Primitive Lambda-Roots

Peter J. Cameron and D. A. Preece

Version of January 2014
The most important examples of finite commutative rings with identity are undoubtedly the rings \( \mathbb{Z}/(n) \) of integers mod \( n \), for \( n \in \mathbb{N} \).

In the case where \( n \) is a prime number \( p \), \( \mathbb{Z}/(p) \) is a field: its non-zero elements form a multiplicative group. This group is cyclic, of order \( n - 1 \), and its generators are the primitive roots mod \( p \).

If \( n \) is not prime, then \( \mathbb{Z}/(n) \) is not a field: an element \( x \) is invertible if and only if it is coprime to \( n \), that is, \( \gcd(n, x) = 1 \). The invertible elements of \( \mathbb{Z}/(n) \) form a group \( U(n) \), the group of units mod \( n \); its order is \( \phi(n) \), where \( \phi \) is Euler’s phi-function.

If this group is cyclic, its generators are again called primitive roots. However, this is a rare event: it occurs only if \( n \) is an odd prime power, or twice an odd prime power, or 4.

To replace this, Carmichael introduced his lambda-function \( \lambda(n) \), the exponent of \( U(n) \), that is, the smallest number \( m \) such that every unit \( x \) satisfies \( x^m = 1 \). A primitive lambda-root (or PLR) is a unit whose order is \( \lambda(n) \). Clearly, primitive lambda-roots exist for all \( n \). They are the object of our study.

The role of finite fields in combinatorial constructions is well known. Our motivation is the fact that, with some ingenuity, the methods can be extended to \( \mathbb{Z}/(n) \) in some cases, with PLRs playing the role of primitive roots. The first chapter gives a couple of examples, the construction of terraces and difference sets.

Three other features of the text should be noted.

1. Our aim is expository: we begin with an account of the algebra we need, and end with a short discussion of the role of the lambda-function in the RSA cryptosystem.
2. We pose many open problems along the way. We hope that other researchers will find something to their taste here, as Thomas Müller and Jan-Christoph Schlage-Puchta have already done in one case.

3. We have implemented many of our calculations in GAP, and a file of documented GAP code accompanies the notes, to make further exploration easy.

The notes in their current form are too short for a monograph, and too long (and expository) for a research paper. Despite several discussions, we came to no firm conclusion about publication. Now that Donald has left us, I want to honour his memory by making the notes easily accessible. In the first instance I am posting them with my lecture note collection at http://cameroncounts.wordpress.com.

Peter J. Cameron
January 2014
## Contents

1 Motivation  

2 Preliminaries  
   2.1 Lagrange’s Theorem  
   2.2 Numbers and number-theoretic functions  
   2.3 Modular arithmetic  
   2.4 Primitive roots  
   2.5 Finite abelian groups  
   2.6 Some theorems on primes  

3 Carmichael’s lambda-function  
   3.1 The group of units  
   3.2 The definition  
   3.3 Denominators of Bernoulli numbers  
   3.4 $p$-rank and $p$-exponent  

4 Primitive lambda-roots  
   4.1 The definition  
   4.2 Another formula  
   4.3 Fraternities  

5 Some special structures for the units  

6 Negating and non-negating PLRs  
   6.1 Definition  
   6.2 A refined canonical form  
   6.3 Generators differing by 1  

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Motivation</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Preliminaries</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>2.1 Lagrange’s Theorem</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>2.2 Numbers and number-theoretic functions</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>2.3 Modular arithmetic</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>2.4 Primitive roots</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>2.5 Finite abelian groups</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>2.6 Some theorems on primes</td>
<td>15</td>
</tr>
<tr>
<td>3</td>
<td>Carmichael’s lambda-function</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>3.1 The group of units</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>3.2 The definition</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>3.3 Denominators of Bernoulli numbers</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>3.4 $p$-rank and $p$-exponent</td>
<td>24</td>
</tr>
<tr>
<td>4</td>
<td>Primitive lambda-roots</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>4.1 The definition</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>4.2 Another formula</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>4.3 Fraternities</td>
<td>33</td>
</tr>
<tr>
<td>5</td>
<td>Some special structures for the units</td>
<td>35</td>
</tr>
<tr>
<td>6</td>
<td>Negating and non-negating PLRs</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>6.1 Definition</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>6.2 A refined canonical form</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>6.3 Generators differing by 1</td>
<td>41</td>
</tr>
</tbody>
</table>
Contents

6.4 Existence of negating PLRs . . . . . . . . . . . . . . . . . . . 45

7 Other special types of PLR . . . . . . . . . . . . . . . . . . . 47
  7.1 Inward and outward PLRs . . . . . . . . . . . . . . . . . . . 47
  7.2 Perfect, imperfect and aberrant PLRs . . . . . . . . . . . . . 49
  7.3 Further properties of PLRs . . . . . . . . . . . . . . . . . . . 54

8 Applications to cryptography . . . . . . . . . . . . . . . . . . 57
  8.1 A number-theoretic result . . . . . . . . . . . . . . . . . . . 57
  8.2 Public-key cryptography . . . . . . . . . . . . . . . . . . . . 58
  8.3 The RSA cryptosystem . . . . . . . . . . . . . . . . . . . . . . 60

9 Tables of PLRs . . . . . . . . . . . . . . . . . . . . . . . . . . . 67

10 GAP functions for PLRs . . . . . . . . . . . . . . . . . . . . 71

Bibliography . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 79
Motivation

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

\[
\begin{array}{cccccccccccccccc}
\text{START} & 10 & 15 & 5 & 3 & 9 & 27 & 11 & 33 & 17 & 16 & 13 & 4 & 12 & 1 & 21 & 7 \\
\vdots & & & & & & & & & & & & & & & & 0 \\
\text{FINISH} & 25 & 20 & 30 & 32 & 26 & 8 & 24 & 2 & 6 & 18 & 19 & 22 & 31 & 23 & 34 & 14 & 28
\end{array}
\]

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

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

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

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

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 \textit{narcissistic half-and-half power-sequence terrace} – see \cite{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 \textit{primitive lambda-root} of 35.

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

\[
6 \ 3 \ \mid 2 \ 4 \ 8 \ 1 \ \mid 10 \ \mid 0 \ \mid 5 \ \mid 14 \ 7 \ 11 \ 3 \ \mid 12 \ 9.
\]

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 $| 2^1 \ 2^2 \ 2^3 \ 2^4 |$.
1. Motivation

(with $2^4 = 2^0 = 1$); this consists of the successive powers of 2, which is a primitive lambda-root of 15. The second, third, fourth and fifth segments of the terrace make up a Whiteman difference set [19, Theorem 1, p. 112], with unsigned differences (written under the difference set, with the element in the $i$th row being the unsigned difference of the two elements $i$ steps apart in the 0th row symmetrically above it) as follows:

<table>
<thead>
<tr>
<th></th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>1</th>
<th>10</th>
<th>0</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>7</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

The purpose of this monograph is to present the basic theory of Carmichael’s lambda-function $\lambda(n)$ (the function giving the maximum order of a unit in $\mathbb{Z}_n$) and primitive lambda-roots (units whose order is $\lambda(n)$). These concepts generalise Euler’s function and primitive roots, for which an extensive theory exists; the generalisations are much less well-known.

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 [11] or LeVeque [13], and Hartley and Hawkes [12], respectively. We are grateful to Donald Keedwell, Matt Ollis and David Rees for their comments.

The last chapter contains a suite of functions written in the language GAP [10] for computations involving Carmichael’s lambda-function and primitive lambda-roots. Throughout the text, we illustrate these and other GAP functions with examples.
In this chapter, we review briefly (but for the most part with proofs) the results we need: some number theory (including the Chinese Remainder Theorem) and the structure theorem for finite abelian groups.

2.1 Lagrange’s Theorem

We will have much to say about groups (especially abelian groups) and rings in this monograph; so we assume that the reader knows what these things are. The definitions can be found in [6], for example. We note here that all our rings will be commutative rings with identity.

Recall that the order of a group element $a$ is the smallest positive integer $s$ such that $a^s = 1$, if one exists, and otherwise is $\infty$. The subgroup generated by $a$ is the subgroup $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ of $A$.

If $a^t = 1$ then the order of $a$ divides $t$. For, if $t = sq + r$ with $0 \leq r \leq t - 1$, then $a^s = a^t = 1$, so $a^r = 1$; thus $r = 0$, by the minimality of $s$.

The order of any element of a finite group $A$ divides the order of $A$. For, if $a \in A$ has order $s$, then the distinct powers of $a$ are $a^0 = 1, a^1 = 1, a^2, \ldots, a^{s-1}$. Now define an equivalence relation on $A$ by putting $b \sim c$ if $b^{-1}c$ is a power of $a$. Each equivalence class has size $s$, so $s$ divides $|A|$.

The equivalence classes are the cosets of the subgroup generated by $a$. So this result is a special case of Lagrange’s Theorem, which asserts that the order of a subgroup of a finite group $A$ must divide the order of $A$.

As a corollary, we see that, in a group of order $n$, every element $a$ satisfies
2. Preliminaries

2.2 Numbers and number-theoretic functions

In this section we review some basic properties of the integers, including the Euler and Möbius functions and properties of the ring of integers modulo \( n \).

2.2.1 Euclid’s algorithm

Many properties of the integers, such as unique factorisation and the Chinese remainder theorem, follow from the fact that any two integers have a greatest common divisor, unique up to sign. Recall that \( d \) is a **greatest common divisor** of \( m \) and \( n \) if

- \( d \) divides both \( m \) and \( n \);
- if an integer \( e \) divides both \( m \) and \( n \), then it divides \( d \).

In other words, “greatest” refers to the order by divisibility, not the usual order.

The greatest common divisor can be calculated by **Euclid’s algorithm**, which can be defined recursively (for positive arguments \( m \) and \( n \)) as follows:

\[
\text{if } n = 0 \text{ then gcd := } m; \text{ else gcd := gcd}(n, m \mod n); \text{ fi};
\]

Here we have used the notation \( m \mod n \) for the remainder when \( m \) is divided by \( n \). Later, we will sometimes mean the congruence class mod \( n \) containing \( m \). The context should make the usage clear.

A crucial property of Euclid’s algorithm is that it can be extended to find integers \( u \) and \( v \) such that

\[ d = um + vn. \]

This is easily proved inductively using the recursive form of the algorithm. If \( n = 0 \) then we may take \( u = 1, \ v = 0 \). If \( m = nq + r \) and \( d = xn + yr \), then we may take \( u = y, \ v = x - yq \).

The greatest common divisor and the values of \( u \) and \( v \) may be computed with **GAP** using the commands \texttt{GcdInt}(\( m, n \)) and \texttt{Gcdex}(\( m, n \)) respectively. The first works as you would expect:

```
gap> GcdInt(720,2450);
10
```

The function \texttt{Gcdex} takes two integer arguments \( m, n \) and returns a record with five fields \( a, b, c, d, e \), where

\[
gcd(m, n) = a, \quad bm + cn = a, \quad dm + en = 0,
\]
and $d$ and $e$ are minimal, so that the general solution of $xm + yn = 0$ is given by

$$x = b + zd, \quad y = c + ze$$

for $z \in F$. The names of the five fields are gcd and coeff$i$ for $i = 1, 2, 3, 4$. For example,

```
gap> Gcdex(720,2450);
rec( gcd := 10, coeff1 := -17, coeff2 := 5,
    coeff3 := 245, coeff4 := -72 )
gap> Gcdex(720,2450).coeff1;
-17
gap> -17*720+5*2450;
10
```

### 2.2.2 Euler and Möbius

Two important number-theoretic functions are Euler’s function $\phi$ (sometimes called Euler’s totient), and the Möbius function $\mu$. They are defined as follows:

- $\phi(n)$ is equal to the number of integers $x$ in the set $\{0, 1, \ldots, n - 1\}$ for which $\text{gcd}(x, n) = 1$.

