M829
ANALYTIC NUMBER THEORY II

Course Notes

Prepared by
Robin Wilson
Contents

Introduction 2

Chapter 8 Periodic arithmetical functions and Gauss sums 3
  Study Session 1: Section 8.1–8.3 (pages 157–162) 3
  Study Session 2: Sections 8.5–8.8 (pages 165–170) 6
  Study Session 3: Sections 8.9–8.12 (pages 171–174) 7

Chapter 9 (last part) Gauss sums and quadratic reciprocity 10
  Study Session 1: Review of Sections 9.1–9.5,
  and Section 9.9 (pages 192–195) 10
  Study Session 2: Sections 9.10–9.11 (pages 195–201) 12

Chapter 10 Primitive roots 16
  Study Session 1: Sections 10.1–10.3 and 10.10
  (pages 204–206 and 213–217) 16
  Study Session 2: Sections 10.4–10.9 (pages 206–213) 18
  Study Session 3: Sections 10.11–10.13 (pages 218–222) 21

Chapter 11 Dirichlet series and Euler products 23
  Study Session 1: Sections 11.1–11.3 (pages 224–227) 23
  Study Session 2: Sections 11.4–11.6 (pages 228–234) 25
  Study Session 3: Sections 11.7–11.9 (pages 234–239) 27

Chapter 12 The functions $\zeta(s)$ and $L(s, \chi)$ 31
  Study Session 1: Sections 12.1–12.4 (pages 249–254) 31
  Study Session 2: Sections 12.5–12.8 (pages 254–260) 34
  Study Session 3: Sections 12.11–12.14 (pages 264–270) 36

Chapter 13 Analytic proof of the prime number theorem 38
  Study Session 1: Sections 13.1–13.3 (pages 278–284) 38
  Study Session 2: Sections 13.4–13.6 (pages 284–289) 40
  Study Session 3: Sections 13.7–13.9 (pages 289–293) 41

Chapter 14 Partitions 43
  Study Session 1: Sections 14.1–14.4 (pages 304–313) 43
  Study Session 2: Sections 14.5–14.7 (pages 313–318) 46
  Study Session 3: Sections 14.8–14.11 (pages 318–324) 48

Postscript 50

Further reading 50

Solutions to the Self-assessment questions 51

Solutions to the Problems 72
Introduction

In this course we study the use of complex analysis in number theory — in particular, the use of the calculus of residues. The main goals of the course are the investigation of primitive roots, the study of Dirichlet series, two analytic proofs of the celebrated prime number theorem and, to conclude, an introduction to Euler’s work on partitions.

As with M823, this course is based on Introduction to Analytic Number Theory by T. M. Apostol. The former course used material from Chapters 1–7 and part of Chapter 9. M829 is based on the remaining chapters, together with a small amount of additional material. As before, these notes will guide you through Apostol’s book, telling you which sections to read, explaining difficult points, and setting Self-assessment Questions (SAQs) and Problems to test your understanding of the material. Full solutions will be found at the end of the Course Notes.

To help you organize your work, we have divided each chapter into two or three study sessions, each covering several sections of the book and each planned to correspond to about three hours’ work. Do not become unduly discouraged if some of the material seems difficult or time-consuming. In particular, you may find that Chapters 8 and 9 are more difficult than Chapter 10, and that some of the contour integration in Chapters 9 and 13 is very time-consuming. We have tried to alleviate the difficulties, in our commentaries, but you should not expect this course to be an easy one.

In order to pace you through the course, we have set four Tutor-marked Assignments (TMAs). These are compulsory in that you cannot pass the course without obtaining a reasonable average grade on them. Your TMAs carry 50% of the total marks for the course, the remaining 50% coming from the three-hour examination at the end of the course. Please note that we cannot accept any TMAs received after the cut-off dates, unless previously arranged with your tutor.

Further information about the assessment and about the telephone answering set-up will be sent to you in the various Stop Presses issued throughout the course.

It is possible that there are errors in these notes, and that we have not found all the errors in Apostol’s book. We should be grateful if you could inform us of any errors or misprints and of any suggested improvements to the Course Notes.
Chapter 8  Periodic arithmetical functions and Gauss sums

In this chapter we introduce various ‘exponential sums’, and show how every periodic function mod $k$ can be expressed as an exponential sum $\sum c(m)e^{2\pi imn/k}$. We then study Ramanujan’s sums, which are exponential sums generalizing the Möbius function. The second half of the chapter is concerned with Gauss sums and their connections with various types of character. Finally, these two topics are brought together in Theorem 8.20, which evaluates the Fourier expansion of a primitive Dirichlet character.

This chapter splits into THREE study sessions.

Study Session 1: Sections 8.1–8.3 (pages 157–162)
Study Session 2: Sections 8.5–8.8 (pages 165–170)
Study Session 3: Sections 8.9–8.12 (pages 171–174)

Section 8.4 is NOT part of the course.

Study Session 1: Section 8.1–8.3 (pages 157–162)

Read  Section 8.1

Commentary

1. Note that a periodic function with period $k$ can be specified uniquely by giving the values $f(0), f(1), \ldots, f(k-1)$. For example, to construct a periodic function with period 5, we choose (say) $f(0) = 4, f(1) = 17, f(2) = -3, f(3) = \frac{1}{2}$ and $f(4) = 2$. Then, for all $n$, $f(5n) = 4, f(5n+1) = 17, f(5n+2) = -3, f(5n+3) = \frac{1}{2}$ and $f(5n+4) = 2$.

2. The exponential function examples are often easier to understand if you let some symbol (such as $x$) stand for an appropriate $k$th root of unity. For example, $f(n) = e^{2\pi imn/k}$ is more clearly expressed as $f(n) = x^n$, where $x = e^{2\pi i/k}$ (so $x^k = 1$). Similarly, if $x = e^{2\pi i/k}$, then $\sum c(m)e^{2\pi imn/k} = \sum c(m)(x^n)^m$.

3. The proof of Theorem 8.1. Recall that the sum of the general geometric series

$$a + ar + ar^2 + \cdots + ar^{k-1}$$

is $a(r^k - 1) / (r - 1)$, if $r \neq 1$.

In this case, $a = 1$ and $r = x$. 

Self-assessment questions

8.1 If \( x = e^{2\pi i/k} \), prove that \( \sum_{n=1}^{k-1} nx^n = k/(x - 1) \), for \( k > 1 \).

8.2 Construct a periodic function \( f \) with period 4 for which \( f(11) = 1 \) and \( f(22) = 2 \).

8.3 Let \( x \) be a complex cube root of unity, so that \( x^3 = 1 \) but \( x \neq 1 \).

What are the values of the following?
(a) \( 1 + x^2 + x^4 \)
(b) \( 1 + x^5 + x^{10} \)
(c) \( 1 + x^9 + x^{18} \)

8.4 Verify the statement of Theorem 8.1 when \( k = 4 \) and \( n = 7 \) and 8.

---

**Commentary**

1. **The proof of Theorem 8.2.** As an example, let \( k = 3 \), \( z_0 = 1 \), \( z_1 = x \) and \( z_2 = x^2 \), where \( x \) and \( x^2 \) are complex cube roots of unity and \( w_0 = 1 + 2i \), \( w_1 = 3 - 5i \), \( w_2 = 7 - 2i \). Then \( A(z) = (z - 1)(z - x)(z - x^2) \), and \( A_0(z) = (z - x)(z - x^2) \), \( A_1(z) = (z - 1)(z - x^2) \), \( A_2(z) = (z - 1)(z - x) \).

The required quadratic polynomial is therefore

\[
P(z) = (1 + 2i) \frac{(z - x)(z - x^2)}{(1 - x)(1 - x^2)} + (3 - 5i) \frac{(z - 1)(z - x^2)}{(x - 1)(x - x^2)} + (7 - 2i) \frac{(z - 1)(z - x)}{(x^2 - 1)(x^2 - x)}.
\]

as can be seen by substituting \( z = 1 \), \( z = x \) and \( z = x^2 \).

2. **The statement of Theorem 8.3.** If \( x = e^{2\pi i/k} \), then

\[
w_m = a_0 + a_1 x^m + \cdots + a_{k-1} x^{(k-1)m} \]

and

\[
a_n = \frac{1}{k} \left( w_0 + w_1 x^{-n} + \cdots + w_{k-1} x^{-(k-1)n} \right).
\]

3. **Page 159, lines –9 to –6.** Since \( w_m = \sum_n a_n x^{mn} \), we have

\[
w_m x^{-mr} = \sum_n a_n x^{(n-r)m},
\]

and so

\[
\sum_m w_m x^{-mr} = \sum_n a_n \sum_m x^{(n-r)m}.
\]

4. **The middle of page 160.** Note the similarity between these results and the standard Fourier series. For example, if we have a Fourier sine series for an odd function

\[
f(x) = \sum_{n=1}^{\infty} a(n) \sin nx, \quad \text{then} \quad a(n) = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \sin nx \, dx.
\]
Self-assessment questions

8.5 Find a polynomial $P(z)$ of degree 3 such that $P(1) = 1 + i$, $P(-1) = 1 - i$, $P(i) = 1 + 2i$ and $P(-i) = 1 - 2i$.

8.6 Verify equation (2) on page 159 for the example in SAQ 8.5.

8.7 In Theorem 8.4, calculate $g(n)$ when $k = 6$ and $f$ is the nonprincipal character mod 6.

Read Section 8.3

Commentary

1. The beginning of Section 8.3. To prove that $\mu(k)$ is the sum of the primitive $k$th roots of unity (that is, complex numbers $x$ such that $x^k = 1$, but $x^r \neq 1$ if $r < k$), we argue as follows.

Let $f(d) = \sum_{1 \leq a \leq d \atop (a,d)=1} e^{2\pi i a/d}$ and $g(k) = \sum_{1 \leq m \leq k} e^{2\pi i m/k}$.

Then $g(k) = \sum_{d|k} f(d)$, since every fraction $m/k$ can be reduced to ‘lowest terms’ $a/d$, where $d|k$ and $1 \leq a \leq d$, $(a,d) = 1$. It follows from the Möbius inversion formula that

$$f(k) = \sum_{d|k} \mu\left(\frac{k}{d}\right) g(d) = \sum_{d|k} \mu\left(\frac{k}{d}\right) \sum_{1 \leq m \leq d} e^{2\pi i m/d}.$$ 

But this last sum is 0 unless $d = 1$ (by Theorem 8.1 with $n = 1$).

So $f(k) = \mu(k)$, as required.

2. Page 161, line 8. The equation $\sum_{d|k} d \mu(k/d) = \phi(k)$ was proved in Theorem 2.3, with $d$ replaced by $n/d$ and $k$ replaced by $n$.

3. The proof of Theorem 8.5. Note that in the application of Theorem 8.4, the letters $m$ and $n$ have been interchanged.

Self-assessment questions

8.8 Calculate the Ramanujan sums $c_4(3)$, $c_8(2)$ and $c_6(3)$, both from the definition and from Theorem 8.6.

8.9 Use Theorem 8.6 to find $c_k(n)$ when $(n, k) = 1$.

8.10 Write down the values of $c_{12}(n)$ for $n = 1, 2, \ldots, 12$.

8.11 Write out the statement and proof of Theorem 8.5 when $f(k) = k$ and $g(k) = \mu(k)$.
Problems for Sections 8.1–8.3

8A Give a direct proof of Theorem 8.6, using the method of Commentary 1 above.

8B Apostol, page 175, number 3, (a) and (b).

Study Session 2: Sections 8.5–8.8 (pages 165–170)

Read Sections 8.5 and 8.6

Commentary

1. The statement of Theorem 8.9. Note that if χ is the principal character χ_1 mod k, then this statement reduces to c_k(n) = μ(k) if (n,k) = 1.

2. The proof of Theorem 8.9. The first sentence follows from Theorem 5.11. In the last line of equations, m has been substituted for nr.

3. The definition of ‘separable’. As an example, let χ be the nonprincipal character mod 4. Then e^{2πni/4} = i, and so

\[ G(n, \chi) = \chi(1)^n + \chi(3)3^n i^n (1 - (-1)^n) = \begin{cases} 2i, & \text{if } n \equiv 1 \pmod{4} \\ -2i, & \text{if } n \equiv 3 \pmod{4} \\ 0, & \text{if } n \equiv 0 \text{ or } 2 \pmod{4}. \end{cases} \]

It follows easily that G(n, \chi) = \chi(n)G(1, \chi) in each case.

4. The statements of Theorems 8.10 and 8.11. If χ is the nonprincipal character mod 4, then it follows from the above commentary that G(n, \chi) = 0 if (n,4) > 1, and |G(1, \chi)|^2 = 4.

5. The statement of Theorem 8.12. If χ is the nonprincipal character mod 6, then it is easy to check that G(n, \chi) \neq 0 when n = 2 or 4 (see SAQ 8.12). In this case, we have d = 3, since χ(a) = 1 whenever (a,6) = 1 and a \equiv 1 \pmod{3}, a = 1 being the only possible value modulo 6.

6. The proof of Theorem 8.12. To say that anm/k \equiv nm/k (mod 1) means simply that anm/k and nm/k differ by an integer, and hence e^{2πianm/k} = e^{2πnm/k}.

Self-assessment questions

8.12 Show that if χ is the nonprincipal character mod 6, then G(2, \chi) and G(4, \chi) are not separable, and |G(1, \chi)|^2 \neq 6.

8.13 Verify that G(n, \chi) is separable for every n when χ is the character χ_3 mod 5 defined on page 139.

Read Sections 8.7 and 8.8
Commentary

1. *The definition of induced modulus.* We have seen above that if \( \chi \) is the nonprincipal character mod 6, then 3 is an induced modulus. The other examples we considered (mod 4 and mod 5) have no induced modulus.

2. *Definition of primitive character.* Note that the characters in Commentary 3 above and SAQ 8.13 are all primitive.

3. *The Note on page 168.* The proof of the converse result (Theorem 8.19), although not difficult, is NOT part of the course.

4. *Example 2 on page 169.* This is the example we considered above, in Commentary 5 and SAQ 8.12.

5. *The proof of Theorem 8.17.* The ‘members’ of (17), referred to twice, mean the two sides of the equation.

Self-assessment questions

8.14 If \( \chi_1 \) is the principal character mod \( k \) and \( d | k \), show that \( d \) is an induced modulus for \( \chi_1 \).

8.15 (a) Write down all the nonprincipal characters mod 8 and mod 12, and determine which of them have an induced modulus.
   (b) For each character \( \chi \) in part (a) with an induced modulus \( d \), find a character \( \psi \) mod \( d \) such that \( \chi(n) = \psi(n) \chi_1(n) \) for all \( n \).

