80	—	—	√	√	5
203	168	84	√	√	√	√	10
205	160	40	—	—	—	—	6
209	180	90	√	—	√	√	6
215	168	84	—	—	√	√	12
217	180	30	—	√	√	—	10
221	192	48	—	—	√	√	6
235	184	92	√	√	√	√	7
245	168	84	√	√	√	√	12
247	216	36	√	√	—	—	5
253	220	110	√	√	—	√	5
259	216	36	√	√	—	—	5
265	208	52	√	√	√	√	7
275	200	20	√	√	√	√	7
287	240	120	—	—	—	—	11
295	232	116	√	√	√	√	7
299	264	132	√	√	—	—	6

References

[1] I. Anderson and N. J. Finizio, Many more Z-cyclic whist tournaments, *Congressus Numerantium* **94** (1993), 123-129.

[2] I. Anderson and D. A. Preece, Locally balanced change-over designs, *Utilitas Mathematica* **62** (2002), 35–39.

[3] I. Anderson and D. A. Preece, Power-sequence terraces for $\mathbb{Z}_n$ where n is an odd prime power, *Discrete Mathematics* **261** (2003), 31–58.

[4] D. M. Burton, *Elementary Number Theory*, Wm. C. Brown, Dubuque, IA, USA, 1988.

[5] C. Caldwell, *The Prime Glossary*, http://primes.utm.edu/glossary/home.php

[6] R. D. Carmichael, Note on a new number theory function, *Bull. Amer. Math. Soc.* **16** (1909–10), 232–238.

[7] R. D. Carmichael, Generalizations of Euler's ϕ-function, with applications to Abelian groups, *Quart. J. Math.* **44** (1913), 94–104.

[8] P. Erdős, C. Pomerance and E. Schmutz, Carmichael's lambda-function, *Acta Arith.* **58** (1991), 363–385.

[9] GAP homepage, http://www-gap.dcs.st-and.ac.uk/~gap/

[10] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (5th edition), Clarendon Press, Oxford, 1979.

[11] B. Hartley and T. O. Hawkes, *Rings, Modules and Linear Algebra*, Chapman and Hall, London, 1970.

[12] W. J. LeVeque, *Topics in Number Theory*, Vol. I, Addison-Wesley, Reading, MA, USA, 1956.

[13] Shuguang Li, Artin's conjecture on average for composite moduli, *J. Number Theory* **84** (2000), 93–118.

[14] W. Sierpiński, *Elementary Theory of Numbers* (transl. A. Hulanicki), Panstwowe Wydawnictwo Naukowe, Warszawa, 1964.

[15] N. J. A. Sloane and S. Plouffe, *On-line Encyclopedia of Integer Sequences*, http://www.research.att.com:80/~njas/sequences/

[16] Eric W. Weisstein's *World of Mathematics*, http://mathworld.wolfram.com/

[17] A. L. Whiteman, A family of difference sets, *Illinois J. Math.* **6** (1962), 107–121.