- $\mu(n) = \begin{cases} (-1)^r & \text{if } n \text{ is a product of } r \text{ distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$

**Proposition 2.1** If $n = p_1^{a_1} \cdots p_r^{a_r}$, where $p_1, \ldots, p_r$ are distinct primes and $a_1, \ldots, a_r > 0$, then

$$\phi(n) = n \prod_{i=1}^{r} \left( 1 - \frac{1}{p_i} \right).$$

**Proof** Let $I = \{1, \ldots, r\}$. Now $\text{gcd}(x, n) = 1$ if and only if $x$ is divisible by no prime $x_i$ for $i \in I$. If $J \subseteq I$, then the number of integers in $\{0, \ldots, n - 1\}$ divisible by the primes $p_j$ for $j \in J$ (and perhaps others) is $n/\prod_{j \in J} p_j$. So, by the Principle of Inclusion and Exclusion,

$$\phi(n) = \sum_{J \subseteq I} (-1)^{|J|} \prod_{j \in J} \frac{1}{p_j} = n \prod_{i=1}^{r} \left( 1 - \frac{1}{p_i} \right),$$

as claimed. \qed

The proof shows that, in fact,

$$\phi(n) = \sum_{m|n} m\mu(n/m). \quad (2.1)$$
On the other hand, \( \gcd(m, n) = d \) if and only if \( d \) divides both \( m \) and \( n \) and \( \gcd(m/d, n/d) = 1 \); so
\[
n = \sum_{m \mid n} \phi(m). \tag{2.2}
\]

In fact, the relation between these two equations is a special case of a more general fact, known as M"obius inversion:

**Theorem 2.2** Let \( f \) and \( g \) be functions on the positive integers. Then the following are equivalent:

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

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

**Proof** We begin with the following identity:
\[
\sum_{m \mid n} \mu(m) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}
\]

This is clear if \( n = 1 \). If \( n > 1 \), choose a prime \( p \) dividing \( n \). The terms in the sum are non-zero only if \( m \) is squarefree; and these values of \( m \) can be split into pairs \((m', m'p)\) where \( m' \) is not divisible by \( p \). The values of \( \mu \) on paired terms have opposite sign, and so cancel.

Now suppose that (b) holds. Then
\[
\sum_{m \mid n} g(m) = \sum_{m \mid n} \sum_{l \mid m} f(l) \mu(m/l) = \sum_{l \mid n} f(l) \sum_{k \mid n/l} \mu(k).
\]
(In the second equation, we have reversed the order of summation and put \( k = m/l \).) The inner sum is zero except when \( l = n \), so the value of the outer sum is \( f(n) \), as required.

The converse implication is similar and we omit it. \( \Box \)

We note one application:

**Proposition 2.3** A cyclic group of order \( n \) has \( \phi(n) \) generators.
2.3. Modular arithmetic

Proof  Let $a$ be a generator of $A$, and let $m$ be an integer with $\gcd(m, n) = d$. If $d > 1$, then every power of $a^m$ is of the form $a^k$, where $d \mid k$, and so $a^m$ is not a generator. On the other hand, if $d = 1$, then there exist integers $u, v$ with $um + vn = 1$; so $a = a^{um+vn} = (a^m)^v$ is a power of $a^m$, so that $a^m$ is a generator. The result follows from the definition of $\phi$. □

The Euler and Möbius functions are built in to GAP, and are accessed as $\text{Phi}(n)$ and $\text{MoebiusMu}(n)$ respectively:

```
gap> Phi(720); 192
```
```
gap> MoebiusMu(720); 0
```

2.3 Modular arithmetic

The ring $\mathbb{Z}/(n)$ of integers modulo $n$ is the factor ring of $\mathbb{Z}$ by its ideal $(n)$ consisting of all multiples of $n$. Thus, its elements are congruence classes

$$[a]_n = \{ x \in \mathbb{Z} : x \equiv a \pmod{n} \},$$

with addition and multiplication given by

$$[a]_n + [b]_n = [a + b]_n, \quad [a]_n \cdot [b]_n = [ab]_n.$$

If the modulus $n$ is clear, we frequently omit it. Also, it is very common to represent each congruence class $[a]$ by the unique element of $\{0, \ldots, n-1\}$ which it contains, and to omit the square brackets as well. Sometimes, however, the more cumbersome notation is useful. For example:

**Proposition 2.4** If $m$ divides $n$, then the map

$$[a]_n \mapsto [a]_m$$

is well-defined, and is a ring homomorphism from $\mathbb{Z}/(n)$ to $\mathbb{Z}/(m)$. □

A non-zero element $a$ of a ring $R$ is a zero-divisor if $ab = 0$ for some non-zero $b \in R$; it is a unit if $ab = 1$ for some non-zero $b \in R$ called the inverse of $a$. No element is both a zero-divisor and a unit; for, if $ab = 0$ and $ac = 1$, then $b = cab = 0$.

**Proposition 2.5** In the ring $\mathbb{Z}/(n)$, the non-zero element $a$ is a zero-divisor if $\gcd(a, n) > 1$, and is a unit if $\gcd(a, n) = 1$, In particular, every non-zero element is either a zero-divisor or a unit.
2. Preliminaries

Proof Let $d = \gcd(a, n)$. If $d > 1$, then $0 < n/d < n$ and $a(n/d) = 0$ (in the ring). If $\gcd(a, n) = 1$, then $ua + vn = 1$ for some integers $u$ and $v$; then $ua = 1$ (in the ring). □

The units in any commutative ring with identity form an abelian group, called the group of units of the ring. We let $U(n)$ denote the group of units of $\mathbb{Z}/(n)$. Thus $U(n)$ is a group of order $\phi(n)$. This fact, together with Lagrange’s Theorem, has the following consequence:

Proposition 2.6 If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$. □

This is a generalisation of Fermat’s Little Theorem, the statement that $a^{p-1} \equiv 1 \pmod{p}$ if $a$ is not divisible by $p$.

The most important result about the structure of these rings and groups is the Chinese Remainder Theorem:

Theorem 2.7 Suppose that $\gcd(m, n) = 1$. Then the map

$$[a]_{mn} \mapsto ([a]_m, [a]_n)$$

is an isomorphism between $\mathbb{Z}/(mn)$ and the direct sum $\mathbb{Z}/(m) \oplus \mathbb{Z}/(n)$. In particular, $U(mn)$ is isomorphic to the direct product $U(m) \times U(n)$.

Proof The crucial thing is that the map defined in the theorem is a bijection, since it clearly preserves addition and multiplication. Now the sets on both sides have cardinality $mn$, so it suffices to prove that the map is either one-to-one or onto; but it is profitable to do both: the first is easier, but the second gives an algorithm for inverting the map.

Suppose that $[a]_m = [b]_m$ and $[a]_n = [b]_n$. Then both $m$ and $n$ divide $a - b$. Since $m$ and $n$ are coprime, $mn$ divides $a - b$, so $[a]_{mn} = [b]_{mn}$.

Now suppose congruence classes $[b]_m$ and $[c]_n$ are given; we must find $a$ which is congruent to $b$ mod $m$ and to $c$ mod $n$. Since $\gcd(m, n) = 1$, there exist $u, v$ with $mu + nv = 1$; now it is easily checked that $a = bnv + cmu$ has the required properties. □

Corollary 2.8 If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$. □

The theorem easily extends to more than two coprime factors. In particular, if $n = p_1^{a_1} \cdots p_r^{a_r}$, where $p_1, \ldots, p_r$ are distinct primes and $a_1, \ldots, a_r > 1$, then

$$\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1^{a_1}) \oplus \cdots \oplus \mathbb{Z}/(p_r^{a_r}),$$
$$U(n) \cong U(p_1^{a_1}) \times \cdots \times U(p_r^{a_r}),$$
$$\phi(n) = \phi(p_1^{a_1}) \cdots \phi(p_r^{a_r}).$$
This allows questions about the structure of the ring \( \mathbb{Z}/(n) \) or the group \( U(n) \) to be reduced to the case when \( n \) is a prime power. For example, we can give an alternative derivation for the formula for \( \phi(n) \), the order of \( U(n) \), as follows.

First, if \( n = p^a \) is a prime power, then the integers in \( \{0, \ldots, n - 1\} \) which are coprime to \( n \) are just those not divisible by \( p \), of which there are clearly \( p^a - p^{a-1} = p^a(1 - 1/p) \).

Next, if \( n = p_1^{a_1} \cdots p_r^{a_r} \), then the multiplicative property shows that

\[
\phi(n) = \prod_{i=1}^{r} \phi(p_i^{a_i}) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).
\]

2.4 Primitive roots

Let \( n \) be an integer greater than 1. We say that \( g \) is a primitive root of \( n \) if every element of \( U(n) \) is equal to a power of \( g \) mod \( n \); equivalently, if \( U(n) \) is cyclic and is generated by \( g \).

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.

We now give necessary and sufficient conditions on \( n \) for the existence of a primitive root. First, two preliminary results:

**Lemma 2.9** The group \( U(2^a) \) is isomorphic to \( C_2 \) if \( a = 2 \), and to \( C_2 \times C_{2^{a-2}} \) if \( a \geq 3 \).

**Proof** The units modulo \( 2^a \) are clearly the odd numbers \( 1, 3, \ldots, 2^a - 1 \). Assume that \( a \geq 2 \). The set of units congruent to 1 mod 4 is closed under multiplication, so forms a subgroup \( K \). Moreover, \( \{1, -1\} \) is a subgroup \( H \) of order 2. We have \( H \cap K = \{1\} \) and \( HK = U(2^a) \); so

\[
U(2^a) = H \times K.
\]

Clearly \( H \cong C_2 \), so it remains only to show that \( K \) is cyclic.

We claim that \( K \) is generated by the unit 5. Indeed, for \( a \geq 3 \),

\[
5^{2^a-3} = (1 + 2^2)^{2^a-3} \equiv 1 + 2^{a-1} \pmod{2^a}
\]

by the Binomial Theorem; so the order of 5 does not divide \( 2^{a-3} \), and so must be \( 2^{a-2} \). \( \Box \)
Lemma 2.10  A finite subgroup of the multiplicative group of a field is cyclic. In particular, if \( p \) is prime, then \( U(p) \) is cyclic.

Proof  The proof depends on the fact that the equation \( x^n = 1 \) over a field has at most \( n \) solutions.

Suppose that \( A \) is a finite subgroup of the multiplicative group of a field. Let \( n \) be the order of \( A \), and let \( f(m) \) be the number of elements of \( A \) whose order is \( m \). (Note that the order of any element must be a divisor of \( n \).) Now the following three assertions hold:

(a) \( \sum_{m|n} \phi(m) = n \).

(b) \( \sum_{m|n} f(m) = n \).

(c) For each \( m \), either \( f(m) = 0 \) or \( f(m) = \phi(m) \).

It follows from these assertions that in fact \( f(m) = \phi(m) \) for all \( m \) dividing \( n \). In particular, \( f(n) = \phi(n) > 0 \), so there is an element of order \( n \) in \( A \), which must generate \( A \).