Problems for Sections 8.5–8.8

8C Apostol, page 175, number 6.
8D Apostol, page 175, number 8.
8E Apostol, page 176, number 9.
8F Apostol, page 176, number 11.

Study Session 3: Sections 8.9–8.12 (pages 171–174)

*Read* Sections 8.9 and 8.10, omitting the proof of Theorem 8.19

Commentary

1. *The statement of Theorem 8.18.* If \( \chi \) is the character mod 9 in Example 1 on page 169, then the conductor is 3, and \( \chi(n) = \psi(n) \chi_1(n) \), where \( \psi \) is as given.

\[
\begin{array}{c|cccccccc}
  n & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
\hline
  \psi(n) & 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 & 0 \\
  \chi_1(n) & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\
  \chi(n) & 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 & 0 \\
\end{array}
\]
Similarly, if \( \chi \) is the character mod 6 in Example 2, then the conductor is again 3, and \( \chi(n) = \psi(n)\chi_1(n) \), with the same function \( \psi \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \psi(n) )</td>
<td>1</td>
<td>−1</td>
<td>0</td>
<td>1</td>
<td>−1</td>
<td>0</td>
</tr>
<tr>
<td>( \chi_1(n) )</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( \chi(n) )</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>−1</td>
<td>0</td>
</tr>
</tbody>
</table>

2. *The statement of Theorem 8.19.* This is the ‘converse’ of Theorem 8.15, referred to in the note on page 168. The proof of this converse result is NOT part of this course; it uses Theorem 5.33(a), which was omitted from M823.

### Self-assessment questions

8.16 Find the conductor of each of the four characters mod 12, and verify the statement of Theorem 8.18 in each case.

8.17 There are two primitive characters \( \chi \) mod 8. Find them, and verify in each case that \( G(n, \chi) \) is separable for \( n = 5 \) and \( n = 7 \).

**Read** Sections 8.11 and 8.12

### Commentary

1. *Equation (19).* Here, and in what follows, all summations range from 1 to \( k \) instead of from 0 to \( k - 1 \) (as used, for example, in Theorem 8.4); clearly this makes no difference.

2. *The statement of Theorem 8.20.* As an example, let \( \chi \) be the nonprincipal character mod 3, and let \( \omega = e^{2\pi i/3} \). Then
\[
\tau_k(\chi) = \frac{1}{\sqrt{3}}(\omega - \omega^2) = i
\]
and
\[
\chi(m) = \frac{i}{\sqrt{3}}(\omega^m - \omega^{-2m}) = \begin{cases} 
0, & \text{if } m \equiv 0 \pmod{3} \\
1, & \text{if } m \equiv 1 \pmod{3} \\
-1, & \text{if } m \equiv 2 \pmod{3}.
\end{cases}
\]

3. *The proof of Theorem 8.20.* By Theorem 8.19, \( \chi \) is separable, and so \( G(-n, \chi) = \frac{\tau(-n)G(1, \chi)}{\tau(1)} \). The rest of the proof is straightforward.

4. *The statement of Theorem 8.21.* The upper bound of \( \sqrt{k} \log k \) is a considerable improvement on \( \phi(k) \) since, by Theorem 3.7, \( \phi(k) \) has average order \( 3k/\pi^2 \). In many cases, even the upper bound of \( \sqrt{k} \log k \) is rather weak — for example, if \( \chi \) is the primitive character mod 4, then
\[
\sum_{m \leq x} \chi(m) = 1 \text{ or } 0, \quad \text{whereas } \sqrt{4} \log 4 = 2.77.
\]
5. The proof of Theorem 8.21. The first few lines of the proof, on page 173, are straightforward. At the top of page 174, the sum \( \sum_{n \leq k} |f(n)| \) is replaced by

\[
2 \sum_{n \leq \frac{1}{2}k} |f(n)|, \text{ and } f(n) \text{ is then estimated by summing the geometric series.}
\]

The inequality \( \sin t \geq 2t/\pi \), for \( 0 \leq t \leq \frac{1}{2} \pi \), can be established by drawing the graphs of \( y = \sin t \) and \( y = 2t/\pi \).

![Graph of \( y = \sin t \) and \( y = 2t/\pi \)]

Alternatively, we observe that

if \( f(t) = \frac{\sin t}{t} \), then \( f'(t) = \frac{t - \tan t}{t^2 \sec t} \),

which is negative for \( 0 < t < \frac{1}{2} \pi \); thus \( f \) is decreasing over this interval, and hence \( \frac{\sin t}{t} \geq \frac{\sin \frac{1}{2} \pi}{\frac{1}{2} \pi} \).

Self-assessment questions

8.18 Calculate \( \tau_8(\chi) \) for each of the primitive characters \( \chi \mod 8 \). In each case, verify that \( |\tau_8(\chi)| = 1 \).

8.19 Verify equation (21) for \( m = 1, 2 \) and 3, when \( \chi \) is the primitive character \( \mod 4 \).

8.20 Verify the statement of Pólya’s inequality when \( x = 13 \), for each of the primitive characters \( \chi \mod 8 \).

Problems for Sections 8.9–8.12

8G Apostol, page 175, number 7.

8H Apostol, page 176, number 10.

8I Apostol, page 176, number 13.
Chapter 9 (last part)  Gauss sums and quadratic reciprocity

In the first part of Chapter 9 (in M823) we introduced quadratic residues and gave Gauss’ proof of the quadratic reciprocity law. We now show how the material on Gauss sums in Chapter 8 can be used to obtain other proofs of the quadratic reciprocity law. The main part of one such proof makes extensive use of the calculus of residues.

This chapter splits into TWO study sessions.

Study Session 1: Review of Sections 9.1–9.5, and Section 9.9 (pages 192–195)

Study Session 2: Sections 9.10–9.11 (pages 195–201)

Study Session 1: Review of Sections 9.1–9.5, and Section 9.9 (pages 192–195)

Review Sections 9.1–9.5

The results from these sections which will be needed later in the chapter are as follows.

Commentary

1. The Legendre symbol is completely multiplicative:

\[(r|p)(s|p) = (rs|p);\]  

in particular, \((r^2|p) = 1\) for all \(r\). (Theorem 9.3)

2. \((m|p) = (n|p)\) whenever \(m \equiv n \pmod{p}\).

3. Any reduced residue system mod \(p\) contains \(\frac{1}{2}(p-1)\) quadratic residues and \(\frac{1}{2}(p-1)\) quadratic nonresidues. Thus

\[\sum_{t=1}^{p-1} (t|p) = 0.\]  

(Theorem 9.1)

4. Euler’s criterion. If \(p\) is an odd prime, then

\[(n|p) \equiv n^{(p-1)/2} \pmod{p}, \quad \text{for all } n.\]  

(Theorem 9.2)

5. The quadratic reciprocity law. If \(p\) and \(q\) are distinct odd primes, then

\[(p|q)(q|p) = (-1)^{(p-1)(q-1)/4}.\]  

(Theorem 9.8)

6. \((-1|p) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4} \\ -1, & \text{if } p \equiv 3 \pmod{4}; \end{cases}\)  

\[(2|p) = \begin{cases} 1, & \text{if } p \equiv 1 \text{ or } 7 \pmod{8} \\ -1, & \text{if } p \equiv 3 \text{ or } 5 \pmod{8}. \end{cases}\]  

(Theorem 9.4)
Commentary

1. Equation (16). The fact that \((r|p)\) is a character mod \(p\) follows from the note at the top of page 181.

2. The statement of Theorem 9.13. Note that, by Theorem 9.4, \(G(1, \chi)^2 = p\) if \(p \equiv 1 \mod{4}\), and \(G(1, \chi)^2 = -p\) if \(p \equiv 3 \mod{4}\).
   For example, if \(p = 3\), then \(G(1, \chi) = \omega - \omega^2 = i\sqrt{3}\) (where \(\omega^3 = 1\)), so \(G(1, \chi)^2 = -3\); if \(p = 5\), then \(G(1, \chi) = \tau - \tau^2 - \tau^3 + \tau^4\) (where \(\tau^5 = 1\)), so
   \[
   G(1, \chi)^2 = (\tau - \tau^2 - \tau^3 + \tau^4)^2 = 4 - \tau - \tau^2 - \tau^3 - \tau^4
   = 5, \quad \text{since } 1 + \tau + \tau^2 + \tau^3 + \tau^4 = 0.
   \]

3. The proof of Theorem 9.13. The last equation on page 192 follows from Theorem 8.1, making adjustments for the fact that the term corresponding to \(r = 0\) is missing. To obtain the equation at the top of page 193, we split off the term for which \(p \mid (1 + t)\) (that is, \(t = p - 1\)).

4. The statement of Theorem 9.14. This theorem shows the equivalence of the quadratic reciprocity law and the congruence (20). In Theorem 9.15 we obtain an identity from which (20) can be deduced, thereby yielding a proof of the quadratic reciprocity law. The proof of Theorem 9.14 is straightforward.

5. The proof of Theorem 9.15. The existence and form of the finite Fourier expansion follow from Theorem 8.4. The rest of the proof is straightforward.
   Note that the line
   \[
   G(1, \chi)G(-1, \chi) = G(1, \chi)\overline{G(1, \chi)} = |G(1, \chi)|^2 = p
   \]
   could be replaced by the following, which uses the separability of \(G\):
   \[
   G(1, \chi)G(-1, \chi) = G(1, \chi)(-1|p)G(1, \chi) = (-1|p)^2p = p.
   \]

6. The proof of the reciprocity law. The first statement follows from equations (20) and (23). To illustrate the rest of the proof, we take \(p = 5\) and \(q = 3\). Then equations (26) and (27) become
   \[
   \sum_{r_1 \equiv 0 \mod{5}} \sum_{r_2 \equiv 0 \mod{5}} \sum_{r_3 \equiv 0 \mod{5}} (r_1r_2r_3|p) \equiv 1 \mod{3}, \quad r_1 + r_2 + r_3 \equiv 3 \mod{5}.
   \]
   If \(r_1 \equiv r_2 \equiv r_3 \equiv 1 \mod{5}\), then each \(r_i \equiv 1 \mod{5}\), so the left-hand side becomes \((1|p)\). Any other term such as that corresponding to \(r_1 \equiv 1, r_2 \equiv 3\) and \(r_3 \equiv 4 \mod{5}\) can be combined with the two other terms obtained by a cyclic permutation (in this case, \(r_1 \equiv 3, r_2 \equiv 4, r_3 \equiv 1\), and \(r_1 \equiv 4, r_2 \equiv 1, r_3 \equiv 3\), and these terms contribute \(3(1 \cdot 3 \cdot 4|p) \equiv 0 \mod{3}\) to the left-hand side. Thus the only non-zero term remaining on the left-hand side is \((1|p) = 1\).

Self-assessment questions

9.1 Verify the statement of Theorem 9.13 when \(p = 11\) and \(p = 13\).
9.2 Assuming the quadratic reciprocity law, verify in each of the following cases that $G(1, \chi)^{q-1} \equiv (q|p) \pmod{q}$.

(a) $p = 13, \quad q = 17$  
(b) $p = 11, \quad q = 13$  
(c) $p = 13, \quad q = 11$  
(d) $p = 11, \quad q = 19$

9.3 Find all the solutions of equation (27) when $p = 5$ and $q = 3$, and hence verify Theorem 9.15 in this case.

**Problems for Section 9.9**

9A Let $p$ be an odd prime, and $\chi(n) = (n|p)$. Prove that the Gauss sum $G(n, \chi)$ is identical to the quadratic Gauss sum $G(n; p) = \sum_{r=1}^{p} e^{2\pi ir^2/p}$ if $p \nmid n$.

Are they equal if $p|n$?

9B Verify Theorem 9.15 when $p = 3$ and $q = 5$.

**Study Session 2: Sections 9.10–9.11 (pages 195–201)**

**Read** Sections 9.10 and 9.11, omitting the proof of Theorem 9.16

**Commentary**

1. This reading section involves the use of quadratic Gauss sums which you met in the TMA for Chapter 8. Their main properties are listed in Exercise 16 on page 177. Note that the proof of Theorem 9.16, which we omit for the time being, forms the next reading section.

2. *Equation (29).* We asked you to prove in Problem 9A above that $G(n; p) = G(n, \chi)$, and the result follows by separability.

3. *Equation (30).* Note that $1 + e^{-\pi im/2} = (1 + \cos \frac{1}{2} \pi m) - i \sin \frac{1}{2} \pi m$, which equals $1 - i$ if $m \equiv 1 \pmod{4}$, $0$ if $m \equiv 2 \pmod{4}$, $1 + i$ if $m \equiv 3 \pmod{4}$, and $2$ if $m \equiv 0 \pmod{4}$.

4. *The note on page 196.* Note that $S(m, 2) = \sum_{r=0}^{1} e^{-\pi ir^2/2} = 1 + e^{-\pi im/2}$, as stated.

5. *The statement of Theorem 9.17.* Note that if we put $h = 1, \quad k = m$ into equation (44), then $G(k; h) = 1$, and the reciprocity law reduces to equation (30) on page 195.

6. *The proof of Theorem 9.17.* Most of this proof is straightforward. In the final set of equalities, note that

$$
\sum_{s=0}^{h-1} e^{-\pi ik(2s+h)^2/2h} = \sum_{s=0}^{h-1} e^{-2\pi ik^2/h} e^{-\piikh/2} = e^{-\piikh/2} \sum_{s=0}^{h-1} e^{-2\pi ik^2/h}.
$$
7. **Section 9.11.** This section is straightforward, and should cause you no difficulties. The ‘multiplicative property’ given here is the result we asked you to prove in the TMA for Chapter 8.

**Self-assessment questions**

9.4 Evaluate $G(1; m)$ for $m = 3, 4$ and $6$, and check that your answers agree with equation (30).

9.5 Evaluate $S(a, m)$ when
   (a) $a = 2, m = 1$;  
   (b) $a = 1, m = 2$;  
   (c) $a = 3, m = 4$.

9.6 Verify equation (29) when $n = 2$ and $p = 5$ and 7.

9.7 Use equation (30) to verify Theorem 9.17 when $h = 5$ and $k = 7$.

---

**Read** the proof of Theorem 9.16

**Commentary**

1. This proof is rather complicated, and you are not expected to understand all of the details. An alternative proof of equation (30) will be outlined in the TMA for this chapter.