We saw the proof of assertion (a) earlier; and (b) holds because each element of \( A \) has order dividing \( n \). To prove (c), suppose that \( f(m) > 0 \). Then there is an element \( a \) of order \( m \); its \( m \) distinct powers all satisfy \( x^m = 1 \), and so they comprise all the solutions of this equation. Those with order precisely \( m \) are the powers \( a^d \), with \( \gcd(a, m) = 1 \); there are \( \phi(m) \) of these. So \( f(m) = \phi(m) \) in this case.

The last sentence of the lemma holds because \( \mathbb{Z}/(p) \) is a field if \( p \) is prime.

\[ \square \]

Now we have the promised result:

Theorem 2.11  Suppose that \( n > 2 \). Then there exists a primitive root of \( n \) if and only if \( n = p^a \), or \( n = 2p^a \) (where \( p \) is an odd prime and \( a > 0 \)), or \( n = 4 \).

Proof  Let \( n = 2^a p_1^{a_1} \cdots p_r^{a_r} \), where \( p_1, \ldots, p_r \) are odd primes and \( a_1, \ldots, a_r > 0 \). By the Chinese Remainder Theorem,

\[ U(n) \cong U(2^a) \times U(p_1^{a_1}) \times \cdots \times U(p_r^{a_r}). \]

Now the order of each group \( U(p_i^{a_i}) \) is even, and so this group contains an element of order 2. Since a cyclic group contains at most one element of order 2, we see that \( U(n) \) is not cyclic if \( r > 1 \). Also, since \( U(2^a) \) is not trivial
if \( a > 1 \) and is not cyclic if \( a > 2 \) (by Lemma 2.9), we see that \( U(n) \) is not cyclic unless \( n \) is one of the cases listed.

Now we prove that primitive roots exist in these cases. This is clear for \( n = 4 \), and follows from Lemma 2.10 if \( n \) is an odd prime.

Suppose that \( n = p^2 \). Choose \( g \) to be a primitive root mod \( p \). We claim that either \( g \) or \( g + p \) fails to have order \( p - 1 \) mod \( p^2 \). For, if \( g^{p-1} \equiv 1 \) (mod \( p^2 \)), then
\[(g + p)^{p-1} \equiv 1 + g^{p-2}p \pmod{p^2},\]
by the Binomial Theorem, and certainly \( g^{p-2} \) is not divisible by \( p \).

So, replacing \( g \) by \( g + p \) if necessary, we see that the order of \( g \) mod \( p^2 \) is divisible by \( p - 1 \) (its order mod \( p \)), but is not equal to \( p - 1 \); since this order divides \( p(p - 1) \), it must be equal to this value, so that \( g \) is a primitive root of \( p^2 \).

An almost identical argument shows that, if \( g \) is a primitive root of \( p^a \), then either \( g \) or \( g + p^a \) is a primitive root of \( p^{a+1} \). So, by induction, primitive roots of all odd prime powers exist.

Finally, the Chinese Remainder theorem shows that
\[U(2p^a) \cong U(2) \times U(p^a) \cong U(p^a)\]
for \( p \) odd; so primitive roots of \( 2p^a \) exist for any odd prime power \( p \). More specifically, if \( g \) is a primitive root of \( p^a \), then either \( g \) or \( g + p^a \) (whichever is odd) is a primitive root of \( 2p^a \).

Counting primitive roots is easy:

**Proposition 2.12** Suppose that primitive roots of \( n \) exist. Then their number is \( \phi(\phi(n)) \).

**Proof** If primitive roots exist, then \( U(n) \) is a cyclic group of order \( \phi(n) \). Now apply Proposition 2.3. \( \square \)

Something about smallest primitive root and Artin’s conjecture.

### 2.5 Finite abelian groups

In this book, \( C_n \) 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 finite abelian 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 [12] for further details.

2.5.1 Smith canonical form

Definition 2.1 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 \( i > 0 \),

\[ \prod_{j=1}^{i} n'_j = \text{lcm} \left( \prod_{j=1}^{i} l_{k_j} : 1 \leq k_1 < \cdots < k_i \leq q \right). \]

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

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

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

\[ n'_1 = \text{lcm}(2, 4, 6) = 12, \]

\[ n'_1 n'_2 = \text{lcm}(8, 12, 24) = 24, \]

\[ n'_1 n'_2 n'_3 = \text{lcm}(48) = 48, \]

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.
2.5. Finite abelian groups

2.5.2 Primary canonical form

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

\[
C_n = C_{p_1^{a_1}} \times C_{p_2^{a_2}} \times \cdots \times C_{p_r^{a_r}}.
\]

Applying this to the factors in the Smith canonical form, 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.

Lemma 2.13 Let \( a, b \) be elements of an abelian group, having orders \( m, n \) respectively. Then the order of \( ab \) divides \( \text{lcm}(m, n) \).

Proof Let \( h = \text{lcm}(m, n) \). Then \((ab)^h = a^hb^h = 1\). The result follows from the preceding observation. \( \square \)

2.5.3 Proofs

Note first that each of the Smith and prime-power canonical forms can be obtained from the other. Given the Smith canonical form, decompose the cyclic summands into cyclic groups of prime power order, 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

\[
C_n = C_{p_1^{a_1}} \times C_{p_2^{a_2}} \times \cdots \times C_{p_r^{a_r}}.
\]

Then sort the factors into the order specified in the prime-power canonical form.

In the other direction, suppose that the prime-power canonical form is given. Choose the largest cyclic group of order a power of each of the primes which occur; combine these using the reverse of the above principle to get the largest term in the Smith canonical form. Then delete these factors from the list and repeat the procedure to find the other factors.

So, to prove the existence and uniqueness, it suffices to consider the prime-power canonical form.
Theorem 2.14 Let $A$ be an abelian group of order $n = p_1^{a_1} \cdots p_r^{a_r}$. Then there is a direct product decomposition

$$A = P_1 \times \cdots \times P_r$$

where $|P_i| = p_i^{a_i}$ for $i = 1, \ldots, r$; the subgroups in the decomposition are unique.

Remark The subgroup $P_i$ is called the Sylow $p_i$-subgroup of $A$.

Proof Let $P_i$ consist of all the elements of $A$ whose order is a power of the prime $p_i$. By Lemma 2.13, $P_i$ is a subgroup of $A$.

Now take any element $a \in A$; by Lagrange’s Theorem, the order of $A$ is $m = p_1^{b_1} \cdots p_r^{b_r}$, where $b_i \leq a_i$ for $i = 1, \ldots, r$. Put $q_i = m/p_i^{b_i}$. Then

$$\text{gcd}(q_1, \ldots, q_r) = 1;$$

by Euclid’s algorithm, there exist integers $c_1, \ldots, c_r$ such that

$$c_1q_1 + \cdots + c_rq_r = 1.$$ 

Put $x_i = a^{c_i q_i}$ for $i = 1, \ldots, r$. Then the order of $x_i$ divides $m/q_i = p_i^{b_i}$, so $x_i \in P_i$; and $a = x_1 \cdots x_r$. Since $A$ was arbitrary, we have

$$P_1 \cdots P_r = A.$$ 

Also, an element of $P_2 \cdots P_r$ has order dividing $p_2^{a_2} \cdots p_r^{a_r}$; so

$$P_1 \cap P_2 \cdots P_r = 1,$$

and similarly each $P_i$ intersects the product of the others in the identity. These conditions guarantee that

$$A = P_1 \times \cdots \times P_r.$$ 

Now every element of $P_i$ has $p_i$-power order. By Cauchy’s Theorem (see below), the order of this group is a power of $p_i$; and since

$$|P_i| \cdots |P_r| = |A|,$$

we must have $|P_i| = p_i^{a_i}$.

Finally, suppose that

$$A = Q_1 \times \cdots \times Q_r,$$

with $|Q_i| = p_i^{a_i}$ for $i = 1, \ldots, r$. Then every element of $Q_i$ has $p_i$-power order, by Lagrange’s Theorem; so $Q_i \leq P_i$. Considering orders shows that equality holds. So the decomposition is unique. \qed
2.6. Some theorems on primes

Cauchy’s Theorem holds in any group, not necessarily abelian, and the proof in general is no more difficult.

**Proposition 2.15** Let $G$ be a finite group whose order is divisible by the prime $p$. Then $G$ contains an element of order $p$.

**Proof** Let

$$X = \{(g_1, g_2, \ldots, g_p) \in G^p : g_1g_2\cdots g_p = 1\}.$$ 

Then $|X| = |G|^{p-1}$, since the first $p-1$ entries of a $p$-tuple in $X$ determine the last. Now

$$(g_1, g_2, \ldots, g_p) \in G \Rightarrow (g_2, \ldots, g_p, g_1) \in G.$$ 

So an element of $X$ whose entries are not all equal has $p$ distinct cyclic shifts in $X$. Since $|X|$ is divisible by $p$, the number of elements $g \in G$ such that $(g, g, \ldots, g) \in X$ is also divisible by $p$. But these are precisely the elements $g \in G$ with $g^p = 1$. Since there is at least one such element (the identity), there are at least $p$ of them. □

2.6 Some theorems on primes

The Prime Number Theorem states that the number of prime numbers less than a given positive real number $x$ is approximately $x/\log x$, where $\log$ denotes the natural logarithm. It is conveniently stated in the language of asymptotic analysis, where (for two non-vanishing real functions $f$ and $g$) we write $f \sim g$ if $\lim_{x \to \infty} f(x)/g(x) = 1$. The theorem was proved by Hadamard and de la Vallée Poussin in the late nineteenth century; an “elementary” proof (not using complex analysis) was found by Erdős and Selberg in the early twentieth century.

**Theorem 2.16** For a positive real number $x$, let $\pi(x)$ denote the number of positive integer primes $p$ satisfying $p \leq x$. Then

$$\pi(x) \sim \frac{x}{\log x}.$$

Another important theorem, due to Dirichlet, answers the question whether there are infinitely many primes of the form $an + b$ for given positive integers $a$ and $b$. This is not possible if $a$ and $b$ have a common factor $d > 1$, since this factor divides every number of the form $an + b$. Dirichlet showed the converse:
Theorem 2.17  Suppose that $a$ and $b$ are positive integers with $\gcd(a, b) = 1$. Then there are infinitely many positive integers $n$ such that $an + b$ is prime.

Finally, we need an observation due to Euler.

Proposition 2.18

\[ \prod_{p \text{ prime}} \left( 1 - \frac{1}{p} \right) = 0. \]

Proof  Consider the infinite product

\[ \prod_{p \text{ prime}} \left( 1 - \frac{1}{p} \right)^{-1}. \]

Since

\[ \left( 1 - \frac{1}{p} \right)^{-1} = 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots, \]

we see that the infinite product on the left is the sum of the reciprocals of all numbers of the form $1/p_1^{a_1} \cdots p_r^{a_r}$. By the Fundamental Theorem of Arithmetic, each integer $n$ has a unique prime factorisation, and so $1/n$ occurs exactly one in the expansion of the product. So

\[ \prod_{p \text{ prime}} \left( 1 - \frac{1}{p} \right)^{-1} = \sum_{n \geq 1} \frac{1}{n} = \infty, \]

as the harmonic series diverges.

Exercises

2.1. A function $f$ on the positive integers is said to be multiplicative if $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$.

(a) Prove that the Euler and Möbius functions are multiplicative.

(b) Prove that, if $f$ and $g$ are multiplicative, then so is $h$, where

\[ h(n) = \prod_{m \mid n} f(m)g(n/m). \]

2.2. Let $f(n)$ be the number of abelian groups of order $n$ up to isomorphism. Prove that $f$ is multiplicative. Prove also that $f(n) \leq n$ for all positive integers $n$. 
2.3. Lemma 2.13 shows that, if elements $a, b$ of an abelian group $A$ have orders $m, n$ respectively, then the order of $ab$ divides $\text{lcm}(m, n)$. Use the Structure Theorem to prove that there is an element $c \in A$ whose order is exactly $\text{lcm}(m, n)$.

Show by means of an example that this conclusion is false for non-abelian groups.

2.4. Turn the argument given for the proof of Proposition 2.18 into a rigorous piece of analysis.
2. Preliminaries
CHAPTER 3

Carmichael’s lambda-function

3.1 The group of units

In the last chapter, we implicitly calculated the form of the group of units in $\mathbb{Z}_n$: 

**Theorem 3.1**  
(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 \(5\). □

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 \( n \).
Proposition 3.2 Given any finite abelian group $A$, there are only a finite number of positive integers $n$ such that $U(n) \cong A$.

Proof Express $A$ in all possible ways as a direct product of cyclic groups. Now a cyclic group $C_m$ is equal to $U(p^r)$ if and only if $p^{r-1}(p-1) = m$, so that either $p = m + 1$ and $r = 1$, or $p$ is the largest divisor of $m$. Also, if $C_2$ is not one of the factors, then the 2-part of $n$ is 1 or 2, while if there is a factor $C_2$, then either the 2-part is 4, or it is $2^a$ where $C_{2^a-2}$ is another of the factors. So for each decomposition there are only finitely many possible values of $n$. □

Problem 3.1 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 [17], where further references appear.

Problem 3.2 (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?

3.2 The definition

Euler’s function $\phi$ has the property that $\phi(n)$ is the order of the group $U(n)$ of units of $\mathbb{Z}_n$. R. D. Carmichael [7] introduced the function $\lambda$:

Definition 3.1 For a positive integer $n$, let $\lambda(n)$ be the exponent of $U(n)$ (the least $m$ such that $a^m = 1$ for all $a \in U(n)$).

Thus, $\lambda(n)$ is equal to the largest invariant factor of $U(n)$ (the order of the largest cyclic summand in the Smith canonical form). From the structure theorem for $U(n)$ (Theorem 3.1), we obtain the formula for $\lambda(n)$:

Proposition 3.3 (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

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

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

(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 [17]. The computer system GAP [10] has the function \( \lambda \) built-in, with the name \texttt{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 3.4**  (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

\[
\sum_{l|\lambda^*(m)} \mu\left(\frac{m}{l}\right) d\left(\lambda^*(l)\right),
\]

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

**Proof**  (a) Suppose that \( n_1 \) divides \( n_2 \). The natural map \( \theta \) 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 \( \theta \) 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 $2^a \mid m$;

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

(Here the notation $p^a \mid m$ 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

$$\lambda^*(12) = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 = 65520.$$ 

The function $\lambda^*$ provided in our suite of GAP functions with the name $\text{LambdaStar}$. It is computed by the algorithm just described.

```
gap> LambdaStar(12);
65520

gap> Lambda(65520);
12
```

Suppose that $m = 2q$, 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 $\lambda$ 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, ... ;
3.2. The definition

(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 \( \lambda \).

Sierpiński [16] 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 \( n < 1000000 \) for which the equation holds.

The formulae show up a couple of errors on p. 236 of \([7]\), 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 \( \lambda(n) = 20 \).

The function \( \lambda^*(n) \) has another property:

**Proposition 3.5** For a fixed even number \( m = \lambda(n) \), the value of \( \phi(n) \) is maximal when \( n = \lambda^*(n) \).

**Proof** It is easily checked that, if \( n_1 \) is a proper divisor of \( n_2 \), then \( \phi(n_1) \leq \phi(n_2) \), 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 \( \phi(n)/\lambda(n) \).)

<table>
<thead>
<tr>
<th>( n )</th>
<th>( \phi(n) )</th>
<th>( \xi(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>7, 9, 14, 18</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>21, 28, 36, 42</td>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>56, 72, 84</td>
<td>24</td>
<td>4</td>
</tr>
<tr>
<td>63, 126</td>
<td>36</td>
<td>6</td>
</tr>
<tr>
<td>168</td>
<td>48</td>
<td>8</td>
</tr>
<tr>
<td>252</td>
<td>72</td>
<td>12</td>
</tr>
<tr>
<td>504</td>
<td>144</td>
<td>24</td>
</tr>
</tbody>
</table>

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 [9]. They showed, among other things, that for \( x \geq 16 \),

\[
\frac{1}{x} \sum_{n \leq x} \lambda(n) = \frac{x}{\log x} \exp \left( \frac{B \log \log x}{\log \log \log x} (1 + o(1)) \right)
\]
A composite positive integer \( m \) is called a \textit{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 \( \lambda(561) = 80 \).

### 3.3 Denominators of Bernoulli numbers

The sequence \( (24, 240, 504, 480, 264, \ldots) \) of values of \( \lambda^*(2m) \) agrees with sequence A006863 in the \textit{Encyclopedia of Integer Sequences} \cite{17}. It 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 \cite{18} for some of these); we simply prove that the formula given in the Encyclopedia agrees with the definition of \( \lambda^*(2m) \).

The \( m \)th term \( a_m \) of the \textit{Encyclopedia} sequence is the gcd of \( kL(k^{2m} - 1) \), 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 \( 2L(2^6 - 1) \), 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 \( kL(k^{2m} - 1) \). 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 \( kL(k^{2m} - 1) \) for all \( k \) (with large enough \( L \)). Since

\[
(k_1k_2)L((k_1k_2)^{2m} - 1) = (k_1k_2)Lk_1^{2m}(k_2^{2m} - 1) + (k_1k_2)L(k_1^{2m} - 1),
\]

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 3.4; that is, \( n_1 \mid p^{2m} - 1 \). So \( n \mid p^a(p^{2m} - 1) \), as required.

### 3.4 \textit{p}-rank and \textit{p}-exponent

**Definition 3.2** Let \( p \) be a prime. The \textit{\textit{p}-rank} of an abelian group \( A \) is the number of its elementary divisors which are powers of \( p \), and the \textit{\textit{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
3.4. \( p \)-\( \text{rank} \) and \( p \)-\( \text{exponent} \)

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 \( 2 \)-\( \text{rank} \) 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 \( p \)-\( \text{rank} \) and \( p \)-\( \text{exponent} \) of \( U(n) \) for odd \( p \).
3. Carmichael’s lambda-function
4.1 The definition

Carmichael [7] defined primitive lambda-roots as a generalisation of primitive roots, to cover cases where the latter do not exist.

Definition 4.1 A primitive lambda-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 $\phi$-root.)

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

Proposition 4.1 Every element in the power class of a primitive lambda-root is a primitive lambda-root.

Proposition 4.2 For any $n$, either $\xi(n) = 1$ or $\xi(n)$ is even.

Proof Theorem 3.1 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 $n = p^aq^bm$ where $p$ and $q$ are distinct odd primes not dividing $m$. Then $\phi(n) = \phi(p^a)\phi(q^b)\phi(m)$ and $\lambda(n) = \text{lcm}\{\phi(p^a), \phi(q^b), \lambda(m)\}$; 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 $\phi(2^am)/\lambda(2^am)$ is even for any odd $m$. $\square$
For example, consider the case $n = 15$. We have $\phi(15) = \phi(3)\phi(5) = 8$, while $\lambda(15) = \text{lcm}(\phi(3), \phi(5)) = 4$, 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:

<table>
<thead>
<tr>
<th>element $x$</th>
<th>powers of $x$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1, 2, 4, 8</td>
</tr>
<tr>
<td>4</td>
<td>1, 4</td>
</tr>
<tr>
<td>7</td>
<td>1, 7, 4, 13</td>
</tr>
<tr>
<td>8</td>
<td>1, 8, 4, 2</td>
</tr>
<tr>
<td>11</td>
<td>1, 11</td>
</tr>
<tr>
<td>13</td>
<td>1, 13, 4, 7</td>
</tr>
<tr>
<td>14</td>
<td>1, 14</td>
</tr>
</tbody>
</table>

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

**Corollary 4.3** If $\lambda(n) > 2$, then the number of primitive lambda-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 4.4** 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 $a_1, a_1 a_2, \ldots, a_1 a_r$ are all PLRs and clearly generate $U(n)$. □

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

**Theorem 4.5** 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

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

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 \( g(m) = \sum_{l \mid m} f(l) \), 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 \( \lambda \)-roots is

\[
\sum_{l \mid 12} \mu(12/l) \gcd(4, l) \gcd(12, l).
\]

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 lambda-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 lambda-roots, and the smallest primitive lambda-root, for certain values of \( n \).

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

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 lambda-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 4.6 The proportion of units which are primitive lambda-roots can be arbitrarily close to 0.

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

\[
\frac{\phi(p-1)/(p-1)}{r \text{ prime}} \prod_{r \mid p-1} \left(1 - \frac{1}{r}\right).
\]

Choosing \( p \) to be congruent to 1 modulo the product of the first \( k \) primes. Note that this is possible, by Dirichlet’s Theorem (Theorem 2.17), since \( \gcd(p_1 p_2 \cdots p_k, 1) = 1 \). For such a prime \( p \), the product on the right is arbitrarily small, since by Proposition 2.18 we have

\[
\prod_{r \text{ prime}} \left(1 - \frac{1}{r}\right) = 0.
\]

In order to obtain proper PLRs, also choose \( p \equiv 1 \pmod{4} \); then the proportion for \( 4p \) is the same as for \( p \). \qed

Problem 4.1 Can the proportion of units which are primitive lambda-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

\[
n = \lambda^*(53130) = 460765909369981425841156813418098240135472867831112,
\]

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

Li [14] 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 \( n \leq x \) such that \( a \) is a PLR of \( n \). This function is more erratic than the corresponding function for primitive roots: the lim inf of \( \left(\sum_{1 \leq a \leq x} N_a(x)\right)/x^2 \) is zero, while the lim sup of this expression is positive.

4.2 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 4.7 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

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

**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 $p^{a(p_i)}$. 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 $p^a$. \[\square\]

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 4.8** 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. \[\square\]
This raises a curious number-theoretic problem: 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). However, Müller and Puchta [15] have shown:

**Proposition 4.9** The proportion of integers \( n \) for which the number of primitive lambda-roots of \( n \) is equal to \( \phi(\phi(n)) \) tends to zero as \( n \to \infty \).

The condition in this proposition can be expressed in a different way, namely, a relationship between the number of power classes of PLRs and the function \( \xi(n) = \phi(n)/\lambda(n) \).

**Proposition 4.10** 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 \( b^{\lambda(n)/p} \). 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. \( \square \)

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 4.1 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

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

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

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

4.3 Fraternities

Definition 4.2 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 Section 3.4.

Proposition 4.11 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 $x^2 \equiv y^2 \pmod{n}$ 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 $e = 1$. \hfill \square

Remark We worked out in Section 3.4 the necessary and sufficient conditions for $e = 1$. 
Proposition 4.12 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 4.13 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. □

Example 4.2 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.
CHAPTER 5

Some special structures for the units

**Theorem 5.1**  Suppose that the Smith canonical form of $U(n)$ is

\[ U(n) \cong C_{\lambda(n)} \times \cdots \times C_{\lambda(n)} \quad (r \text{ factors}), \]

with $r > 1$. Then either

(a) $n = 8, 12 \text{ or } 24$; 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 $n = 2^ap_1 \cdots p_s$, 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

\[ p_1^{a_1-1}(p_1 - 1) = \cdots = p_r^{a_r-1}(p_r - 1). \]
5. Some special structures for the units

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 \( p_2 = p^{a_1} - 1(p - 1) + 1 \) and \( a_2 = 1 \).