2. The basic idea of the proof is to consider the integral of the function

\[ f(z) = \sum_{r=0}^{m-1} e^{\pi ia(z+r)^2/m} / (e^{2\pi iz} - 1) \]

around the contour shown in Figure 9.1. The only singularity of $f$ inside this contour is a simple pole at 0 with residue $S(a, m) / 2\pi i$, and so, by Cauchy’s residue theorem, the value of the integral is precisely $S(a, m)$. The integrals along the top and bottom of the parallelogram are estimated, and are shown to tend to zero as $R \to \infty$. The integrals from $A + 1$ to $B + 1$ and from $B$ to $A$ combine to give an integral involving

\[ \phi(z) = e^{\piiaz^2/m} \sum_{n=0}^{a-1} e^{2\pi inz}, \]

and this integral is estimated using two further parallelogram contours.

3. **Page 196, line 10.**

\[ g(z + 1) - g(z) = \sum_{r=0}^{m-1} e^{\pi ia(z+r+1)^2/m} - \sum_{r=0}^{m-1} e^{\pi ia(z+r)^2/m} \]

\[ = \left( \sum_{r=1}^{m} - \sum_{r=0}^{m-1} \right) e^{\pi ia(z+r)^2/m} = e^{\pi ia(z+m)^2/m} - e^{\piiaz^2/m} \]

\[ = e^{\piiaz^2/m} \left( e^{\pi ia(2z+m)} - 1 \right) = e^{\piiaz^2/m} \left( e^{2\pi ia} - 1 \right) \]

\[ = e^{\piiaz^2/m} \left( e^{2\pi iz} - 1 \left( 1 + e^{2\pi iz} + e^{4\pi iz} + \ldots + e^{2\pi i(a-1)} \right) \right) \]

\[ = e^{\piiaz^2/m} \left( e^{2\pi iz} - 1 \right) \sum_{n=0}^{a-1} e^{2\pi inz}, \text{ as required.} \]
4. **Figure 9.1.** Note that the diagonal sides of the parallelogram cross the \(x\)-axis at the points \(-\frac{1}{2}\) and \(\frac{1}{2}\). Since the poles of \(f\) occur at the integers, the only pole lying inside the parallelogram is the pole at 0.

5. **The bottom of page 197.** The expression in braces is

\[
\left(\frac{\pi a}{m}\right) \left\{ (t + R \cos \frac{1}{4} \pi + r)^2 - (R \sin \frac{1}{4} \pi)^2 + 2i (t + R \cos \frac{1}{4} \pi + r) (R \sin \frac{1}{4} \pi) \right\},
\]

which has real part

\[
-\frac{2\pi a}{m} \left( t + \frac{R}{\sqrt{2}} + r \right) \left( \frac{R}{\sqrt{2}} \right) = -\pi a \left( \sqrt{2} t R + R^2 + \sqrt{2} r R \right) / m.
\]

6. **Page 198, lines 2–4.** We have

\[
\exp \left\{ \frac{-\pi a}{m} \left( \sqrt{2} t R + R^2 + \sqrt{2} r R \right) \right\}
\]

\[
= \exp \left\{ -\pi a R^2 \right\} \cdot \exp \left\{ -\pi a \sqrt{2} t R \right\} \cdot \exp \left\{ -\pi a \sqrt{2} r R \right\}
\]

\[
\leq \exp \left\{ -\pi a R^2 \right\} \cdot \exp \left\{ -\pi a \sqrt{2} t R \right\} \cdot 1
\]

\[
\leq \exp \left\{ -\pi a R^2 \right\} \cdot \exp \left\{ -\pi a \sqrt{2} R \right\} / m, \text{ since } |t| \leq \frac{1}{2}.
\]

7. **Page 198, line 7.** We have

\[
|\exp \{2\pi i \gamma(t)\}| = |\exp 2\pi i (t + R \cos \frac{1}{4} \pi + R i \sin \frac{1}{4} \pi)|
\]

\[
= \exp (-2\pi i R \sin \frac{1}{4} \pi) |\exp 2\pi i (t + R \cos \frac{1}{4} \pi)|
\]

\[
= \exp (-2\pi R \sin \frac{1}{4} \pi), \text{ since } |e^{x+iy}| = e^x.
\]

8. **Page 198, line 10.** As \(R \to \infty\), \(1 - e^{-\sqrt{2} \pi \gamma R} \to 1\). In the numerator, the term involving \(e^{-\pi a R^2/m}\) approaches 0 faster than the other term increases, so the numerator tends to 0.

9. **Page 198, equation (39).** Our aim now is to replace the integral from \(A\) to \(B\) by a similar (but simpler) integral from \(-\alpha\) to \(\alpha\). The aim of the next eleven lines is to show that \(\int_{\alpha}^{B} \phi = \int_{-\alpha}^{\alpha} \phi + o(1)\).

10. **Page 199, lines 1–3.** We ask you to supply the details of this estimation in Problem 9D, below.

11. **Page 199, lines 8–10.** Note that

\[
e^{\pi a z^2 / m} e^{2\pi i n z} = e^{-\pi i mn^2 / a} \exp \left\{ \frac{\pi i a}{m} \left( z + \frac{nm}{a} \right)^2 \right\}.
\]

12. **Page 199, lines 11–16.** The reason for invoking Cauchy’s theorem yet again is to replace the integral from \(-\alpha\) to \(\alpha\) by a similar integral from \(-\alpha - nm/a\) to \(\alpha - nm/a\). The result of this is that we can then make a change of variable that simplifies the integral considerably.

13. **Page 199, last two lines.** We calculated \(S(1, 2)\) and \(S(2, 1)\) in SAQ 9.5, above.

---

**Self-assessment question**

9.8 Outline the main steps of the proof of Theorem 9.16.
Problems for Sections 9.10–9.11

9C Use equation (30) to verify Theorem 9.17 when \( h \) and \( k \) are both odd primes. [Hint: consider separately the cases \( h \equiv 1 \) or 3 (mod 4), \( k \equiv 1 \) or 3 (mod 4).]

9D Justify the following steps in the proof of Theorem 9.16:

(a) page 199, lines 2–3: \ldots the integral of \( \phi \) along the horizontal line segment from \( B \) to \( \alpha \) tends to 0 as \( R \to +\infty \);

(b) page 199, lines 12–13: \ldots the integral along the horizontal line segment from \( \alpha - (nm/a) \) to \( \alpha \) tends to 0 as \( R \to +\infty \).
Chapter 10  Primitive roots

After the technicalities of Chapters 8 and 9, this chapter should provide some welcome relief. However, the material included here is most important, especially the central result that primitive roots mod $m$ exist only when $m = 1, 2, 4, p^a$ or $2p^a$. At the end of this chapter we tie up some loose ends from Chapters 6 and 8, involving characters and exponential sums.

This chapter splits into THREE study sessions.

Study Session 1: Sections 10.1–10.3 and 10.10 (pages 204–206 and 213–217)

Study Session 2: Sections 10.4–10.9 (pages 206–213)

Study Session 3: Sections 10.11–10.13 (pages 218–222)

Study Session 1: Sections 10.1–10.3 and 10.10 (pages 204–206 and 213–217)

Read  Sections 10.1 to 10.3

Commentary

1. The definitions on page 204. As an example, the exponent of 2 modulo 7 is 3, since $2^3 \equiv 1 \pmod{7}$, but $2 \not\equiv 1 \pmod{7}, 2^2 \not\equiv 1 \pmod{7};$ so $\exp_7(2) = 3$. Similarly, the exponent of 3 modulo 7 is 6, since $3^6 \equiv 1 \pmod{7}$, but $3^1 \not\equiv 1 \pmod{7}, 3^2 \not\equiv 1 \pmod{7}, 3^3 \not\equiv 1 \pmod{7}, 3^4 \not\equiv 1 \pmod{7}, 3^5 \not\equiv 1 \pmod{7};$ so $\exp_7(3) = 6$. Since $\phi(7) = 6$, 3 is a primitive root mod 7.

2. The statement of Theorem 10.1(b). The fact that $f|\phi(m)$ is very useful for testing whether or not a given number is a primitive root. For example, to test whether 3 is a primitive root mod 11, we need check only 3, $3^2$, $3^3$, $3^4$, $3^5$, $3^6$, $3^7$, $3^8$, $3^9$, $3^{10}$, since $\phi(11) = 10$. This is much quicker than testing all of $3, 3^2, 3^3, \ldots, 3^{10} \pmod{11}$.

3. The statement of Theorem 10.2. As an example, take $m = 7$ again.

For $a = 2$: $2, 2^2, 2^3, 2^4, 2^5, 2^6 \equiv 2, 4, 1, 2, 4, 1 \pmod{7}$;
for $a = 3$: $3, 3^2, 3^3, 3^4, 3^5, 3^6 \equiv 3, 2, 6, 4, 5, 1 \pmod{7}$.

Since 3 is a primitive root mod 7, we obtain a reduced residue system mod 7; 2 is not a primitive root mod 7, so we do not obtain a reduced residue system mod 7.

4. Page 205, line –10. The ‘powerful tool’ mentioned here is the index calculus of Section 10.10.

5. The statement of Theorem 10.3. If $x$ is an odd integer, then the theorem tells us that the exponent of $x$ modulo $2^a$ is at most $\frac{1}{2}\phi(2^a)$, and so $x$ cannot be a primitive root mod $2^a$. Clearly, $x$ cannot be a primitive root if $x$ is even.

Self-assessment questions

10.1 Calculate $\exp_8(3), \exp_{10}(3)$ and $\exp_{11}(3)$.
10.2 Verify that 2 is a primitive root mod 5, 11 and 13, but not mod 17.

10.3 Find all primes \( p \) (7 \( \leq p \leq 20 \)) for which 5 is a primitive root.

10.4 Give a direct proof, without using part (a), of Theorem 10.1(b).

**Read** Section 10.10

**Commentary**

1. *The definition of ‘index’.* As an example, take \( m = 7 \) and \( g = 3 \). Then, by Commentary 3 above, we have
   \[
   \text{ind} 1 = 6, \quad \text{ind} 2 = 2, \quad \text{ind} 3 = 1, \quad \text{ind} 4 = 4, \quad \text{ind} 5 = 5, \quad \text{ind} 6 = 3.
   \]

2. *The proof of Theorem 10.10.* To prove part (a), let
   \[
   \text{ind} a = k \quad \text{and} \quad \text{ind} b = \ell.
   \]
   Then \( g^k \equiv a \pmod{m} \), \( g^\ell \equiv b \pmod{m} \), and so \( g^{k+\ell} \equiv ab \pmod{m} \).
   Thus \( k + \ell \equiv \text{ind} ab \pmod{\phi(m)} \), as required.
   Part (b) follows from part (a), and parts (c) and (d) are straightforward.
   Part (e) appears as SAQ 10.6 below.

3. *Page 214, lines 10–11.* This table is extremely useful, as you will see.
   The base \( g \) for each modulus \( p \) can be found by locating the 1 in each column, or by referring to Table 10.1 on page 213.

4. *The linear congruence* \( 9x \equiv 13 \pmod{47} \). It is easier to see what is happening here if we write out the relevant part of Table 10.2 as follows.
   \[
   \begin{array}{cccccccc}
   a & 2 & 3 & 4 & \ldots & 9 & \ldots & 13 & \ldots & 38 & \ldots \\
   \text{ind} a & 18 & 20 & 36 & \ldots & 40 & \ldots & 11 & \ldots & 17 & \ldots \\
   \end{array}
   \]
   Note that, when using Table 10.2 in this way, we do not need to know the value of \( g \).

5. *Page 215, lines 17–18.* These references to quadratic residues and nonresidues will become clearer after you have studied Section 10.5.

6. *Page 215, last line.* This means that the solutions of \( 25x \equiv 17 \pmod{47} \) are \( x \equiv 8 \) and 31 (mod 46).

**Self-assessment questions**

10.5 Using Table 10.2, write down the following.
   (a) \( \text{ind} 10 \) (for \( p = 19 \)) \quad (b) \( \text{ind} 15 \) (for \( p = 31 \))
   (c) \( \text{ind} 19 \) (for \( p = 41 \))
   What is the corresponding base \( g \) in each case?

10.6 Prove Theorem 10.10(e).

10.7 Use the index calculus to solve
   (a) the linear congruences \( 7x \equiv 9 \pmod{11} \) and \( 8x \equiv 7 \pmod{43} \);
   (b) the binomial congruences \( x^2 \equiv 5 \pmod{11} \) and \( x^8 \equiv 17 \pmod{43} \);
   (c) the exponential congruences \( 3^x \equiv 5 \pmod{11} \) and \( 8^x \equiv 3 \pmod{43} \).
Problems for Sections 10.1–10.3 and 10.10

10A (a) If \( p \) is an odd prime divisor of the integer \( n^2 + 1 \), prove that \( p \) is of the form \( 4k + 1 \). (Use Theorem 10.1.)

(b) If \( p \) is an odd prime divisor of the integer \( n^4 + 1 \), prove that \( p \) is of the form \( 8k + 1 \).

(c) If \( p \) is an odd prime divisor of the integer \( n^a + 1 \), must \( p \) be of the form \( 2ak + 1 \)?

10B Apostol, page 222, number 2.

10C Show that 2 is not a primitive root of any Fermat prime \( F_n = 2^{2^n} + 1 \), for \( n > 1 \).

Study Session 2: Sections 10.4–10.9 (pages 206–213)

Read Sections 10.4 and 10.5

Commentary

1. The proof of Lemma 1. The equivalence of the congruences \( kx \equiv 0 \pmod{f} \) and \( x \equiv 0 \pmod{f/d} \), where \( d = (k, f) \), arises from Theorem 5.4.

2. The statement of Theorem 10.4. As an example, let \( p = 11 \) and \( d = 1, 2, 5 \) and 10. Then there is \( \phi(1) = 1 \) number \( a \) such that \( \exp(a) = 1 \) — namely, \( a = 1 \); there is \( \phi(2) = 1 \) number \( a \) such that \( \exp(a) = 2 \) — namely, \( a = 10 \); there are \( \phi(5) = 4 \) numbers \( a \) such that \( \exp(a) = 5 \) — namely, \( a = 3, 4, 5, 9 \); and there are \( \phi(10) = 4 \) numbers \( a \) such that \( \exp(a) = 10 \) — namely, \( a = 2, 6, 7, 8 \).

3. The proof of Theorem 10.4.

(a) By the above commentary, we have

\[
A(1) = \{1\}, A(2) = \{10\}, A(5) = \{3, 4, 5, 9\}, A(10) = \{2, 6, 7, 8\},
\]

and so \( f(1) = f(2) = 1 \) and \( f(5) = f(10) = 4 \); note that \( f(d) = \phi(d) \) for each \( d \).

(b) The fact that the solutions of (4) are incongruent mod \( p \) follows from Theorem 10.1, and the fact that there are at most \( d \) of them follows from Lagrange’s theorem (Theorem 5.21).