The odd numbers \( n < 1000000 \) occurring in case (b) of the theorem are

\[
\begin{align*}
63 &= 9 \cdot 7, \\
513 &= 27 \cdot 19, \\
2107 &= 49 \cdot 43, \\
12625 &= 125 \cdot 101, \\
26533 &= 169 \cdot 157, \\
39609 &= 243 \cdot 163, \\
355023 &= 729 \cdot 487.
\end{align*}
\]

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

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

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

**Problem 5.1** 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 \( n = \lambda^*(157080) \), a number with 122 digits, the multiplicity of \( C_{157080} \) in the Smith normal form of \( U(n) \) is 16.

This problem is related to Problem 4.1 as follows:

**Proposition 5.2** 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 \( n \) satisfies

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

where \( \zeta \) is the Riemann zeta-function.
Proof  We use the formula of Theorem 4.7. The number \( m(p) \) is at least \( d \) for each prime dividing \( \phi(n) \), so we have:

\[
F(n)/\phi(n) = \prod_{p|\phi(n)} (1 - 1/p^{m(p)}) \\
\geq \prod_{p|\phi(n)} (1 - 1/p^d) \\
\geq \prod_p (1 - 1/p^d) \\
= \zeta(d)^{-1} \\
\geq \left( 1 + \frac{1}{2^d} + \frac{1}{2^d} + \frac{1}{4^d} + \frac{1}{4^d} + \frac{1}{4^d} + \frac{1}{4^d} + \frac{1}{8^d} + \cdots \right)^{-1} \\
= \left( \frac{1}{1 - 1/2^{d-1}} \right)^{-1} \\
= 1 - 1/2^{d-1}.
\]

(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.)

\[\square\]
5. Some special structures for the units
CHAPTER 6

Negating and non-negating PLRs

6.1 Definition

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

(a) Is $-x$ also a primitive lambda-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 6.1 Let $x$ be a primitive lambda-root of $n$, where $n > 2$. Then $-x$ is also a primitive lambda-root if either $n$ has a prime factor congruent to 1 (mod 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 lambda-root if and only if $-1$ is not a power of $x$. Necessary and sufficient conditions for this are given in Section 6.4 below.

Definition 6.1 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 6.2** Suppose that $\lambda(n)$ is twice an odd number (so that $n$ is not divisible by 16 or by any prime congruent to 1 (mod 4)).

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

(b) Otherwise, some primitive lambda-roots $x$ have the property that $-x$ is a primitive lambda-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 6.3** If a primitive lambda-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 6.1** 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 6.2** 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?

### 6.2 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 6.4** 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 3.1, 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 $i$th 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. \qed

### 6.3 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 $U(n) \cong C_{\lambda(n)} \times C_{\xi(n)}$, 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 6.5** Let $p$ and $q$ be primes congruent to 5 (mod 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

$$x_1 \equiv a \pmod{p}, \quad x_1 \equiv b \pmod{q},$$
$$x_2 \equiv a \pmod{p}, \quad x_2 \equiv -b \pmod{q},$$
$$a^2 \equiv -1 \pmod{p}, \quad b^2 \equiv -1 \pmod{q}.$$

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 \(-1 \in \langle x \rangle \cap \langle x + 1 \rangle \). \( \Box \)

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 except 13 and 37. The table gives all instances with \( pq < 300 \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>( x )</th>
</tr>
</thead>
<tbody>
<tr>
<td>65 = 5 \cdot 13</td>
<td>\pm 18</td>
</tr>
<tr>
<td>145 = 5 \cdot 29</td>
<td>\pm 12</td>
</tr>
<tr>
<td>185 = 5 \cdot 37</td>
<td>\pm 68</td>
</tr>
<tr>
<td>265 = 5 \cdot 53</td>
<td>\pm 83</td>
</tr>
</tbody>
</table>

A similar argument works in other cases, with some modification. If \( q \equiv 1 \) (mod 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 \( 2^8 \equiv 1 \) (mod 85) but \( 2^4 \equiv 16 \) (mod 85). So \( 2x \) has order 8, and \( (x + 1) \) has order 16, if \( x \) is any solution of \( x^2 \equiv -1 \) (mod 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 \( 2^{10} \equiv -1 \) (mod 205). Thus \( (2x)^{10} \equiv 1 \) (mod 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 6.6** Let \( p \) and \( q \) be primes with \( p \equiv 5 \) (mod 8) and \( q \equiv 1 \) (mod 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.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$x$</th>
</tr>
</thead>
<tbody>
<tr>
<td>85</td>
<td>$5 \cdot 17$</td>
</tr>
<tr>
<td>221</td>
<td>$13 \cdot 17$</td>
</tr>
</tbody>
</table>

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 $-1 \in \langle x \rangle$.

**Theorem 6.7** Let $p$ and $q$ be primes congruent to 7 (mod 12), such that $\gcd(p - 1, q - 1) = 6$. Suppose that 3 is a primitive root modulo both $p$ and $q$. Then there exists a number $x$ such that

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

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 almost identical to that of the previous theorem. If $x^3 \equiv -1$, then $x^2 - x + 1 \equiv 0$, and so $(x + 1)^2 \equiv 3x$. \hfill $\square$

Since 3 is a primitive root of 7, 19 and 31, the theorem gives the following values:

<table>
<thead>
<tr>
<th>$n$</th>
<th>$x$</th>
</tr>
</thead>
<tbody>
<tr>
<td>133</td>
<td>$7 \cdot 19$</td>
</tr>
<tr>
<td>217</td>
<td>$7 \cdot 31$</td>
</tr>
</tbody>
</table>

**Problem 6.3** 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.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$x$</th>
</tr>
</thead>
<tbody>
<tr>
<td>91</td>
<td>$7 \cdot 13$</td>
</tr>
<tr>
<td>247</td>
<td>$13 \cdot 19$</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>$n$</th>
<th>$x$</th>
</tr>
</thead>
<tbody>
<tr>
<td>91</td>
<td>$7 \cdot 13$</td>
</tr>
<tr>
<td>259</td>
<td>$7 \cdot 37$</td>
</tr>
</tbody>
</table>

**Problem 6.4** (a) What happens for larger values of $\xi(pq)$?

(b) What happens for larger numbers of prime factors of $n$?
6.4 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 6.2** 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 6.8** 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 6.4, \( U(n) = A \times B \), 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. \( \square \)

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 3.1), thus describes when negating PLRs exist.

**Theorem 6.9** Let \( n = 2^am \) 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 (mod 4). In this case the rank of \( S \) is \( r + a - 1 \).
6. Negating and non-negating PLRs
CHAPTER 7

Other special types of PLR

7.1 Inward and outward PLRs

Definition 7.1 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 7.1 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 7.2 If a primitive lambda-root is inward, then so is every element of its power class.

Proposition 7.3 (a) Every primitive lambda-root of $n$ is outward if and only if $n$ is even.

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

47
7. Other special types of PLR

**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 (mod 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.

<table>
<thead>
<tr>
<th>$n$</th>
<th>Power class</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>2, 11</td>
<td>inward non-negating</td>
</tr>
<tr>
<td></td>
<td>19, 10</td>
<td>outward non-negating</td>
</tr>
<tr>
<td></td>
<td>5, 17</td>
<td>inward negating</td>
</tr>
<tr>
<td>28</td>
<td>11, 23</td>
<td>outward non-negating</td>
</tr>
<tr>
<td></td>
<td>5, 17</td>
<td>outward non-negating</td>
</tr>
<tr>
<td></td>
<td>3, 19</td>
<td>outward negating</td>
</tr>
<tr>
<td>42</td>
<td>11, 23</td>
<td>outward non-negating</td>
</tr>
<tr>
<td></td>
<td>19, 31</td>
<td>outward non-negating</td>
</tr>
<tr>
<td></td>
<td>5, 17</td>
<td>outward negating</td>
</tr>
</tbody>
</table>

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 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,
7.2. **Perfect, imperfect and aberrant PLRs**

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 7.1** 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: \( n = 35, 55, 77, 95, \ldots \))

## 7.2 Perfect, imperfect and aberrant PLRs

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

**Definition 7.2** 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 7.4** 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 \( p_i^{b_i} \), 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 3.4(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. \( \square \)

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 \( x \equiv x_i (\text{mod } p_i^{a_i}) \), 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 7.5 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 \( x \equiv 1 \pmod{p_i} \) 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 7.3(a).) \( \square \)

Theorem 7.6 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 \( p_i^{a_i} \), 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. \( \square \)

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 7.7 Every PLR of \( n \) is perfect if and only if \( n \) is a prime power or twice a prime power.
7.2. Perfect, imperfect and aberrant PLRs

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

<table>
<thead>
<tr>
<th>n</th>
<th>perfect PLRs</th>
<th>imperfect PLRs</th>
<th>aberrant PLRs</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>2, 8</td>
<td>7, 13</td>
<td>—</td>
</tr>
<tr>
<td>21</td>
<td>5*, 17*</td>
<td>2, 11; 10, 19</td>
<td>—</td>
</tr>
<tr>
<td>35</td>
<td>3, 12, 17, 33</td>
<td>2, 18, 23, 32</td>
<td>—</td>
</tr>
<tr>
<td>63</td>
<td>5*, 38*, 47*, 59*</td>
<td>2, 18, 23, 32</td>
<td>13, 34; 44, 53</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>17*, 26*, 41*;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>29, 50; 31, 61; 40, 52</td>
</tr>
</tbody>
</table>

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 7.8** 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. \qed

**Corollary 7.9** If $n = p_j^{1}(p^{i-1}(p-1)+1)$, where $j > 1$ and $p$ and $p^{i-1}(p-1)+1$ 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 7.2** Find families of integers $n$ for which aberrant PLRs exist.

**Problem 7.3** 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!)

### 7.2.1 Deeply aberrant and nearly perfect PLRs

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

**Definition 7.3** 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 7.4** Count the deeply aberrant PLRs of $n$.

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

**Definition 7.4** 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 7.5** 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 7.10** 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. \qed

Note also that, if $n$ is odd, then any nearly perfect PLR of $n$ is inward; in other words, Theorem 7.5 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 $p \equiv 1 \pmod{4}$. 
7. Other special types of PLR

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

7.3 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 7.5** 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 6.3 and Corollary 7.2 that, if a PLR is strong, then so is every PLR in the same power class.

**Problem 7.6** 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 7.7** Count the strong PLRs of $n$.

**Problem 7.8** 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 5.1(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 $U(n)$. 
7.3. Further properties of PLRs

**Definition 7.6** 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 7.11** 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 \( \xi(n) = 2 \). \( \square \)

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 \( \pm 3 \) are:

\[
\begin{array}{cccccccccccc}
3 & 1 & 3 & 9 & 27 & 16 & 48 & 14 & 42 & 61 & 53 & 29 & 22 \\
-3 & 1 & 62 & 9 & 38 & 16 & 17 & 14 & 23 & 61 & 12 & 29 & 43
\end{array}
\]

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:

\[
\begin{array}{cccccccccccc}
2 & 1 & 2 & 4 & 8 & 16 & 32 & 64 & 37 & 74 & 57 & 23 & 46 \\
32 & 1 & 32 & 23 & 8 & 74 & 2 & 64 & 46 & 16 & 57 & 4 & 37
\end{array}
\]

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

**Problem 7.9** 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 7.10** 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.
7. Other special types of PLR
In this chapter, we describe the role of Carmichael's function in the RSA public-key cryptosystem. After a preliminary number-theoretic result, we give a brief introduction to public-key cryptography, and then discuss the RSA system.

8.1 A number-theoretic result

By definition, if $\lambda(n)$ divides $m$, then $x^m \equiv 1 \pmod{n}$ for all units $x$ of $\mathbb{Z}_n$. For squarefree numbers, a stronger property holds.

**Proposition 8.1** Suppose that $n$ is squarefree. Then, for a positive integer $m$, we have

$$x^m \equiv x \pmod{n}$$

for all $x \in \mathbb{Z}_n$ if and only if $\lambda(n)$ divides $m - 1$.

**Proof** In the reverse direction, if $u$ is a primitive lambda-root, then $u^m \equiv u$ if and only if $u^{m-1} \equiv 1$, which occurs if and only if $\lambda(n)$ divides $m - 1$.

For the converse, it is enough to show that $x^{\lambda(n)+1} \equiv x \pmod{n}$ for all $x \in \mathbb{Z}_n$. For then an easy induction shows that, if $\lambda(n)$ divides $m - 1$, then $x^m \equiv x \pmod{n}$.

Suppose first that $n$ is prime. Then $\lambda(n) = n - 1$. We have $x^{n-1} \equiv 1 \pmod{n}$ for all $x \neq 0$, and so $x^n \equiv x$ for all $x \neq 0$; but clearly this equation holds for $x = 0$, so it holds for all $x$.

Now if $n$ is squarefree, then $x^m \equiv x \pmod{n}$ if and only if this congruence holds modulo each prime divisor $p$ of $n$, by the Chinese Remainder Theorem. This holds if and only if $p - 1$ divides $m - 1$, by the preceding paragraph.
So the congruence mod \( n \) holds if and only if \( m - 1 \) is divisible by the least common multiple of \( p - 1 \) over all prime divisors \( p \) of \( n \); but this least common multiple is \( \lambda(n) \). \( \square \)

Conversely, if \( n \) is not squarefree, then there is no number \( m > 1 \) such that \( x^m \equiv x \pmod{n} \) for all \( x \in \mathbb{Z}_n \). For suppose that \( p \) is prime, and that \( p^a \) is the exact power of \( p \) dividing \( n \). If \( m > a \), then \( p^m \equiv 0 \pmod{p^a} \), and so \( p^m \equiv p \pmod{n} \) is impossible. But certainly \( a \) is smaller than \( \lambda(n) \), whereas considering the units we see that \( m > \lambda(n) \) is necessary for the equation to hold.

\section{Public-key cryptography}

The idea of public-key cryptography based on the fact that there are easy and hard problems was devised by Diffie and Hellman in the 1970s. This is one of the great ideas of the twentieth century! It answers the question “how can a cipher be secure when the key is publicly known?”

We will not be precise about what is meant by easy and difficult problems: the intention is that a method of solution of a difficult problem is known in principle but it would take unfeasibly long to carry out even using the most advanced computers available.

The general set-up is that Alice wishes to send a message to Bob in such a way that Bob can read the message, but an unauthorised interceptor Eve cannot read it.

Let \( \mathcal{P} \) be the set of plaintext messages that users of the system might wish to send. (Thus, \( \mathcal{P} \) might be the set of all strings of letters and punctuation marks, or strings of zeros and ones, or certain strings of dots and dashes.) Let \( \mathcal{K} \) be the set of keys, and \( \mathcal{Z} \) the set of ciphertexts. Then there is an encryption function

\[ e : \mathcal{P} \times \mathcal{K} \rightarrow \mathcal{Z} \]

and a decryption function

\[ d : \mathcal{Z} \times \mathcal{K} \rightarrow \mathcal{P} \]

which must satisfy the relationship

(PK1) \: \: d(e(p,k), k) = p.

This simply says that encryption followed by decryption using the same key must recover the original plaintext.

Now the first requirement of public-key cryptography is:

(PK2) Evaluating \( e \) should be easy.

(PK3) Evaluating \( d \) should be difficult.
This means that we may assume that Eve not only knows the ciphertext \( z \) that Alice sent to Bob, but she also knows the key \( k \) and the functions \( e \) and \( d \) used for encoding and decoding; so all she has to do is to evaluate \( d(z,k) \). However, this is a hard problem.

But if decryption is hard, how does Bob (the legitimate recipient) manage to do it? The answer is that there is yet another layer. There is a set \( S \) of secret keys, together with an inverse pair of functions

\[
g : S \rightarrow K, \quad h : K \rightarrow S.
\]

(Think of the mnemonics ‘go public’ and ‘hide’.) Now we make the following requirements:

(PK4) Evaluating the composite function \( d^*(z,s) = d(z,g(s)) \) is easy.

(PK5) Evaluating \( g \) is easy

(PK6) Evaluating \( h \) is hard.

Assumption (PK4) means that, given \( s \) and \( z \), it is easy to compute \( p \) such that \( d(z,k) = p \) (or equivalently \( e(p,k) = z \)) for the unique \( k \) which satisfies \( h(k) = s \) (or equivalently \( g(s) = k \)). Note that this does not mean that it is easy to compute \( g(s) = k \) and then \( d(z,k) = p \), since the latter computation is assumed to be hard; there should be an easy way to compute the composite function \( d^* \).

Now let us see how the system works. Alice wants to send a message to Bob which is secure from the eavesdropper Eve. Bob chooses a ‘secret key’ from the set \( S \) and tells nobody of his choice. He computes the corresponding ‘public key’ \( k = g(s) \in K \) and makes this available to Alice. Bob is aware that Eve will also have access to his public key \( k \). We observe that this computation is assumed to be easy.

Alice wants to send Bob the plaintext message \( p \). Knowing his public key \( k \), she computes the ciphertext \( e(p,k) \) and sends this to Bob. (This computation is also easy.)

Bob is now faced with the problem of decrypting the message. But Bob already knows the secret key \( s \), and so he only has to do the easy computation of \( p = d^*(z,s) \). Since \( g(s) = k \), we have \( p = d(z,k) \), so that \( p \) is indeed the correct plaintext that Alice wanted to send.

What about Eve? Her position is different, since she doesn’t know the secret key. Either she has to compute \( d(z,k) \) directly (which is hard), or she could decide to compute Bob’s secret key \( s \) by evaluating the function \( s = h(k) \) (which is also hard).

Note that Eve knows in principle how to evaluate either of these functions; the only thing keeping the cipher secure is the complexity of the computations.
The important thing is that the secret key, which enables Bob to decrypt the message, is never communicated to anyone else; Bob chooses it, and uses it only to decrypt messages sent to him.

Now in principle we have a method for any set of people to communicate securely. Suppose we have a number of users $A, B, C, \ldots$. Each user chooses his or her own secret key: thus, Alice chooses $s_A$, Bob chooses $s_B$, and so on. These choices are never communicated to anyone else. Now Alice computes $k_A = g(s_A)$ and publishes it; and similarly Bob computes $k_B = g(s_B)$ and so on. Then anyone who wishes to send a message $p$ to Alice first obtains her public key $k_A$ (which may be in a directory or on her Web page), and then encrypts it as $z = e(p, k_A)$ and transmits this to Alice. She can calculate $p = d^*(z, s_A) = d(z, k_A)$; but nobody else can read the message without performing a hard calculation.

Some terminology that is often used here is that of ‘one-way functions’. A function $f : A \to B$ is said to be one-way if it is easy to compute $f$ but hard to compute the inverse function from $B$ to $A$. It is a trapdoor one-way function if there is a piece of information which makes the computation of the inverse function easy. Thus, for public-key cryptography, we want encryption to be a trapdoor one-way function, where the key to the trapdoor is the secret key; the function from secret key to public key should be a one-way function.

8.3 The RSA cryptosystem

Preliminaries

The system depends on the following problems. The easy problems are all in $P$. Unfortunately the hard problems are not known to be $\mathsf{NP}$-complete!

Easy problems

(1) Test whether an integer $N$ is prime.

(2) Given $a$ and $n$, find $\gcd(a, n)$ and (if it is 1) find an inverse of $a \mod n$.

(3) Calculate the transformation $T_d : x \mapsto x^d \mod N$.

Hard problems

(4) Given an integer $N$, factorise it into its prime factors.

(5) Given an integer $N$, calculate $\lambda(N)$ (or $\phi(N)$).

(6) Given $N$ and $d$, find $e$ such that $T_e$ is the inverse of $T_d \mod N$. 
Notes about the easy problems

Problem (1): Note that trial division does not solve this problem efficiently. For a number \(N\) requiring \(n\) bits of input is one which has \(n\) digits when written in base 2, and hence is of size roughly \(2^n\); its square root is about \(2^{n/2}\), and trial division would require about half this many steps in the worst case. Only in 2002 was an algorithm found which solves this problem in a polynomial number of steps, by Manindra Agrawal, Neeraj Kayal and Nitin Saxena at the Indian Institute of Technology, Kanpur. However, the result had been widely expected, since ‘probabilistic’ algorithms which tested primality with an arbitrarily small chance of giving an incorrect answer have been known for some time.

Problem (2): This is solved by Euclid’s algorithm.

Problem (3). On the face of it, this problem seems hard, for two reasons:

- First, the number \(x^d\) will be absolutely vast, with about \(d \log x\) digits;
- Second, we have on the face of it to perform \(d - 1\) multiplications to find
  \[ x^d = x \cdot x \cdot x \cdots x \quad d \text{ factors}. \]

But these difficulties can both be overcome:

- We perform all arithmetic operations modulo \(N\); in other words, given two numbers \(a\) and \(b\) smaller than \(N\), we multiply them and calculate the remainder mod \(N\). No number larger than \(N^2\) ever appears in the calculation.

- The number of multiplications is reduced from \(d - 1\) to \(2 \log d\) by the scheme below.

Write \(d\) in base 2: \(d = 2^{a_1} + 2^{a_2} + \cdots + 2^{a_k}\). Suppose that \(a_1\) is the greatest exponent. Then \(k \leq a_1 + 1\) and \(a_1 \leq \log_2 d\). By \(a_1 - 1\) successive squarings, calculate \(x^2, x^{2^2}, \ldots, x^{2^{a_1}} \pmod{N}\). Now

\[ x^d = x^{2^{a_1}} \cdot x^{2^{a_2}} \cdots x^{2^{a_k}} \]

can be obtained by \(k - 1\) further multiplications. The total number of multiplications required is \(a_1 + k - 2 < 2 \log_2 d\).

For example, let us compute \(123^{321} \pmod{557}\).

First we find by successive squaring

<table>
<thead>
<tr>
<th>(i)</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>123^{2^i} \mod 557</td>
<td>123</td>
<td>90</td>
<td>302</td>
<td>413</td>
<td>127</td>
<td>533</td>
<td>19</td>
<td>361</td>
<td>540</td>
</tr>
</tbody>
</table>
8. Applications to cryptography

Now $321 = 2^8 + 2^6 + 1$, so two further multiplications mod 557 give

$$123^{321} \equiv 540 \cdot 19 \cdot 123 \equiv 234 \cdot 123 \equiv 375 \pmod{557}.$$

The GAP function \texttt{PowerMod} performs this calculation for us if preferred:

\begin{verbatim}
gap> PowerMod(123,321,557);
gap> 375
\end{verbatim}

**Notes about the hard problems** Problems (4)–(6) are not known to be “hard” in the sense of computational complexity (for example, NP-complete); so it is possible that they may not be as hard as we would like. However, centuries of work by mathematicians has failed to discover any ‘easy’ algorithm to factorise large numbers. (The advent of quantum computation could change this assertion! But to discuss this would take us too far afield.)

We will be concerned only with numbers $N$ which are the product of two distinct primes $p$ and $q$. So we really need the special case of (4) which asks:

Given a number $N$ which is known to be the product of two distinct prime factors, find the factors.