(c) There is an alternative proof that \( f(d) = \phi(d) \) which uses Möbius inversion. By considering the sets \( A(d) \), it is not difficult to see that if \( d \mid (p - 1) \), then \( \sum_{c \mid d} f(c) = d \), and \( f \) is a multiplicative function. It follows, by Möbius inversion and Theorem 2.3, that

\[
f(d) = \sum_{c \mid d} \mu(c)(d/c) = \phi(d).
\]
4. The statement of Theorem 10.5. As an example, let \( p = 11 \) and \( g = 2 \). Then the even powers (quadratic residues) are \( 2^2 \equiv 4, 2^4 \equiv 5, 2^6 \equiv 9, 2^8 \equiv 3 \) and \( 2^{10} \equiv 1 \), and the odd powers (quadratic nonresidues) are \( 2^1 \equiv 2, 2^3 \equiv 8, 2^5 \equiv 10, 2^7 \equiv 7 \) and \( 2^9 \equiv 6 \). These results agree with the table on page 179.

Self-assessment questions

10.8 Verify Lemma 1 when \( m = 13 \), \( a = 4 \) and \( k = 3 \) and \( 5 \).

10.9 Write down the sets \( A(d) \) when \( p = 17 \) and \( p = 19 \).

10.10 Verify Theorem 10.5 with \( p = 13 \) and \( g = 7 \), and check that your answers agree with the table on page 179.

Read Sections 10.6 and 10.7

Commentary

1. The bottom of page 208. As an example, we know that 2 is a primitive root mod 11. But \( 2^{10} = 1024 \not\equiv 1 \pmod{121} \), so 2 is a primitive root mod 121 and, more generally, mod 11\(^\alpha\), for all \( \alpha \geq 2 \).

2. The proof of Theorem 10.6.

   Line 3: The fact that \( g_1 \) is a primitive root follows from
   \[ g_1^k = (g + p)^k = g^k + \binom{k}{1} g^{k-1} p + \cdots \equiv g^k \pmod{p}, \]
   for all \( k \).

   Line 6: The letter \( t \) refers to some integer arising from the binomial expansion. It has no connection with the \( t \) that appears later in the proof.

   Line 15: The converse hinges on the fact that if \( t \) is the exponent of \( g \) modulo \( p^\alpha \), then \( g^t \equiv 1 \pmod{p^\alpha} \) and so \( g^t \equiv 1 \pmod{p} \). Thus \( t|\phi(p^\alpha) \) by Theorem 10.1(b), and \( \phi(p)|t \). We deduce that \( (p - 1)|t \) and \( t|p^\beta - 1 \) and so \( t \) has the form \( p^\beta(p - 1) \) for \( \beta \leq \alpha - 1 \), and we then prove that \( \beta = \alpha - 1 \). This last part needs a lemma which is proved separately.

3. Line 7 of the proof of Lemma 2. Note that in raising the equation for \( g^{\phi(p^\alpha - 1)} \) to the \( p \)th power, we have
   \[ g^{\phi(p^\alpha - 1)p} = g^{p^\alpha\phi(p^\alpha - 1)} = g^{\phi(p^\alpha)} \]
   the letter \( r \) that appears refers to some integer arising from the binomial expansion.

4. The proof of Theorem 10.7. This proof works because \( \phi(2p^\alpha) = \phi(p^\alpha) \).

   If \( f \) is the exponent of \( g \) modulo \( 2p^\alpha \), we show that \( f|\phi(2p^\alpha) \) and \( \phi(p^\alpha)|f \), and hence \( f = \phi(2p^\alpha) \).

Self-assessment questions

10.11 Show that 2 is a primitive root modulo 25 and 27.

10.12 Verify Lemma 2 when \( g = 2 \), \( p = 5 \) and \( \alpha = 3 \).

10.13 Find a primitive root modulo 50 and a primitive root modulo 54.
Read Sections 10.8 and 10.9

Commentary

1. The proof of Theorem 10.8. The idea of the proof is to write
   \( m = 2^{\alpha} p_1^{\alpha_1} \cdots p_s^{\alpha_s} \), and prove that
   \( a^{\phi(m)/2} \equiv 1 \pmod{2^{\alpha}} \) and
   \( a^{\phi(m)/2} \equiv 1 \pmod{p_i^{\alpha_i}} \). Combining these congruences gives the result.

   To prove that \( a^{\phi(m)/2} \equiv 1 \pmod{2^{\alpha}} \), we choose a primitive root \( g \)
   modulo \( 2^{\alpha} \), and show that \( a^{\phi(m)/2} \equiv g^{t \phi(p_1^{\alpha_1})} \pmod{p_i^{\alpha_i}} \), where \( t \) is an
   integer; since \( g^{\phi(p_1^{\alpha_1})} \equiv 1 \pmod{p_i^{\alpha_i}} \), the result follows.

   To prove that \( a^{\phi(m)/2} \equiv 1 \pmod{2^{\alpha}} \), we consider separately the cases \( \alpha \geq 3 \)
   and \( \alpha \leq 2 \). If \( \alpha \geq 3 \), the result follows from Theorem 10.3, and if \( \alpha = 1 \) or 2,
   the argument is straightforward.

2. The statement of Theorem 10.9. As an example, let \( p = 11 \) and \( g = 2 \). Then
   \( (n, \phi(11)) = 1 \) when \( n = 1, 3, 7 \) or 9. The primitive roots modulo 11 are
   therefore 2, 2^3, 2^7 and 2^9 — that is, 2, 8, 128 (≡ 7) and 512 (≡ 6); these
   answers agree with those we obtained earlier.

3. The proof of Theorem 10.9. The proof of this result relies heavily on
   Lemma 1 to show that if \( g \) is a primitive root modulo \( m \), then so is \( g^n \).

4. Table 10.1. This table gives the smallest primitive root of the prime \( p \), for
   all primes \( p < 1000 \). The other primitive roots of \( p \) can be obtained from
   Theorem 10.9, and primitive roots modulo \( p^{\alpha} \) and \( 2p^{\alpha} \) can be deduced from
   Theorems 10.6 and 10.7.

Self-assessment questions

10.14 Prove that \( 5^{2^\beta} \equiv 1 \pmod{2^{3^\beta+2}} \), for \( \beta \geq 1 \).

10.15 For which values of \( m \leq 50 \) does there exist a primitive root?
   For each such number \( m \), write down a primitive root, and the number of
   incongruent primitive roots.

10.16 Find all the primitive roots modulo 18 and modulo 27.

Problems for Sections 10.4–10.9

10D Given that 3 is a primitive root of 43, find all positive integers \( a \) less than
43 with:
   (a) \( \exp_{43}(a) = 6 \);  \quad \text{(b)} \exp_{43}(a) = 21 \).

10E Use the fact that each prime \( p \) has a primitive root to prove Wilson’s
   theorem: \( (p - 1)! \equiv -1 \pmod{p} \).
**Study Session 3: Sections 10.11–10.13**  
*(pages 218–222)*

**Read** Section 10.11

**Commentary**

1. In this study session we combine the results of Chapter 10 with Dirichlet characters from Chapter 6 and exponential sums from Chapter 8. You may wish to re-read Sections 6.8, 8.1 and 8.7 before proceeding.

2. **Equation (21).** Letting \( \omega \) be a primitive \( \phi(p^\alpha) \)th root of unity, we have

\[
\chi_h(n) = \omega^{hb(n)} \quad \text{if} \quad p \nmid n, \quad \text{and} \quad 0 \quad \text{if} \quad p|n.
\]

For a primitive root \( g \) we have \( \chi_h(g) = \omega^h \). We leave it to you (in SAQ 10.18) to verify that \( \chi_h \) is completely multiplicative and periodic with period \( p^\alpha \). Note that \( \chi_1 \) is no longer the principal character.

3. **The statement of Theorem 10.11.** Note the presence of the term \((-1)^{(n-1)/2}\), and the requirement that \( n \) is odd. We shall use the numbers \( b(n) \) determined by this theorem to define Dirichlet characters mod \( 2^\alpha \), for \( \alpha \geq 3 \).

4. **The proof of Theorem 10.11.** The first part of the proof shows that if \( f = \exp_{2\alpha}(5) \), then \( f = \phi(2^\alpha)/2 = 2^{\alpha-2} \). The rest of this proof consists of showing that the \( \phi(2^\alpha) \) numbers

\[
5, 5^2, \ldots, 5^f, -5, -5^2, \ldots, -5^f
\]

are all incongruent mod \( 2^\alpha \), using Theorem 10.1(c) and a ‘mod 4’ argument.

5. **The definitions of \( f(n) \) and \( g(n) \).** In SAQ 10.18 we ask you to verify that \( f \) and \( g \) are characters mod \( 2^\alpha \).

6. **Equation (25).** Note that if \( a = 1 \) and \( n \) is odd, then

\[
\chi_{1,c}(n) = \begin{cases} 
 e^{2\pi i cb(n)/2^{\alpha-2}}, & \text{if } n \equiv 1 \pmod{4} \\
 -e^{2\pi i cb(n)/2^{\alpha-2}}, & \text{if } n \equiv 3 \pmod{4},
\end{cases}
\]

and if \( a = 2 \) and \( n \) is odd, then \( \chi_{2,c}(n) = e^{2\pi i cb(n)/2^{\alpha-2}} \).

**Self-assessment questions**

10.17 Let \( \omega \) be a primitive 6th root of unity. Use equation (21) to write down all the characters \( \chi_h(n) \) in terms of \( \omega \), when \( p^\alpha = 9 \).

10.18 Verify that \( \chi_h \) is completely multiplicative and periodic with period \( p^\alpha \), and that \( f \) and \( g \) are characters mod \( 2^\alpha \).

10.19 Write down the characters \( \chi_{a,c}(n) \) in equation (25), when \( \alpha = 3 \).
Commentary

1. The statement of Theorem 10.12. Note that in the tables on page 139, there are only two real-valued characters mod 3, 5 and 7. The essential idea is that a primitive root $g \mod p^\alpha$ must take one of the values 1 or $-1$, and all the other values $\chi(n) = \chi(g^{\text{ind } n})$ are then determined.

2. The statement of Theorem 10.13. We have already seen, in our work on Chapter 6 (in M823), that there are exactly four real characters mod 8 and mod 16.

3. The statements of Theorems 10.14 and 10.15. These theorems give very simple criteria for determining whether or not a character mod $p^\alpha$ or mod $2^\alpha$ is primitive. The proof of Theorem 10.14 is straightforward; we ask you to prove Theorem 10.15 in Problem 10G.

Self-assessment questions

10.20 Use Table 10.2 to write down the two real characters mod 29 and the two real characters mod 43.

10.21 Write down the real characters mod 27, mod 32 and mod 24.

10.22 Which characters are primitive mod 25, mod 32 and mod 72?

10.23 Prove that there are exactly two real primitive characters mod 8, and write down their values.

Problems for Sections 10.11–10.13

10F Calculate the numbers $b(n)$ in Theorem 10.11 when $\alpha = 6$.

10G Prove Theorem 10.15.

10H Let $\chi$ be a real primitive character mod $m$, where $m$ is not a power of 2. Prove that $m$ has the form

$$m = 2^\alpha p_1 \ldots p_r,$$

where the odd primes $p_i$ are distinct, and $\alpha = 0, 2$ or 3.
Solutions to the Self-assessment questions

Chapter 8

8.1 \((x - 1) \sum_{n=1}^{k-1} nx^n = (k-1)x^k - x^{k-1} - \cdots - x^2 - x\)
\[= kx^k - (x + x^2 + \cdots + x^k)\]
\[= k, \text{ since } x^k = 1 \text{ and } x + x^2 + \cdots + x^k = 0.\]
The result follows on dividing by \(x - 1\).

8.2 Let \(f\) be defined by \(f(4n) = f(4n + 1) = 0, f(4n + 2) = 2\) and \(f(4n + 3) = 1\), for all integers \(n\). (Other answers are possible.)

8.3 (a) \(1 + x^2 + x^4 = 1 + x^2 + x = 0\)
(b) \(1 + x^5 + x^{10} = 1 + x^2 + x = 0\)
(c) \(1 + x^9 + x^{18} = 1 + 1 + 1 = 3\)

8.4 \(n = 7: \ g(7) = 1 + i^7 + i^{14} + i^{21} = 1 - i - 1 + i = 0;\)
\(n = 8: \ g(8) = 1 + i^8 + i^{16} + i^{24} = 1 + 1 + 1 + 1 = 4.\)

8.5 \(A(z) = (z-1)(z-i)^2 = (z^2 - 1)(z-i)^2 = z^4 - 1, \text{ and}\)
\(A_0(z) = (z+1)(z^2 + 1), \ A_1(z) = (z-1)(z^2 + 1), \ A_2(z) = (z^2 - 1)(z + i),\)
\(A_3(z) = (z^2 - 1)(z - i).\)

So
\[P(z) = \frac{(1+i)z(1-z)}{(1+i)(1-z)} + \frac{(1-i)(1+z)}{(-1-1)((-1)^2 + 1)} + \frac{(1+2i)(z^2 - 1)(z+i)}{(i^2-1)(i+i)} + \frac{(1-2i)(z^2 - 1)(z-i)}{((-i)^2-1)(-i-i)}\]
\[= \frac{z^2 + 1}{2} (iz + 1) - \frac{z^2 - 1}{2} (2z + 1) = \frac{1}{2}(i-2)z^3 + \frac{1}{2}(i+2)z + 1.\]

8.6 \(a_0 = \frac{1}{4}\{(1+i) + (1+2i) + (1-i) + (1-2i)\} = 1;\)
\(a_1 = \frac{1}{4}\{(1+i) + (1+2i)i^{-1} + (1-i)i^{-2} + (1-2i)i^{-3}\} = \frac{1}{4}(i + 2);\)
\(a_2 = \frac{1}{4}\{(1+i) + (1+2i)i^{-2} + (1-i)i^{-4} + (1-2i)i^{-6}\} = 0;\)
\(a_3 = \frac{1}{4}\{(1+i) + (1+2i)i^{-3} + (1-i)i^{-6} + (1-2i)i^{-9}\} = \frac{1}{4}(i - 2).\)

8.7 \(g(n) = \frac{1}{6}(\chi(1)x^{-n} + \chi(5)x^{-5n}), \text{ where } x^6 = 1,\)
\[= \frac{1}{6}(x^{-n} - x^n).\]

8.8 From the definition:
\(c_4(3) = i^3 + i^0 = 0;\)
\(c_8(2) = x^2 + x^6 + x^{10} + x^{14} = 0 \text{ (where } x^8 = 1);\)
\(c_6(3) = x^3 + x^{15} = -2 \text{ (where } x^6 = 1).\)

From Theorem 8.6:
\(c_4(3) = 1\mu(4) = 0;\)
\(c_8(2) = 1\mu(8) + 2\mu(4) = 0;\)
\(c_6(3) = 1\mu(6) + 3\mu(2) = -2.\)

8.9 \(c_k(n) = \mu(k)\)

8.10
\[
\begin{array}{c|cccccccccccc}
  n & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\
  \hline
  c_{12}(n) & 0 & 2 & 0 & -2 & 0 & -4 & 0 & -2 & 0 & 2 & 0 & 4 \\
\end{array}
\]
8.11 Theorem. Let \( s_k(n) = \sum_{d|(n,k)} d\mu(k/d). \)

Then \( s_k(n) \) has the finite Fourier expansion

\[
s_k(n) = \sum_{m \mod k} a_k(m)e^{2\pi i mn/k},
\]

where \( a_k(m) = \sum_{d|(m,k)} \mu(d). \)

Proof. By Theorem 8.4, we have

\[
a_k(m) = \frac{1}{k} \sum_{n \mod k} s_k(n)e^{-2\pi i mn/k} = \frac{1}{k} \sum_{n=1}^{k} \sum_{d|n} \mu(k/d) e^{-2\pi i mn/k}.
\]

Writing \( n = cd \), we have

\[
a_k(m) = \frac{1}{k} \sum_{d|k} \mu(k/d) \sum_{c=1}^{d} e^{-2\pi i cd m/d} = \frac{1}{k} \sum_{d|k} \mu(d) \sum_{c=1}^{d} e^{-2\pi i cd m/d}.
\]

8.12 \( G(n, \chi) = \chi(1)x^n + \chi(5)x^{5n} = x^n - x^{5n} \) (where \( x^6 = 1 \)).
So \( G(1, \chi) = x - x^{-1}, G(2, \chi) = x^2 - x^{-2} \) and \( G(4, \chi) = x^4 - x^{-4} \).