Even this problem is intractable at present.

However, if we know that $N$ is the product of two distinct primes, then problems (4) and (5) are equivalent, in the sense that knowledge of a solution to one enables us to solve the other.

**Proposition 8.2** Suppose that $N$ is the product of two distinct primes. Then, from any one of the following pieces of information, we can compute the others in a polynomial number of steps:

- the prime factors of $N$;
- $\phi(N)$;
- $\lambda(N)$.

For suppose first that $N = pq$ where $p$ and $q$ are primes (which we know). Then $\phi(N) = (p-1)(q-1)$ can be found by simple arithmetic. Also, $\lambda(N) = \text{lcm}(p-1,q-1) = (p-1)(q-1)/\gcd(p-1,q-1)$; the greatest common divisor can be found by Euclid’s Algorithm, and the rest is arithmetic.

Suppose that we know $\phi(N)$. Then we know the sum and product of $p$ and $q$, (namely, $p + q = N - \phi(N) + 1$ and $pq = N$); and so the two factors are roots of the quadratic equation

$$x^2 - (N - \phi(N) + 1)x + N = 0,$$
8.3. The RSA cryptosystem

which can be solved by arithmetic (using the standard algorithm for finding the square root).

The case where we know \( N \) and \( \lambda(N) \) is a bit more complicated. Suppose that \( p \) is the larger prime factor. Then \( \lambda(N) = \text{lcm}(p-1, q-1) \) is a multiple of \( p-1 \), and divides \( \phi(N) \). Let \( r = N \mod \lambda(N) \) be the remainder on dividing \( N \) by \( \lambda(N) \). Then

- \( N - \phi(N) \equiv r \pmod{\lambda(N)} \), since \( \lambda(N) \mid \phi(N) \);
- \( N - \phi(N) = p + q - 1 < 2\lambda(N) \), since \( \lambda(N) \geq p - 1 > q \) (assuming that \( N > 6 \)).

So \( N - \phi(N) = r \) or \( N - \phi(N) = r + \lambda(N) \). We can solve the quadratic for each of these two possible values of \( \phi(N) \); one of them will give us the factors of \( N \).

**Example** Suppose that \( N = 589 \) and \( \lambda(N) = 90 \). Now \( 589 \mod 90 = 49 \). Trying \( \phi(N) = 540 \), we get that the prime factors of \( N \) are the roots of the quadratic

\[
x^2 - 50x + 589 = 0,
\]

so that

\[
p, q = 25 \pm \sqrt{625 - 589} = 25 \pm 6 = 31, 19.
\]

There is no need to try the other case.

**Example** Suppose that \( N = 21 \) and \( \lambda(N) = 6 \). Then \( N - \phi(N) = 3 \) or 9. In the first case the quadratic is \( x^2 - 4x + 21 = 0 \), which has imaginary roots. In the second, it is \( x^2 - 10x + 21 = 0 \), with roots 3 and 7. Note that we only need the second case if \( q - 1 \) divides \( p - 1 \), since otherwise \( \lambda(N) \geq 2(p - 1) \).

Finally, we remark that, if \( \phi(N) \) or \( \lambda(N) \) is known, then problem (6) is easy. For we choose \( e \) to be the inverse of \( d \mod \lambda(N) \), using Euclid’s Algorithm.

In the other direction, if we know a solution to problem (6) (that is, if we know \( d \) and \( e \) such that \( T_e \) is the inverse of \( T_d \mod N \)), we can often factorise \( N \). The algorithm is as follows. We assume that \( N \) is the product of two primes (neither of them being 2).

Let \( de - 1 = 2^a \cdot b \), where \( b \) is odd. Choose a random \( x \) with \( 0 < x < N \).

First, calculate \( \gcd(x, N) \). If this is not 1, we’ve found a factor already and we can stop.

If \( \gcd(x, N) = 1 \), we proceed as follows. Let \( y = x^b \mod N \). If \( y \equiv \pm 1 \pmod{N} \), the algorithm has failed. Repeatedly replace
y by $y^2 \mod N$ (remembering the preceding value of $y$ - more formally, $z := y$ and $y := y^2 \mod N$) until $y \equiv \pm 1 \pmod N$.

If $y \equiv -1 \pmod N$, the algorithm has failed.

However, if $y \equiv 1 \pmod N$, then we have found $z$ such that $z^2 \equiv 1 \pmod N$ and $z \not\equiv \pm 1 \pmod N$. Then $\gcd(N, z + 1)$ and $\gcd(N, z - 1)$ are the prime factors of $N$.

Remarks:

- The chance that $\gcd(x, N) \neq 1$ is very remote. However, we should make this test, since the rest of the algorithm depends on the assumption that the gcd is 1.

- The loop where we do $z := y$ and $y := y^2 \mod N$ will be repeated at most $a$ times. For we know that $\lambda(N)$ divides $de$, so that $x^{de} \equiv x \pmod N$. Since $x$ is coprime to $N$, it has an inverse, and so $x^{de - 1} \equiv 1 \pmod N$. But $x^{de - 1} = x^{2a - b} \equiv y^a$, where $x \equiv x^b$, so after $a$ successive squarings we certainly have 1; the loop will terminate no later than this step.

- If $z^2 \equiv 1 \pmod N$, then $N$ divides $z^2 - 1 = (z + 1)(z - 1)$. Both the factors lie between 1 and $N - 1$, so $\gcd(N, z + 1)$ and $\gcd(N, z - 1)$ are proper divisors of $N$. They are coprime, so they must be the two prime factors of $N$.

- It can be shown that, choosing $x$ randomly, the probability that the algorithm succeeds in factorising $N$ is approximately $1/2$. So, by repeating a number of times with different random choices of $x$ if necessary, we can be fairly sure of finding the factorisation of $N$.

**Example**  Suppose that $N = 589$ and we are told that the private exponent corresponding to $d = 7$ is $e = 13$. Now $de - 1 = 90 = 2 \cdot 45$. Apply the algorithm with $x = 2$. We do have $\gcd(2, 589) = 1$. Now $y = 2^{45} \mod 589 = 94$. At the next stage, $z = 94$ and $y = z^2 \mod 589 = 1$. So the factors of 589 are $\gcd(589, 95) = 19$ and $\gcd(589, 93) = 31$ (these gcds are found by Euclid’s algorithm).

**Implementation**

Bob chooses two large prime numbers $p_B$ and $q_B$. This involves a certain amount of randomness. By the Prime Number Theorem a fraction of about $1/(k \ln 10)$ of $k$-digit numbers are prime. Thus, if Bob repeatedly chooses a random $k$-digit number and tests it for primality, in $mk$ trials the probability that he has failed to find a prime number is exponentially small (as a function
8.3. The RSA cryptosystem

Each primality test takes only a polynomial number of steps. The chances of success at each trial can be doubled by the obvious step of choosing only odd numbers; and excluding other small prime divisors such as 3 improve the chances still further. We conclude that in a polynomial number of steps (in terms of \( k \)), Bob will have found two primes, with an exponentially small probability of failure.

Knowing \( p_B \) and \( q_B \), Bob computes their product \( N_B = p_B q_B \). He can also compute \( \lambda(N_B) = \text{lcm}(p_B - 1, q_B - 1) \). He now computes an ‘exponent’ \( e_B \) satisfying \( \gcd(e_B, k_B) = 1 \) (again by choosing a random \( e \) and using Euclid’s algorithm). The application of Euclid’s algorithm also gives the inverse of \( e_B \mod \lambda(N_B) \), that is the number \( d_B \) such that \( e_B d_B \equiv 1 \mod \lambda(N_B) \). It follows from Proposition 8.1 that \( T_{d_B} \) is the inverse of \( T_{e_B} \), where

\[
T_{e_B} : x \mapsto x^{e_B} \pmod{N_B}.
\]

Bob publishes \( N_B \) and \( e_B \), and keeps the factorisation of \( N_B \) and the number \( d_B \) secret.

If Alice wishes to send a message to Bob, she first transforms her message into a number \( x \) less than \( N_B \). (For example, if the message is a binary string, break it into blocks of length \( k \), where \( 2^k < N_B \), and regard each block as an integer in the interval \([0, 2^k - 1]\) written to the base 2. Now she computes \( z = T_{e_B}(x) \) and sends this to Bob.

Bob deciphers the message by applying the inverse function \( T_{d_B} \) to it. This gives a number less than \( N_B \) and congruent to \( x \mod N_B \). Since \( x \) is also less than \( N_B \), the resulting decryption is correct.

If Eve intercepts the message \( z \), she has to compute \( T_{d_B}(z) \), which is a hard problem (problem (6) above). Alternatively, she could compute \( d_B \) from the published value of \( e_B \). Since \( d_B \) is the inverse of \( e_B \mod \lambda(N_B) \), this requires her to calculate \( \lambda(N_B) \), which is also hard (problem (5)). Finally, she could try to factorise \( N_B \): this, too, is hard (problem (4)). So the cipher is secure.
8. Applications to cryptography
This chapter contains some tables giving information about the smallest PLRs.
## 9.0.1 PLRs for composite odd multiples of 3

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

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\phi(n)$</th>
<th>$\lambda(n)$</th>
<th>PLR?</th>
<th>minPLR</th>
</tr>
</thead>
<tbody>
<tr>
<td>-----</td>
<td>------------</td>
<td>--------------</td>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>35</td>
<td>24</td>
<td>12</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>55</td>
<td>40</td>
<td>22</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>65</td>
<td>48</td>
<td>12</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>77</td>
<td>60</td>
<td>30</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>85</td>
<td>64</td>
<td>16</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>91</td>
<td>72</td>
<td>12</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>95</td>
<td>72</td>
<td>36</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>115</td>
<td>88</td>
<td>44</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>119</td>
<td>96</td>
<td>48</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>133</td>
<td>108</td>
<td>18</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>143</td>
<td>120</td>
<td>60</td>
<td>√</td>
<td>—</td>
</tr>
<tr>
<td>145</td>
<td>112</td>
<td>28</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>155</td>
<td>120</td>
<td>60</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>161</td>
<td>132</td>
<td>66</td>
<td>—</td>
<td>√</td>
</tr>
<tr>
<td>175</td>
<td>120</td>
<td>60</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>185</td>
<td>144</td>
<td>36</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>187</td>
<td>160</td>
<td>80</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>203</td>
<td>168</td>
<td>84</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>205</td>
<td>160</td>
<td>40</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>209</td>
<td>180</td>
<td>90</td>
<td>√</td>
<td>—</td>
</tr>
<tr>
<td>215</td>
<td>168</td>
<td>84</td>
<td>—</td>
<td>√</td>
</tr>
<tr>
<td>217</td>
<td>180</td>
<td>30</td>
<td>—</td>
<td>√</td>
</tr>
<tr>
<td>221</td>
<td>192</td>
<td>48</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>235</td>
<td>184</td>
<td>92</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>245</td>
<td>168</td>
<td>84</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>247</td>
<td>216</td>
<td>36</td>
<td>√</td>
<td>—</td>
</tr>
<tr>
<td>253</td>
<td>220</td>
<td>110</td>
<td>√</td>
<td>—</td>
</tr>
<tr>
<td>259</td>
<td>216</td>
<td>36</td>
<td>√</td>
<td>—</td>
</tr>
<tr>
<td>265</td>
<td>208</td>
<td>52</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>275</td>
<td>200</td>
<td>20</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>287</td>
<td>240</td>
<td>120</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>295</td>
<td>232</td>
<td>116</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>299</td>
<td>264</td>
<td>132</td>
<td>√</td>
<td>—</td>
</tr>
</tbody>
</table>
9. Tables of PLRs
This chapter describes some functions which can be used with GAP for computations involving primitive lambda-roots. The contents of this file can be obtained from the web page for the book. The file includes documentation explaining what the functions do.

# This file defines a number of GAP functions for computing with PLRs. #
# Please refer to "Primitive Lambda-Roots" for definitions. #
# Note one small difference - invariant factors and elementary divisors #
# are ordered differently here! (This may change.) #

# Note that GAP already defines such functions as: #
# - Lambda(n) (Carmichael's lambda-function) #
# - Phi(n) (Euler's phi-function) #
# - MoebiusMu(n) (Moebius' mu-function) #
# - OrderMod(x,n) (The order of x mod n) #
# - PowerMod(x,d,n) (x^d mod n) #
#

# The new functions are the following. The first few are calculated by #
# formulae given in "Primitive Lambda-Roots". #
# - Xi(n) (Phi(n)/Lambda(n)) #
# - LambdaStar(m) (The maximum n for which Lambda(n) divides m) #
# - ElemDivs(n) (The list of elementary divisors of U(n), #
# ordered by prime power and decreasing exponent) #
# - InvFacts(n) (The list of invariant factors of U(n), #
# ordered by reverse divisibility) #
# - NrPLRs(n) (The number of PLRs of n) #
# - NrPCs(n) (The number of power classes of PLRs of n) #
# - NrNegatingPLRs(n) (The number of negating PLRs of n) #
# - NrNegatingPCs(n) #
# - NrFraternities(n) (The number of fraternities of PLRs of n) #

71
10. GAP functions for PLRs

# From here on we don't know formulae, so we list!
# This is likely to be much slower.
# - PowerClass(x,n) (The power class of x mod n, where x is a PLR)
# - EPowerClass(x,n) (All powers of x mod n)
# - IsPLR(x,n), PLRs(n) (The test for and list of PLRs of n)
# - SmallestPLR(n) (the smallest PLR of n)
# - IsNegatingPLR(x,n), NegatingPLRs(n)
# - IsInwardPLR(x,n), InwardPLRs(n)
# - NrInwardPLRs(n) and NrInwardPCs(n)
# - IsStrongPLR(x,n), StrongPLRs(n) (strong = inward and non-negating)
# - NrStrongPLRs(n) and NrStrongPCs(n)
# - IsSelfSeekingPLR(x,n), SelfSeekingPLRs(n)
# - SubofUnits(l,n) (The subgroup of U(n) generated by the list l)
# - ListSubofUnits(l,n), NrSubofUnits(l,n)
#
# Xi(n) = Phi(n)/Lambda(n), measure of how far PLRs from primitive roots
Xi:=function(n)
  return QuoInt(Phi(n),Lambda(n));
end;

# The function "LambdaStar" is computed using the algorithm
# given in "Primitive Lambda-Roots"
# LambdaStar:=function(m)
#  local l,x,y,p;
#  if RemInt(m,2)=1 then return 2; fi;
#  l:=PrimePowersInt(m);
#  x:=2^l[l[2]+2];
#  for p in [1..QuoInt(m,2)] do
#    if RemInt(m,2*p)=0 then
#      if IsPrimeInt(2*p+1) then
#        y:=1;
#        while RemInt(m,y)=0 do y:=y*(2*p+1); od;
#        x:=x*y;
#        fi;
#    fi;
#  od;
#  return x;
#end;
# The function "ppfi" computes the prime power factors of its integer
# argument, based on the GAP function PrimePowersInt (which gives
# primes and exponents).
# ppfi:=function(n)
#  local l,11,m;
l:=PrimePowersInt(n);
ll:=[ ];
for m in [1..QuoInt(Size(l),2)] do
  Add(ll, l[2*m-1]^l[2*m]);
od;
return ll;
end;
#
# The function "orderpp" is used to put the result in order: we order
# prime powers first by the prime involved and then by the exponent.
#
orderpp:=function(q1,q2) # both prime powers
  local p1,p2;
p1:=FactorsInt(q1)[1]; p2:=FactorsInt(q2)[1];
  if p1<>p2 then
    return p1<p2;
  else
    return q1>q2;
  fi;
end;
#
# The function "ElemDivs" computes the elementary divisors of U(n),
# in the order given by the function "orderpp" above.
# It computes the elementary divisors of U(q) for the
# prime power factors q of n and concatenate.
# If q is even then ElemDivs = [], [2], or [q/4,2] according as
# q=2, 4, or >4.
# If q is odd then ElemDivs is the list of prime power factors of Phi(q).
# Finally sort the list using the ordering given by "orderpp".
#
ElemDivs:=function(n)
  local l, ll, x;
l:=ppfi(n);
ll:=[ ];
for x in l do
  if RemInt(x,2)=0 then
    if x>2 then Add(ll,2); fi;
    if x>4 then Add(ll,QuoInt(x,4)); fi;
  else
    Append(ll,ppfi(Phi(x))); fi;
  od;
Sort(ll,orderpp); return ll;
end;
#
# The function "InvFacts" computes the invariant factors of U(n),
# in decreasing order by divisibility.
# It starts with the elementary divisors and combines them in the
# usual way.
# Note that the largest invariant factor is Lambda(n).
# isnull := function(x)
  return x<>[];
end;

# InvFacts := function(n)
local l, ll, lll, m, x;
l := ElemDivs(n); lll := [];
while l<>[] do
  ll := List(l, x->PrimePowersInt(x));
m := Size(l); x := 1;
  while m>=1 do
    if (m=1) or (ll[m][1]<>ll[m-1][1]) then
      x := x*l[m]; l[m] := [];
    fi;
m := m-1;
  od;
  Add(lll, x); l := Filtered(l, isnull);
  od;
return lll;
end;

# The function "eltsoforder" finds the number of elements of order m
# in an abelian group where l is the list of cyclic factors in any
# direct sum decomposition. See "Primitive Lambda-Roots".
eltsoforder := function(m, l)
local t, x, y, z;
x := 0;
for t in [1..m] do
  if RemInt(m, t)=0 then
    y := MoebiusMu(QuoInt(m, t));
    for z in l do y := y*GcdInt(t, z) od;
x := x+y;
  fi;
od;
return x;
end;

# Now the number of PLRs is obtained when
# l is the list of invariant factors
# and m is its first element
NrPLRs := function(n)
local l;
l := InvFacts(n);
if n<=2 then return 1; fi;
return eltsoforder(l[1], l);
end;

#
# The size of a power class is $\phi(\Lambda(n))$. Dividing by this number
# gives the number of power classes of PLRs
#
NrPCs:=function(n)
return QuoInt(NrPLRs(n),\phi(\Lambda(n)));
end;
#
# The number of negating PLRs is zero if the Sylow $2$-subgroup is not
# homocyclic, and is $1/(2^s - 1)$ of the number of PLRs if it is
# homocyclic of rank $s$. See "Primitive Lambda-Roots".
#
NrNegatingPLRs:=function(n)
local l,s;
if n<=2 then return 1; fi; # otherwise $l[1]$ is even
l:=ElemDivs(n);
s:=0;
while Size(l) >= s+1 and RemInt(l[s+1],2)=0 do s:=s+1; od;
if l[1]=l[s] then return QuoInt(NrPLRs(n),2^s-1);
else return 0;
fi;
end;
#
NrNegatingPCs:=function(n)
return QuoInt(NrNegatingPLRs(n),\phi(\Lambda(n)));
end;
#
# NrFraternities(n) returns the number of fraternities of $n$
#
NrFraternities:=function(n)
local l,s,e;
if n<=2 then return 1; fi;
l:=ElemDivs(n);
s:=0;
while Size(l) >= s+1 and RemInt(l[s+1],2)=0 do s:=s+1; od;
if l[1]>2 then return QuoInt(NrPLRs(n), 2^s);
else return QuoInt(NrPLRs(n), 2^s-1);
fi;
end;
#
# IsPLR(x,n) checks if $x$ is a PLR of $n$
#
IsPLR:=function(x,n)
return OrderMod(x,n)=\Lambda(n);
end;
#
# SmallestPLR(n) does what it says
#
SmallestPLR:=function(n)
local x,m;
x:=0; m:=\Lambda(n);
while OrderMod(x,n)<m do x:=x+1; od;
return x;
end;
#
# PowerClass(x,n) gives the power class of x mod n
#
PowerClass:=function(x,n) # we assume x is a PLR
local l,i;
l:=[ ];
for i in [1..Lambda(n)] do
  if GcdInt(i,Lambda(n))=1 then Add(l,PowerMod(x,i,n)); fi;
od;
return Set(l);
end;
#
# EPowerClass:=function(x,n) # all powers!
local l,i;
l:=[ ];
for i in [1..Lambda(n)] do Add(l,PowerMod(x,i,n)); od;
return Set(l);
end;
#
# Produce a list of PLRs by direct checking
#
PLRs:=function(n)
local x,l,m;
l:=[ ]; m:=Lambda(n);
for x in [0..n-1] do
  if OrderMod(x,n)=m then Add(l,x); fi;
od;
return l;
end;
#
# Code for listing negating PLRs
#
IsNegatingPLR:=function(x,n)
local e;
e:=QuoInt(Lambda(n),2);
return PowerMod(x,e,n)=n-1;
end;
#
# NegatingPLRs:=function(n)
local e;
e:=QuoInt(Lambda(n),2);
return Filtered(PLRs(n), x->PowerMod(x,e,n)=n-1);
end;
#
# Code for listing inward PLRs
#
IsInwardPLR:=function(x,n)
return GcdInt(x-1,n)=1;
end;
#
InwardPLRs:=function(n)
return Filtered(PLRs(n), x->GcdInt(x-1,n)=1);
end;
#
NrInwardPLRs:=function(n);
return Size(InwardPLRs(n));
end;
#
NrInwardPCs:=function(n);
return QuoInt(NrInwardPLRs(n),Phi(Lambda(n)));
end;
#
# Code for strong PLRs
#
IsStrongPLR:=function(x,n)
return IsInwardPLR(x,n) and not IsNegatingPLR(x,n);
end;
#
StrongPLRs:=function(n)
local e;
e:=QuoInt(Lambda(n),2);
return Filtered(InwardPLRs(n),x->PowerMod(x,e,n)<n-1);
end;
#
NrStrongPLRs:=function(n)
return Size(StrongPLRs(n));
end;
#
NrStrongPCs:=function(n)
return QuoInt(NrStrongPLRs(n),Phi(Lambda(n)));  
end;
#
# Code for self-seeking PLRs
#
IsSelfSeekingPLR:=function(x,n)
local l;
l:=EPowerClass(x,n);
return (IsStrongPLR(x,n) and ((x-1 in l) or (n+1-x in l)));
end;
#
SelfSeekingPLRs:=function(n)
return Filtered(StrongPLRs(n),x->IsSelfSeekingPLR(x,n));
end;
#
# "SubofUnits" returns the subgroup of U(n) generated by l
#
SubofUnits:=function(l,n)
local R,U,x;
for x in l do
    if GcdInt(x,n)<>1 then return fail; fi;
od;
R:=ZmodnZ(n); U:=Units(R);
return Subgroup(U,List(1,x->ZmodnZObj(x,n)));
end;

ListSubofUnits:=function(l,n)
    local ll;
    ll:=SubofUnits(l,n); if ll=fail then return fail; fi;
    return Set(List(Set(ll), x-> Int(x)));
end;

NrSubofUnits:=function(l,n)
    local ll;
    ll:=SubofUnits(l,n); if ll=fail then return fail; fi;
    return Size(ll);
end;
Bibliography


Bibliography