Since \( G(2, \chi) \) and \( G(4, \chi) \) are non-zero, and \( \overline{\chi}(2) = \overline{\chi}(4) = 0 \),
\( G(2, \chi) \) and \( G(4, \chi) \) are not separable.

Also, \( |G(1, \chi)|^2 = |x - x^{-1}|^2 = |2i\sin(\pi/3)|^2 = 3. \)

8.13 \( G(n, \chi_3) = x^n + ix^{2n} - ix^{3n} - x^{4n} \) (where \( x^5 = 1 \)),
and \( G(1, \chi_3) = x + ix^2 - ix^3 - x^4 \).

If \( n \equiv 1 \pmod{5} \), \( G(n, \chi_3) = x + ix^2 - ix^3 - x^4 = 1 \cdot G(1, \chi_3) \).

If \( n \equiv 2 \pmod{5} \), \( G(n, \chi_3) = x^2 + ix^4 - ix - x^3 = -i \cdot G(1, \chi_3) \).

If \( n \equiv 3 \pmod{5} \), \( G(n, \chi_3) = x^3 + ix - ix^4 - x^2 = i \cdot G(1, \chi_3) \).

If \( n \equiv 4 \pmod{5} \), \( G(n, \chi_3) = x^4 + ix^2 - x = -1 \cdot G(1, \chi_3) \).

If \( n \equiv 0 \pmod{5} \), \( G(n, \chi_3) = 1 + i - i - 1 = 0 \cdot G(1, \chi_3) \).

It follows that \( G(n, \chi_3) \) is separable for every \( n \).

8.14 Since \( \chi_1(a) = 1 \) whenever \( (a, k) = 1 \), it follows that \( \chi_1(a) = 1 \) whenever \( (a, k) = 1 \) and \( a \equiv 1 \pmod{d} \).

8.15 (a) \( \text{mod } 8 \):
\[
\begin{align*}
\chi_2(1) &= \chi_2(3) = 1, \chi_2(5) = \chi_2(7) = -1; \text{ primitive.} \\
\chi_3(1) &= \chi_3(5) = 1, \chi_3(3) = \chi_3(7) = -1; \text{ induced modulus } 4. \\
\chi_4(1) &= \chi_4(7) = 1, \chi_4(3) = \chi_4(5) = -1; \text{ primitive.}
\end{align*}
\]

Clearly, 8 is also an induced modulus in each case.

\( \text{mod } 12 \):
\[
\begin{align*}
\chi_2(1) &= \chi_2(5) = 1, \chi_2(7) = \chi_2(11) = -1; \text{ induced modulus } 4. \\
\chi_3(1) &= \chi_3(7) = 1, \chi_3(5) = \chi_3(11) = -1; \text{ induced moduli } 3, 6. \\
\chi_4(1) &= \chi_4(11) = 1, \chi_4(5) = \chi_4(7) = -1; \text{ primitive.}
\end{align*}
\]

Clearly, 12 is also an induced modulus in each case.

(b) \( \text{mod } 8 \):
For \( d = 4 \), let \( \psi(1) = 1, \psi(3) = -1; \) then \( \chi_3(n) = \psi(n)\chi_1(n) \) for all \( n \).

\( \text{mod } 12 \):
For \( d = 4 \), let \( \psi(1) = 1, \psi(3) = -1; \) then \( \chi_2(n) = \psi(n)\chi_1(n) \) for all \( n \).
For \( d = 3 \), let \( \psi(1) = 1, \psi(2) = -1; \) then \( \chi_3(n) = \psi(n)\chi_1(n) \) for all \( n \).
For \( d = 6 \), let \( \psi(1) = 1, \psi(5) = -1; \) then \( \chi_3(n) = \psi(n)\chi_1(n) \) for all \( n \).
8.16 Using the notation of the solution of SAQ 8.15, we see that \( \chi_1 \) has conductor 1, \( \chi_3 \) has conductor 4, \( \chi_3 \) has conductor 3, and \( \chi_4 \) is primitive and has conductor 12. The equality \( \chi(n) = \psi(n)\chi_1(n) \) follows as in the solution of SAQ 8.15(b) for \( \chi_2 \) and \( \chi_3 \). For \( \chi_1 \), we take \( \psi \) to be the trivial character mod 1 for which \( \psi(1) = 1 \). For \( \chi_4 \), we take \( \psi = \chi_4 \).

8.17 \( \chi(1) = \chi(3) = 1; \chi(5) = \chi(7) = -1; \chi(2k) = 0. \)

If \( n = 5 \), then with \( \omega^8 = 1 \),
\[
G(n, \chi) = \omega^5 + \omega^{15} - \omega^{25} - \omega^{35} = \omega^5 + \omega^7 - \omega - \omega^3 = -G(1, \chi);
\]
if \( n = 7 \), then
\[
G(n, \chi) = \omega^7 + \omega^{21} - \omega^{35} - \omega^{49} = \omega^7 + \omega^5 - \omega^3 - \omega = -G(1, \chi).
\]
In each case, \( G(n, \chi) = \overline{\chi(n)G(1, \chi)} \), and is thus separable.

\( \chi(1) = \chi(7) = 1; \chi(3) = \chi(5) = -1; \chi(2k) = 0. \)

If \( n = 5 \), then
\[
G(n, \chi) = \omega^5 - \omega^{15} - \omega^{25} + \omega^{35} = \omega^5 - \omega^7 + \omega + \omega^3 = -G(1, \chi);
\]
if \( n = 7 \), then
\[
G(n, \chi) = \omega^7 - \omega^{21} - \omega^{35} + \omega^{49} = \omega^7 - \omega^5 - \omega^3 + \omega = G(1, \chi).
\]
In each case, \( G(n, \chi) = \overline{\chi(n)G(1, \chi)} \), and is thus separable.

8.18 \( \tau_8(\chi) = \frac{1}{\sqrt{8}}G(1, \chi) = \frac{1}{\sqrt{8}}(\omega + \omega^3 - \omega^5 - \omega^7) \),
where \( \omega = \cos \pi/4 + i \sin \pi/4 = (1 + i)/\sqrt{2} \); so
\[
\tau_8(\chi) = \frac{1}{\sqrt{8}} \left\{ \frac{1}{\sqrt{2}}(1 + i) + \frac{1}{\sqrt{2}}(-1 + i) - \frac{1}{\sqrt{2}}(-1 - i) - \frac{1}{\sqrt{2}}(1 - i) \right\}
= \frac{1}{4} \cdot 4i = i.
\]
Clearly, \(|\tau_8(\chi)| = 1. \)

Similarly,
\[
\tau_8(\chi) = \frac{1}{\sqrt{8}}G(1, \chi) = \frac{1}{\sqrt{8}}(\omega - \omega^3 - \omega^5 + \omega^7)
= \frac{1}{\sqrt{8}} \left\{ \frac{1}{\sqrt{2}}(1 + i) - \frac{1}{\sqrt{2}}(-1 + i) + \frac{1}{\sqrt{2}}(-1 - i) + \frac{1}{\sqrt{2}}(1 - i) \right\}
= \frac{1}{4} \cdot 4 = 1.
\]
Clearly, \(|\tau_8(\chi)| = 1. \)

8.19 Since \( \tau_4(\chi) = \frac{1}{2}(i - i^3) = i \), the right-hand side of equation (21) is
\[
\frac{i}{2}(i^{-m} - i^{-3m}) = \begin{cases} 
1, & \text{if } m = 1 \\
0, & \text{if } m = 2 \\
-1, & \text{if } m = 3.
\end{cases}
\]
In each case, this is equal to \( \chi(m) \), as required.

8.20 If \( \chi(1) = \chi(3) = 1, \chi(5) = \chi(7) = -1, \) then
\[
\left| \sum_{m \leq 13} \chi(m) \right| = |\chi(1) + \chi(3) + \chi(5) + \chi(7) + \chi(9) + \chi(11) + \chi(13)| = 1.
\]
Clearly, this is less than \( \sqrt{8} \log 8 \approx 5.88. \)

If \( \chi(1) = \chi(7) = 1, \chi(3) = \chi(5) = -1, \) then
\[
\left| \sum_{m \leq 13} \chi(m) \right| = |\chi(1) + \cdots + \chi(13)| = 1.
\]
As before, this is less than \( \sqrt{8} \log 8. \)
Chapter 9

9.1  \( p = 11 \): If \( \omega^{11} = 1 \), then

\[
G(1, \chi)^2 = (\omega - \omega^2 + \omega^3 + \omega^4 + \omega^5 - \omega^6 - \omega^7 - \omega^8 + \omega^9 + \omega^{10})^2
\]

\[
= \omega^2 - 2\omega^3 + 3\omega^4 + \omega^5 - 2\omega^7 + 3\omega^8 + \omega^{10} - 10\omega^{11} + \omega^{12} + 3\omega^{14}
\]

\[
= -10 + (\omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6 + \omega^7 + \omega^8 + \omega^9 + \omega^{10})
\]

\[
= -11, \quad \text{since} \quad \omega + \omega^2 + \cdots + \omega^{10} = -1.
\]

9.2  (a) \( G(1, \chi)^2 = 13 \), so

\[
G(1, \chi)^{9-1} = 13^8 \equiv (13|17) \pmod{17} \quad \text{(by Euler's criterion)}
\]

\[
\equiv (17|13) \pmod{17}, \quad \text{since} \quad 13 \equiv 17 \equiv 1 \pmod{4}.
\]

(b) \( G(1, \chi)^2 = -11 \), so

\[
G(1, \chi)^{9-1} = (-11)^6 = 11^6 \equiv (11|13) \pmod{13}
\]

\[
\equiv (13|11) \pmod{13}, \quad \text{since} \quad 13 \equiv 1 \pmod{4}, \quad 11 \equiv 3 \pmod{4}.
\]

(c) \( G(1, \chi)^2 = 13 \), so

\[
G(1, \chi)^{9-1} = 13^5 \equiv (13|11) \pmod{11}
\]

\[
\equiv (11|13) \pmod{11}, \quad \text{since} \quad 11 \equiv 3 \pmod{4}, \quad 13 \equiv 1 \pmod{4}.
\]

(d) \( G(1, \chi)^2 = -11 \), so

\[
G(1, \chi)^{9-1} = (-11)^9 = -11^9 \equiv (-11|19) \pmod{19}
\]

\[
\equiv (19|11) \pmod{19}, \quad \text{since} \quad 11 \equiv 19 \equiv 3 \pmod{4}.
\]

9.3  The solutions of \( r_1 + r_2 + r_3 \equiv 3 \pmod{5} \), and the corresponding values of

\( R = (r_1 r_2 r_3 | 5) \), are as follows.

<table>
<thead>
<tr>
<th>( r_1 )</th>
<th>( r_2 )</th>
<th>( r_3 )</th>
<th>( R )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1 0 1 3 4 1 4 3 1 0 2 2 4 2 3 3 3 3 0 0 4 0 4</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1 3 4 1 4 3 1 0 2 1 2 4 2 3 3 2 0 0 3 0 4 4</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
<td>1 2 4 1 3 3 1 4 2 1 0 4 2 2 3 2 3 0 3 0 4 4 0</td>
</tr>
</tbody>
</table>

The right-hand side of equation (23) is therefore

\[
(3|5) \{1 + 3(0 - 1 - 1 + 0 + 1 - 1 + 0 + 0)\} = -1(1 - 6) = 5,
\]

and the left-hand side is \( G(1, \chi)^2 = (-1|5)5 = 5 \).

9.4  If \( m = 3 \) and \( \omega = -\frac{1}{2} + \frac{i}{2}\sqrt{3} \), then \( \omega^3 = 1 \) and

\[
G(1; m) = \omega + \omega^4 + \omega^9 = 1 + 2\omega = 1 + 2\left(-\frac{1}{2} + \frac{i}{2}\sqrt{3}\right) = i\sqrt{3}.
\]

If \( m = 4 \), then

\[
G(1; m) = i + i^4 + i^9 + i^{16} = 2 + 2i = (1 + i)\sqrt{4}.
\]

If \( m = 6 \) and \( \omega^6 = 1 \), then

\[
G(1; m) = \omega + \omega^4 + \omega^9 + \omega^{16} + \omega^{25} + \omega^{36} = 2\omega + 2\omega^4 + \omega^3 + 1
\]

\[
= (1 + \omega^3)(1 + 2\omega) = 0, \quad \text{since} \quad \omega^3 = -1.
\]
9.5  
(a) $S(2, 1) = e^0 = 1$
(b) $S(1, 2) = e^0 + e^{\pi i/2} = 1 + i$
(c) $S(3, 4) = e^0 + e^{3\pi i/4} + e^{3\pi i} + e^{27\pi i/4} = 1 + \left(\frac{-1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) - 1 + \left(\frac{-1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) = \sqrt{2}(-1 + i)$

9.6  
$n = 2, p = 5$
If $\omega^5 = 1$, then
$G(1; 5) = \omega + \omega^4 + \omega^9 + \omega^{16} + \omega^{25} = 1 + 2(\omega + \omega^4)$,
and $G(2; 5) = \omega^2 + \omega^8 + \omega^{18} + \omega^{32} + \omega^{50} = 1 + 2(\omega^2 + \omega^3)$.
Thus $G(2; 5) + G(1; 5) = 2(1 + \omega + \omega^2 + \omega^3 + \omega^4) = 0$,
and so $G(2; 5) = -G(1; 5) = (2/5)G(1; 5)$.
If $\omega^7 = 1$, then
$G(1; 7) = \omega + \omega^4 + \omega^9 + \omega^{16} + \omega^{25} + \omega^{36} + \omega^{49} = 1 + 2\omega + 2\omega^2 + 2\omega^4$,
and $G(2; 7) = \omega^2 + \omega^8 + \omega^{18} + \omega^{32} + \omega^{50} + \omega^{72} + \omega^{98} = 1 + 2\omega + 2\omega^2 + 2\omega^4$,
and so $G(2; 7) = G(1; 7) = (2/7)G(1; 7)$.

9.7  
When $h = 5$ and $k = 7$, we have $G(h; k) = (5/7)G(1; 7) = -i\sqrt{7}$, and
\[
\sqrt{\frac{1}{5}} \frac{1 + i}{2} \left(1 + e^{-\pi i k/2}\right) G(k; h) = \sqrt{\frac{7}{5}} \frac{1 + i}{2} \left(1 + e^{-35\pi i/2}\right) (7/5)G(1; 5)
\]
\[
= \sqrt{\frac{7}{5}} \frac{1 + i}{2} (1 + i)(-1)i\sqrt{7} = -i\sqrt{7},
\]
as required.

9.8  
Step 1. Define $\phi(z) = f(z + 1) - f(z)$, where
\[
f(z) = \left(\sum_{r=0}^{m-1} e^{\pi imz^2/m} \right) / (e^{2\pi iz} - 1).
\]
Then $\phi(z) = e^{\pi iz^2/m} \sum_{n=0}^{a-1} e^{2\pi inz}$, and $\phi$ is analytic everywhere.

Step 2. By Cauchy’s residue theorem, $S(a, m) = \int_A f(z) \, dz$, where $\gamma$ is the parallelogram contour in Figure 9.1. Hence we can write
\[
S(a, m) = \int_A f(z) \, dz + \int_{A+1} f(z) \, dz - \int_B f(z) \, dz.
\]
Step 3. We show that as $R \to \infty$, the last two integrals in Step 2 tend to 0. Thus
\[
S(a, m) = \int_A f(z) \, dz + o(1), \quad \text{as } R \to \infty.
\]
Step 4. We replace the integral from $A$ to $B$ in Step 3 by an integral from $-\alpha$ to $\alpha$, where $\alpha = Re^{\pi i/4}$. Thus
\[
S(a, m) = \int_{-\alpha}^\alpha f(z) \, dz + o(1), \quad \text{as } R \to \infty.
\]
Step 5. We rewrite the result of Step 4 as
\[
S(a, m) = \sum_{n=0}^{a-1} e^{-\pi in^2/a} \int_{-\alpha}^\alpha \exp \left\{ \frac{\pi a}{m} \left( z + \frac{nm}{a} \right)^2 \right\} \, dz.
\]
Step 6. By means of another contour integral, we make a change of variable in this last integral, giving
\[
S(a, m) = \sum_{n=0}^{a-1} e^{-\pi in^2/a} \sqrt{\frac{m}{a}} \lim_{T \to \infty} \int_{-Te^{\pi i/4}}^{Te^{\pi i/4}} e^{\pi iw^2} \, dw,
\]
where $T = \sqrt{a/m} \cdot R$. 

55
Step 7. We deduce that
\[ S(a, m) = \sqrt{\frac{m}{a}} S(m, a) I, \]
where \( I \) is the limit in Step 6. Substituting \( a = 1, m = 2 \) gives
\[ I = (1 + i)/\sqrt{2}, \]
and the result follows.

Chapter 10

10.1 In each case, we need consider only those powers \( 3^k \) for which \( k|\phi(m) \).
Thus:
\[ 3^1 \equiv 3 \pmod{8}, \quad 3^2 \equiv 1 \pmod{8}, \quad \text{so exp}_8(3) = 2; \]
\[ 3^1 \equiv 3 \pmod{10}, \quad 3^2 \equiv 9 \pmod{10}, \quad 3^4 \equiv 1 \pmod{10}, \quad \text{so exp}_{10}(3) = 4; \]
\[ 3^1 \equiv 3 \pmod{11}, \quad 3^2 \equiv 9 \pmod{11}, \quad 3^4 \equiv 1 \pmod{11}, \quad \text{so exp}_{11}(3) = 5. \]

10.2 \( 2^1 \equiv 2 \pmod{5}, \quad 2^2 \equiv 4 \pmod{5}, \quad 2^4 \equiv 1 \pmod{5}, \) so 2 is a primitive root mod 5.
\[ 2^1 \equiv 2 \pmod{11}, \quad 2^2 \equiv 4 \pmod{11}, \quad 2^4 \equiv 1 \pmod{11}, \]
so 2 is a primitive root mod 11.
\[ 2^1 \equiv 2 \pmod{13}, \quad 2^2 \equiv 4 \pmod{13}, \quad 2^4 \equiv 1 \pmod{13}, \]
so 2 is a primitive root mod 13.
\[ 2^8 \equiv 1 \pmod{17}, \) so 2 is not a primitive root mod 17.

Alternatively, we can use Theorem 10.2 and just ‘keep doubling’ \((\pmod{m})\). For example,
\[ m = 11: \quad 2, 2^2, 2^3, \ldots, 2^{10} \equiv 2, 4, 8, 5, 10, 9, 7, 3, 6, 1; \]
this is a reduced residue system mod 11, so 2 is a primitive root mod 11.
\[ m = 13: \quad 2, 2^2, 2^3, \ldots, 2^{12} \equiv 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1; \]
this is a reduced residue system mod 13, so 2 is a primitive root mod 13.

10.3 \( p = 7: \quad 5^1 \equiv 5 \pmod{7}, \quad 5^2 \equiv 4 \pmod{7}, \quad 5^3 \equiv 6 \pmod{7}, \quad 5^6 \equiv 1 \pmod{7}, \)
so 5 is a primitive root mod 7.
\( p = 11: \quad 5^1 \equiv 1 \pmod{11}, \) so 5 is not a primitive root mod 11.
\( p = 13: \quad 5^1 \equiv 1 \pmod{13}, \) so 5 is not a primitive root mod 13.
\( p = 17: \quad 5^1 \equiv 5 \pmod{17}, \quad 5^2 \equiv 8 \pmod{17}, \quad 5^4 \equiv 13 \pmod{17}, \quad 5^8 \equiv 16 \pmod{17}, \quad 5^{16} \equiv 1 \pmod{17}, \)
so 5 is a primitive root mod 17.
\( p = 19: \quad 5^9 \equiv 1 \pmod{19}, \) so 5 is not a primitive root mod 19.

10.4 Suppose that \( a^k \equiv 1 \pmod{m} \). If \( k = qf + r, \) where \( 0 \leq r < f, \) then
\[ 1 \equiv a^k = a^{qf+r} \equiv a^r \pmod{m}, \]
so \( r = 0 \) and \( k \equiv 0 \pmod{f} \).
Conversely, if \( k \equiv 0 \pmod{f} \), then \( k = qf, \) so \( a^k \equiv 1 \pmod{m} \), since \( a^f \equiv 1 \pmod{m} \).

10.5 (a) \( \text{ind} 10 = 17, \quad g = 2. \)
(b) \( \text{ind} 15 = 21, \quad g = 3. \)
(c) \( \text{ind} 19 = 9, \quad g = 6. \)

10.6 If \( \text{ind}_a a = k \) and \( \text{ind}_{g'} g' = \ell, \) then \( (g')^k \equiv a \pmod{m} \) and \( g^\ell \equiv g' \pmod{m} \),
and hence \( g^{k\ell} \equiv a \pmod{m} \). Thus
\[ \text{ind}_{g'} a \equiv k\ell \equiv \text{ind}_{g'} a \cdot \text{ind}_{g'} g' \pmod{\phi(m)}. \]
10.7 (a) If \( 7x \equiv 9 \pmod{11} \), then \( \text{ind } x \equiv \text{ind } 9 - \text{ind } 7 \pmod{10} \).
Now \( \text{ind } 9 = 6 \) and \( \text{ind } 7 = 7 \), so \( \text{ind } x \equiv 9 \pmod{10} \).
Thus \( x \equiv 6 \pmod{11} \).
If \( 8x \equiv 7 \pmod{43} \), then \( \text{ind } x \equiv \text{ind } 7 - \text{ind } 8 \pmod{42} \).
Now \( \text{ind } 7 = 35 \) and \( \text{ind } 8 = 39 \), so \( \text{ind } x \equiv 38 \pmod{42} \).
Thus \( x \equiv 17 \pmod{43} \).
(b) If \( x^2 \equiv 5 \pmod{11} \), then \( 2 \text{ ind } x \equiv \text{ind } 5 \pmod{10} \).
Now \( \text{ind } 5 = 4 \), so \( \text{ind } x \equiv 2 \) or \( 7 \pmod{10} \).
Thus \( x \equiv 4 \) or \( 7 \pmod{11} \).
If \( x^8 \equiv 17 \pmod{43} \), then \( 8 \text{ ind } x \equiv \text{ind } 17 \pmod{42} \).
Now \( \text{ind } 17 = 38 \), so \( \text{ind } x \equiv 10 \) or \( 31 \pmod{42} \).
Thus \( x \equiv 10 \) or \( 33 \pmod{43} \).
(c) If \( 3^x \equiv 5 \pmod{11} \), then \( x \text{ ind } 3 \equiv \text{ind } 5 \pmod{10} \).
Now \( \text{ind } 3 = 8 \) and \( \text{ind } 5 = 4 \), so \( x \equiv 3 \) or \( 8 \pmod{10} \).
If \( 8x \equiv 3 \pmod{43} \), then \( x \text{ ind } 8 \equiv \text{ind } 3 \pmod{42} \).
Now \( \text{ind } 8 = 39 \), so \( 39x \equiv 1 \pmod{42} \).
Since \( (39, 42) \neq 1 \), there are no solutions.

10.8 \( f = \exp_{13}(4) = 6 \), \( \exp_{13}(4^3) = 2 \) and \( \exp_{13}(4^5) = 6 \);
for \( k = 3 \), \( \frac{\exp_{13}(4)}{3, 6} = \frac{6}{3} = \exp_{13}(4^3) \);
for \( k = 5 \), \( \frac{\exp_{13}(4)}{5, 6} = \frac{6}{1} = \exp_{13}(4^5) \).

10.9 \( p = 17 \): \( A(1) = \{1\} \), \( A(2) = \{16\} \), \( A(4) = \{4, 13\} \), \( A(8) = \{2, 8, 9, 15\} \), \( A(16) = \{3, 5, 6, 7, 10, 11, 12, 14\} \);
\( p = 19 \): \( A(1) = \{1\} \), \( A(2) = \{18\} \), \( A(3) = \{7, 11\} \), \( A(6) = \{8, 12\} \), \( A(9) = \{4, 5, 6, 9, 16, 17\} \), \( A(18) = \{2, 3, 10, 13, 14, 15\} \).

10.10 The even powers are \( 7^2 \equiv 10, 7^4 \equiv 9, 7^6 \equiv 12, 7^8 \equiv 3, 7^{10} \equiv 4 \) and \( 7^{12} \equiv 1 \);
the odd powers are \( 7^1 \equiv 7, 7^3 \equiv 5, 7^5 \equiv 11, 7^7 \equiv 6, 7^9 \equiv 8 \) and \( 7^{11} \equiv 2 \).
These agree with the table on page 179.

10.11 \( 2 \) is a primitive root mod 5, and \( 2^4 \not\equiv 1 \pmod{25} \); by Theorem 10.6, \( 2 \) is a primitive root mod 25.
\( 2 \) is a primitive root mod 3, and \( 2^2 \not\equiv 1 \pmod{9} \); by Theorem 10.6, \( 2 \) is a primitive root mod 27.

10.12 \( g^{p-1} = 2^4 = 16 \not\equiv 1 \pmod{25} \);
\( g^{6(p^{a-1})} = 2^{20} = 1 \, 048 \, 576 \not\equiv 1 \pmod{125} \).

10.13 \( 2 \) is a primitive root mod 25, so \( 2 + 25 = 27 \) is a primitive root mod 50. \( 2 \) is a primitive root mod 27, so \( 2 + 27 = 29 \) is a primitive root mod 54.

10.14 This follows immediately from Theorem 10.8 with \( a = 5 \) and \( m = 2^{\beta+2} \).

10.15 \( m \) 1 2 3 4 5 6 7 9 10 11 13 14 17 18 19 22
\( g \) 1 1 1 2 3 2 5 3 2 7 2 2 3 3 11 2 13
no. 1 1 1 1 2 1 2 2 2 4 4 2 8 2 6 4
\( m \) 23 25 26 27 29 31 34 37 39 41 43 46 47 49 50
\( g \) 5 2 15 2 2 3 3 2 21 6 3 5 5 3 27
no. 10 8 4 6 12 8 8 12 6 16 12 10 22 12 8
10.16 \textit{mod 18}: 11 is a primitive root mod 18, so the primitive roots mod 18 are 
\{11^n : 1 \leq n \leq 6, (n, 6) = 1\} = \{11, 11^5\}.

Since 11^5 = 161051 \equiv 5 \pmod{18}, the primitive roots are 5 and 11.

\textit{mod 27}: 2 is a primitive root mod 27, so the primitive roots mod 27 are 
\{2^n : 1 \leq n \leq 18, (n, 18) = 1\} = \{2^1, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}\}.

Thus the primitive roots are $2^1 \equiv 2$, $2^5 \equiv 5$, $2^7 \equiv 20$, $2^{11} \equiv 23$, $2^{13} \equiv 11$ 
and $2^{17} \equiv 14$.

10.17 We have $\chi(n) = \omega^{\delta(n)}$ if $3 \nmid n$, and 0 if $3|n$.

Taking $g = 2$, we have $b(1) = 0$, $b(2) = 1$, $b(4) = 2$, $b(5) = 5$, $b(7) = 4$ 
and $b(8) = 3$. This leads to the following table.

<table>
<thead>
<tr>
<th>( n )</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>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \chi_0(n) )</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>( \chi_1(n) )</td>
<td>1</td>
<td>( \omega )</td>
<td>( \omega^2 )</td>
<td>( \omega^5 )</td>
<td>( \omega^4 )</td>
<td>( \omega^4 )</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>( \chi_2(n) )</td>
<td>1</td>
<td>( \omega^2 )</td>
<td>( \omega^4 )</td>
<td>( \omega^4 )</td>
<td>( \omega^2 )</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>( \chi_3(n) )</td>
<td>1</td>
<td>( \omega^3 )</td>
<td>0</td>
<td>1</td>
<td>( \omega^3 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>( \chi_4(n) )</td>
<td>1</td>
<td>( \omega^4 )</td>
<td>( \omega^2 )</td>
<td>0</td>
<td>( \omega^4 )</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>( \chi_5(n) )</td>
<td>1</td>
<td>( \omega^5 )</td>
<td>( \omega^4 )</td>
<td>0</td>
<td>( \omega^2 )</td>
<td>( \omega^3 )</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

We can simplify this table by writing $\omega^3 = -1$, $\omega^4 = -\omega$, $\omega^5 = -\omega^2$.

10.18 $\chi_h(m) = \omega^{\delta^h(m)}$ and $\chi_h(n) = \omega^{\delta(n)}$, if $p \nmid m$, $p \nmid n$. Thus
\[ \chi_h(m)\chi_h(n) = \omega^{\delta^h(m)+\delta(n)} \]
\[ = \omega^{\delta^h(mn)}, \quad \text{by Theorem 10.10(a),} \]
\[ = \chi_h(mn). \]

If $p|m$ or $p|n$, then $\chi_h(m)\chi_h(n) = \chi_h(mn) = 0$, by definition. Thus $\chi_h$ is completely multiplicative.

Also, $\chi_h(n+p^a) = \omega^{\delta^h(n+p^a)} = \omega^{\delta^h(n)} = \chi_h(n)$, so $\chi_h$ is periodic with period $p^a$.

We must prove that $f(rs) = f(r)f(s)$, and $g(rs) = g(r)g(s)$, for all integers $r, s$. Since these results are clearly true when $r$ and/or $s$ is even, we assume that $r$ and $s$ are odd. If $r \equiv s \pmod{4}$, then $f(rs) = f(r)f(s) = 1$; if $r \equiv -s \pmod{4}$, then $f(rs) = f(r)f(s) = -1$. Also,
\[ g(rs) = e^{2\pi i \delta^h(rs)/2} = e^{2\pi i (\delta^h(r)+\delta^h(s))/2} = e^{2\pi i \delta^h(r)} = g(r)g(s), \]

as required.

10.19 We have $f(1) = f(5) = 1$, $f(3) = f(7) = -1$, $f(\text{even}) = 0$.

Also, $b(1) = 2$, since $1 \equiv (-1)^5 \equiv 1 \pmod{8}$, and similarly, $b(3) = b(5) = 1$, $b(7) = 2$. Thus $g(1) = g(7) = 1$, $g(3) = g(5) = -1$, $g(\text{even}) = 0$.

This leads to the following table.

<table>
<thead>
<tr>
<th>( n )</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>( \chi_{1,1}(n) )</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>( \chi_{1,2}(n) )</td>
<td>1</td>
<td>0</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_{2,1}(n) )</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>( \chi_{2,2}(n) )</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

10.20 The first character in each case is the principal character, defined by $\chi(n) = 1$ if $p \nmid n$, and $\chi(n) = 0$ if $p|n$ ($p = 29, 43$).

To obtain the second character, we write $\chi(n) = 1$ if $\gcd(n, p) = 1$, and $\chi(n) = -1$ if $\gcd(n, p) = p$.
\( p = 29: \)
\( \chi(n) = 1 \) for \( n = 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28; \)
\( \chi(n) = -1 \) for \( n = 2, 3, 8, 10, 11, 12, 14, 15, 17, 18, 19, 21, 26, 27; \)
\( \chi(n) = 0 \) for \( n = 29. \)

\( p = 43: \)
\( \chi(n) = 1 \) for \( n = 1, 4, 6, 9, 10, 11, 13, 14, 15, 16, 17, 21, 23, 24, 25, 31, \)
\( 35, 36, 38, 40, 41; \)
\( \chi(n) = -1 \) for \( n = 2, 3, 5, 7, 8, 12, 18, 19, 20, 22, 26, 27, 28, 29, 30, 32, \)
\( 33, 34, 37, 39, 42; \)
\( \chi(n) = 0 \) for \( n = 43. \)

10.21 mod 27:
The two real characters are \( \chi_0 \) and \( \chi_9 \), defined by:
\( \chi_0(n) = 1 \) if \( 3 \nmid n \), \( \chi_0(n) = 0 \) if \( 3 \mid n; \)
\( \chi_9(n) = 1 \) if \( b(n) \) is even — that is, \( n = 1, 4, 7, 10, 13, 16, 19, 22, 25; \)
\( \chi_9(n) = -1 \) if \( b(n) \) is odd — that is, \( n = 2, 5, 8, 11, 14, 17, 20, 23, 26; \)
\( \chi_9(n) = 0 \) if \( 3 \mid n. \)

mod 32:
The four real characters are \( \chi_{1,4}, \chi_{2,4}, \chi_{1,8} \) and \( \chi_{2,8}; \) to define them, we need to calculate the values of \( b(n) \) in Theorem 10.11: \( b(1) = b(31) = 8, \)
\( b(3) = b(29) = 3, b(5) = b(27) = 1, b(7) = b(25) = 2, b(9) = b(23) = 6, \)
\( b(11) = b(21) = 5, b(13) = b(19) = 7, b(15) = b(17) = 4. \) So
\( \chi_{1,4}(n) = 1 \) if \( n = 1, 3, 9, 11, 17, 19, 25, 27; \)
\( \chi_{1,4}(n) = -1 \) if \( n = 5, 7, 13, 15, 21, 23, 29, 31; \)
\( \chi_{2,4}(n) = 1 \) if \( n = 1, 7, 9, 15, 17, 23, 25, 31; \)
\( \chi_{2,4}(n) = -1 \) if \( n = 3, 5, 11, 13, 19, 21, 27, 29; \)
\( \chi_{1,8}(n) = 1 \) if \( n \equiv 1 \) (mod 4);
\( \chi_{1,8}(n) = -1 \) if \( n \equiv 3 \) (mod 4);
\( \chi_{2,8}(n) = 1 \) for all odd \( n. \)
In each case, \( \chi(n) = 0 \) if \( n \) is even.

mod 24:
The four real characters mod 8 are \( \chi_{1,1}, \chi_{2,1}, \chi_{1,2} \) and \( \chi_{2,2}, \) defined by:
\( \chi_{1,1}(n) = 1 \) if \( n = 1 \) or 3; \( \chi_{1,1}(n) = -1 \) if \( n = 5 \) or 7;
\( \chi_{2,1}(n) = 1 \) if \( n = 1 \) or 7; \( \chi_{2,1}(n) = -1 \) if \( n = 3 \) or 5;
\( \chi_{1,2}(n) = 1 \) if \( n = 1 \) or 5; \( \chi_{1,2}(n) = -1 \) if \( n = 3 \) or 7;
\( \chi_{2,2}(n) = 1 \) for all odd \( n. \)
The two real characters mod 3 are \( \chi_0 \) and \( \chi_1, \) defined by:
\( \chi_0(1) = \chi_0(2) = 1; \chi_1(1) = 1, \chi_1(2) = -1. \)
Combining these, we obtain the following eight real characters mod 24.

<table>
<thead>
<tr>
<th>( n )</th>
<th>1</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \chi_{1,1}\chi_0 )</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_{2,1}\chi_0 )</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_{1,2}\chi_0 )</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_{2,2}\chi_0 )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_{1,1}\chi_1 )</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_{2,1}\chi_1 )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_{1,2}\chi_1 )</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_{2,2}\chi_1 )</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
</tr>
</tbody>
</table>

10.22 mod 25: \( \chi_1, \chi_2, \chi_3, \chi_4, \chi_5, \chi_7, \chi_8, \chi_9, \chi_{11}, \chi_{12}, \chi_{13}, \chi_{14}, \chi_{16}, \chi_{17}, \chi_{18}, \chi_{19}, \chi_{21}, \chi_{22}, \chi_{23}, \chi_{24}; \)

mod 32: \( \chi_{1,1}, \chi_{1,3}, \chi_{1,5}, \chi_{1,7}, \chi_{2,1}, \chi_{2,3}, \chi_{2,5}, \chi_{2,7}; \)

mod 72: \( \chi_{1,1}\chi_{1,1}, \chi_{1,2}\chi_{1,1}, \chi_{2,1}\chi_{1,1}, \chi_{2,2}\chi_{1,1}, \chi_{4}\chi_{1,1}, \chi_{5}\chi_{1,1}, \chi_{5}\chi_{2,1}; \)

59
8A Let \( g_k(n) = \sum_{m \mod k} e^{2\pi i mn/k} \) and \( c_k(n) = \sum_{(m,k)=1} e^{2\pi i mn/k} \).

Then \( g_k(n) = \sum_{d|k} c_d(n) \), since every fraction \( m/k \) can be reduced to lowest terms \( a/d \), where \( d/k \) and \( 1 \leq a \leq d \), \( (a,d) = 1 \).

It follows from the Möbius inversion formula that

\[
c_k(n) = \sum_{d|k} \mu \left( \frac{k}{d} \right) g_d(n) = \sum_{d|k} \mu \left( \frac{k}{d} \right) \sum_{1 \leq m \leq d} e^{2\pi i mn/d}.
\]

But this last sum is 0 unless \( d|n \) (by Theorem 8.1), and equals \( d \) if \( d|n \).

Thus \( c_k(n) = \sum_{d|k} \mu \left( \frac{k}{d} \right) d = \sum_{d|(n,k)} d \mu \left( \frac{k}{d} \right) \).

8B (a) \[
\sum_{k=1}^{n} c_k(m) = \sum_{k=1}^{n} \sum_{d|m, (m,k)} d \mu \left( \frac{k}{d} \right) = \sum_{d|m} d \sum_{k=1}^{n} \mu \left( \frac{k}{d} \right) = \sum_{d|m} d \sum_{r \leq n/d} \mu(r) \quad (\text{where } r = k/d)
\]

\[
= \sum_{d|m} d \sum_{r \leq n/d} \mu(r) = \sum_{d|m} d \sum_{r \leq n/d} \mu(r) = \sum_{d|m} d \sum_{r \leq n/d} \mu(r) = M \left( \frac{n}{d} \right).
\]

(b) When \( n = m \), we have

\[
\sum_{k=1}^{m} c_k(m) = \sum_{d|m} d M \left( \frac{m}{d} \right) = \sum_{d|m} m \sum_{d|m} \frac{M(d)}{d} = \sum_{d|m} \frac{M(d)}{d}.
\]

By the Möbius inversion formula, we have

\[
M(m) = m \sum_{d|m} \frac{\mu(m/d)}{d} \sum_{k=1}^{d} c_k(d), \quad \text{as required.}
\]

8C Let \( d = (k_1, k_2) \). We aim to prove the criterion of Theorem 8.16, that \( \chi(a) = \chi(b) \) when \( a \equiv b \pmod{d} \) with \( (a,k) = (b,k) = 1 \). We do this by constructing an integer \( m \) such that

(i) \( m \equiv a \pmod{k_1} \), \quad (ii) \( m \equiv b \pmod{k_2} \), \quad and \quad (iii) \( (m,k) = 1 \).

Then (i) and (iii) imply that \( \chi(m) = \chi(a) \), whereas (ii) and (iii) imply that \( \chi(m) = \chi(b) \). Hence \( \chi(a) = \chi(b) \), as required.

Write \( d = sk_1 + tk_2 \) by Euclid’s algorithm, and then write \( a - b = rd \). Set \( n = a - rsk_1 = b + rtk_2 \), so that \( n \equiv a \pmod{k_1} \) and \( n \equiv b \pmod{k_2} \). Now let \( k' = \text{lcm}(k_1, k_2) \) and let \( q \) be the product of all the primes that divide \( k \) but not \( n \) (we take \( q = 1 \) if there are no such primes). We can then take \( m = n + qk' \) in order to satisfy (i), (ii) and (iii).
8D (a) Since the integers \( k_i \) are relatively prime in pairs, it follows from the Chinese remainder theorem that there is a unique integer \( a_i \mod k \) such that
\[
a_i \equiv a \mod (k_i), \quad a_i \equiv 1 \mod (k_j) \quad \text{for} \quad j \neq i.
\]
(b) By part (a), \( a \equiv a_1a_2 \ldots a_r \mod k_j \) for \( j = 1, 2, \ldots, r \), and hence \( a \equiv a_1a_2 \ldots a_r \mod (k) \).

Define \( \chi_i \) by the equation \( \chi_i(a) = \chi(a_i) \). Then \( \chi_i \) is a character mod \( k_i \).

For, if \( a \equiv b \mod (k) \), then \( a_i \equiv b_i \mod (k_i) \), and \( \chi_i(a) = \chi_i(b) \).

Moreover, if \( \ell \equiv m \mod (k_i) \), then \( \ell_i \equiv m_i \mod (k) \), and \( \chi_i(\ell) = \chi(\ell_i) = \chi(m_i) = \chi_i(m) \).

8E With the notation of Problem 8D, we have
\[
\chi(a) = \chi(a_1a_2 \ldots a_r) = \chi(a_1)\chi(a_2) \cdots \chi(a_r) = \chi_1(a)\chi_2(a) \cdots \chi_r(a).
\]

If \( \chi(a) = \chi_1(a)\chi_2(a) \cdots \chi_r(a) \), then
\[
\chi_i(a) = \chi_i(a_1)\chi_2(a) \cdots \chi_r(a_i) = \chi_i(a),
\]
so the decomposition is unique.

Thus \( \chi \) can be factored uniquely as \( \chi = \chi_1\chi_2 \cdots \chi_r \).

8F Let \( k = k_1k_2 \ldots k_r \), and \( K_i = k/k_i \). Then the greatest common divisor of the set \( \{K_1, \ldots, K_r\} \) is 1, and we can find integers \( g_1, \ldots, g_r \) such that
\[
g_1K_1 + g_2K_2 + \cdots + g_rK_r = 1.
\]

Given an integer \( m \), we can use the Chinese remainder theorem to find integers \( m_i \) such that
\[
m_i = m \mod (k_i), \quad \text{and} \quad m_i \equiv 1 \mod (k_j) \quad \text{for} \quad j \neq i.
\]

Thus
\[
G(a, \chi) = \sum_{m=1}^{k} \chi(m)e^{2\pi ima/k}
\]
\[
= \prod_{j=1}^{r} \left( \sum_{m_j=1}^{k_j} \chi_j(m_j)e^{2\pi im_ja_jg_j/k_j} \right)
\]
\[
= \prod_{j=1}^{r} \chi_j(g_j) \left( \sum_{m_j=1}^{k_j} \chi_j(g_jm_j)e^{2\pi im_ja_jg_j/k_j} \right)
\]
\[
= \prod_{j=1}^{r} \chi_j(g_j)G(a_j, \chi_j),
\]

since \( g_jm_j \) goes through a complete set of residues mod \( k_j \) as \( m_j \) does.

But \( g_jK_j \equiv 1 \mod (k_j) \), so \( \chi_j(K_j) = \chi_j(k/k_j) \).

Thus \( G(a, \chi) = \prod_{j=1}^{r} \chi_j(K_j)G(a_j, \chi_j) \), as required.

8G Let \( d \) be the conductor of \( \chi \), and let \( k \) be an induced modulus for \( \chi \).

If \( (d, k) = d' \), then by Exercise 6, \( d' \) is an induced modulus for \( \chi \).

But \( d \) is the smallest induced modulus for \( \chi \), so \( d' = d \).

Since \( (d, k) = d \), we have \( d|k \), as required.
We have $\chi = \chi_1 \chi_2 \cdots \chi_r$, where $\chi_i$ is a character modulo $k_i$ for each $i$. Note that $f(\chi_i) | k_i$ for each $i$, so the numbers $f(\chi_i)$ are pairwise coprime.

Let $d = f(\chi_1) f(\chi_2) \cdots f(\chi_r)$. We first show that $d$ is an induced modulus for $\chi_i$. For, suppose that $a \equiv 1 \pmod{d}$ and $(a, k_i) = 1$ for each $i$. Then $a \equiv 1 \pmod{f(\chi_i)}$ and $(a, k_i) = 1$ for each $i$, and so $\chi_i(a) = 1$ for each $i$. Thus $\chi(a) = 1$, as required. This shows that $f(\chi_1) | f(\chi_2) \cdots f(\chi_r)$.

Now let $d_i = f(\chi_i, k_i)$ for each $i$, so that $f(\chi) = d_1 d_2 \cdots d_r$. We show that $d_i$ is an induced modulus for $\chi_i$. For, suppose that $a \equiv 1 \pmod{d_i}$ and $(a, k_i) = 1$. Then $\chi_i(a) = \chi(a_i)$, where $a_i$ is chosen (by the Chinese Remainder Theorem) to satisfy $a_i \equiv a \pmod{k_i}$ and $a_i \equiv 1 \pmod{k_j}$, for each $j \neq i$.

Note that $a_i \equiv 1 \pmod{d_j}$ and $(a_i, k_j) = 1$ for every $j = 1, 2, \ldots, r$. Hence $a_i \equiv 1 \pmod{f(\chi_i)}$ and $(a, k) = 1$, so $\chi_i(a) = \chi(a_i) = 1$, as required.

This shows that $f(\chi_1) f(\chi_2) \cdots f(\chi_r) | f(\chi)$, which completes the proof that $f(\chi) = f(\chi_1) f(\chi_2) \cdots f(\chi_r)$.

By Abel’s identity with $a(m) = \chi(m)$ and $f(t) = 1/t$, we have

$$\int_{m=N+1}^{M} \frac{\chi(m)}{m} \, dm \leq \int_{m=N+1}^{M} \frac{\chi(m)}{N+1} \, \sqrt{\log k} \, \frac{1}{t} \, dt \leq \frac{1}{N+1} \sqrt{k \log k} + \frac{1}{N+1} \sqrt{k \log k} = \frac{2}{N+1} \sqrt{k \log k},$$

as required.

Chapter 9

Let $\omega = e^{2\pi i/p}$, then $G(n, \omega) = \sum_r \chi(r) \omega^{nr}$ and $G(n; p) = \sum_r \omega^{nr^2}$.

If $\sum_1$ and $\sum_2$ denote summations over the quadratic residues and nonresidues mod $p$, respectively, then

$$G(n, \omega) = \sum_1 \omega^{nr} - \sum_2 \omega^{nr}$$

and $1 + \sum_1 \omega^{nr} + \sum_2 \omega^{nr} = \sum_{r \equiv 0 \pmod{p}} \omega^{nr} = 0$, since $p \nmid n$.

Thus $G(n, \omega) = 1 + 2 \sum_1 \omega^{nr}$.

But the quadratic residues mod $p$ can be chosen to be $1^2, 2^2, \ldots, (\frac{1}{2}(p-1))^2$, and so

$$G(n, \omega) = 1 + 2 \sum_{r=1}^{\frac{1}{2}(p-1)} \omega^{nr^2} = \sum_r \omega^{nr^2},$$

since $\sum_{r=1}^{\frac{1}{2}(p-1)} \omega^{r(p-r)^2} = \sum_{r=1}^{\frac{1}{2}(p-1)} \omega^{nr^2}$, for $r = 1, 2, \ldots, \frac{1}{2}(p-1)$.

Thus $G(n, \omega) = G(n; p)$ if $p \nmid n$.

If $p | n$, then $G(n, \omega) = 0$ and $G(n; p) = p$, so $G(n, \omega) \neq G(n; p)$. 

74
Since we wish to find \( R = (r_1 r_2 r_3 r_4 r_5)^3 \), we need the solutions of \( r_1 + r_2 + r_3 + r_4 + r_5 \equiv 5 \pmod{3} \), where each \( r_i \) is non-zero; these are as follows.

\[
\begin{array}{cccccccc}
  r_1 & 1 & 1 & 2 & 2 & 2 & 1 & 2 & 2 & 2 & 2 & 1 \\
  r_2 & 1 & 2 & 2 & 1 & 1 & 2 & 1 & 2 & 2 & 2 & 1 \\
  r_3 & 2 & 2 & 1 & 1 & 2 & 2 & 1 & 2 & 1 & 1 \\
  r_4 & 2 & 2 & 1 & 1 & 2 & 2 & 2 & 1 & 2 & 1 & 1 \\
  r_5 & 2 & 1 & 2 & 2 & 2 & 2 & 1 & 2 & 1 & 1 & 1 \\
\end{array}
\]

The right-hand side of equation (23) is therefore

\[
(5|3)^{-1} - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 + 1 = -(-9) = 9,
\]

and the left-hand side is \( G(1, \chi)^4 = ((-1|3)^2)^2 = 9 \).

\[9\text{C}\]

We have to show that

\[
(h|k)G(1;k) = \sqrt[\frac{k}{h}]
\frac{1 + i}{2}(1 + e^{-\pi i k/2})(k|h)G(1;h).
\]

When \( h \equiv k \equiv 1 \pmod{4}, (k|h) = (h|k) \) and \( e^{-\pi i k/2} = -i \), the right-hand side becomes

\[
\sqrt[\frac{k}{h}]
\frac{1 + i}{2}(1 - i) \cdot (h|k) \cdot \sqrt{k} = (h|k)G(1;k).
\]

When \( h \equiv 1 \pmod{4}, k \equiv 3 \pmod{4}, (k|h) = (h|k) \) and \( e^{-\pi i k/2} = i \), and the right-hand side becomes

\[
\sqrt[\frac{k}{h}]
\frac{1 + i}{2}(1 + i) \cdot (h|k) \cdot \sqrt{k} = (h|k)G(1;k).
\]

When \( h \equiv 3 \pmod{4}, k \equiv 1 \pmod{4}, (k|h) = (h|k) \) and \( e^{-\pi i k/2} = i \), and the right-hand side becomes

\[
\sqrt[\frac{k}{h}]
\frac{1 + i}{2}(1 + i) \cdot (h|k) \cdot (-i\sqrt{k}) = (h|k)\sqrt{k} = (h|k)G(1;k).
\]

When \( h \equiv k \equiv 3 \pmod{4}, (k|h) = -(h|k) \) and \( e^{-\pi i k/2} = -i \), and the right-hand side becomes

\[
\sqrt[\frac{k}{h}]
\frac{1 + i}{2}(1 - i) \cdot -(h|k) \cdot (-i\sqrt{k}) = (h|k)i\sqrt{k} = (h|k)G(1;k).
\]

The result therefore follows in all cases.

\[9\text{D}\]

(a) Putting \( z = t + Re^{i\pi/4} \), where \(-\frac{1}{2} \leq t \leq 0 \), we have

\[
|\phi(z)| \leq \sum_{n=0}^{a-1} \left| \exp\left\{ \frac{\pi ia(t + Re^{i\pi/4})^2}{m} + 2\pi in(t + Re^{i\pi/4}) \right\} \right|.
\]

The expression in braces has real part

\[
-\frac{\pi a}{m}\left( R\sqrt{2t} + R^2 \right) - \sqrt{2}\pi n R
\]

\[
\leq \frac{\pi a R\sqrt{2}}{2m} - \frac{\pi a R^2}{m} - \sqrt{2}\pi n R, \text{ since } t \geq -\frac{1}{2}.
\]

So

\[
|\phi(z)| \leq m \exp\left\{ \frac{\pi a}{\sqrt{2}m} \left( R - \sqrt{2}R^2 \right) \right\} \exp(-\sqrt{2}\pi n R) = o(1),
\]

as \( R \to \infty \). Since the path of integration has finite length \( \left( \frac{1}{2} \right) \), we have

\[
\int_B \phi = o(1), \text{ as } R \to \infty.
\]
(b) Putting \( z = t + Re^{i\pi/4} \), where \( -\frac{nm}{a} \leq t \leq 0 \), we have

\[
\exp \left\{ \frac{\pi a}{m} \left( z + \frac{nm}{a} \right)^2 \right\} = \exp \left\{ \frac{\pi a}{m} \left( t + Re^{i\pi/4} + \frac{nm}{a} \right)^2 \right\}.
\]

Since \( t \geq -\frac{nm}{a} \), the expression in braces has real part

\[
-\frac{\pi a R \sqrt{2}}{m} \left( t + \frac{nm}{a} + R \frac{\sqrt{2}}{a} \right) \leq -\frac{\pi a R \sqrt{2}}{m} \left( -\frac{nm}{a} + \frac{nm}{a} + R \frac{\sqrt{2}}{a} \right) = -\frac{\pi a R^2}{m}.
\]

So

\[
\exp \left\{ \frac{\pi a}{m} \left( z + \frac{nm}{a} \right)^2 \right\} \leq \exp \left( -\frac{\pi a R^2}{m} \right) \exp(-\pi nR\sqrt{2}) = o(1),
\]

as \( R \to \infty \).

Since the path of integration has finite length \((nm/a)\), we deduce that the integral from \( \alpha - mn/a \) to \( \alpha \) is \( o(1) \), as \( R \to \infty \).

### Chapter 10

**10A** (a) If \( n^2 \equiv -1 \pmod{p} \), then \( n^4 \equiv 1 \pmod{p} \).

By Theorem 10.1(b), \( 4|\phi(p) \), so \( p - 1 = 4k \), as required.

(b) If \( n^4 \equiv -1 \pmod{p} \), then \( n^8 \equiv 1 \pmod{p} \).

By Theorem 10.1(b), \( 8|\phi(p) \), so \( p - 1 = 8k \), as required.

(c) No: for example, take \( n = 2, a = 3 \) and \( p = 3 \); then \( 3|(2^3 + 1) \), but \( 3 \neq 6k + 1 \) for any \( k \).

**10B** If \( \exp_m(a) = k \) and \( \exp_m(b) = \ell \), then \( (k, \ell) = 1 \) and

\[
a^k \equiv 1 \pmod{m}, \quad b^\ell \equiv 1 \pmod{m}.
\]

Thus \( (ab)^{k\ell} \equiv 1 \pmod{m} \).

Moreover, since \( k \) and \( \ell \) are the least integers satisfying \((*)\), and \( (k, \ell) = 1 \), \( k\ell \) is the least integer for which \( (ab)^{k\ell} \equiv 1 \pmod{m} \).

Thus \( \exp_m(ab) = k\ell = \exp_m(a) \exp_m(b) \).

**10C** Since \( 2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1) \), we have \( 2^{2^{n+1}} \equiv 1 \pmod{F_n} \).

So if \( f \) is the exponent of \( 2 \pmod{F_n} \), then \( f|2^{2^n+1} \).

It follows that if \( 2 \) is a primitive root mod \( F_n \), then \( f = \phi(F_n) = 2^{2^n} \), and hence that \( 2^{2^{n+1}} \), which is clearly false for \( n > 1 \). It follows that \( 2 \) is not a primitive root mod \( F_n \), for \( n > 1 \).

**10D** (a) By Theorem 10.4, there are exactly \( \phi(6) = 2 \) integers with exponent \( 6 \pmod{43} \). Since the exponent of \( 3 \) is \( 42/\phi(42) \), by Lemma 1, and this equals \( 6 \) if and only if \( (k, 42) = 7 \).

Thus \( k = 7 \) or \( 35 \).

But \( 3^7 \equiv 2187 \equiv 37 \pmod{43} \), and \( 3^{35} \equiv 37^5 \equiv (-6)^5 \equiv 7 \pmod{43} \), so the only integers with exponent \( 6 \) are \( 7 \) and \( 37 \pmod{43} \).

(b) There are exactly \( \phi(21) = 12 \) integers with exponent \( 21 \pmod{43} \). The exponent of \( 3 \) is \( 42/\phi(42) \), which equals \( 21 \) if and only if \( (k, 42) = 2 \).

Thus \( k = 2, 4, 8, 10, 16, 20, 22, 26, 32, 34, 38 \) or \( 40 \pmod{43} \), and \( 3^k \equiv 9, 38, 25, 10, 23, 14, 40, 15, 31, 17 \) or \( 24 \pmod{43} \).

So the only integers with exponent \( 21 \) are \( 9, 10, 13, 14, 15, 17, 23, 24, 25, 31, 38 \) and \( 40 \).
10E If $g$ is a primitive root mod $p$ then, by Theorem 10.2,

\[ (p-1)! = 1 \cdot 2 \ldots (p-1) \equiv g \cdot g^2 \cdot g^3 \ldots g^{p-1} \pmod{p} \]
\[ \equiv g^{1+2+\ldots+(p-1)} \pmod{p} \]
\[ \equiv g^{\phi(p-1)} \pmod{p} \]
\[ \equiv -1 \pmod{p}, \quad \text{as required.} \]

10F We have $n \equiv (-1)^{(n-1)/2}5^{b(n)} \pmod{64}$. Now mod 64, we have

<table>
<thead>
<tr>
<th>$5^1$</th>
<th>$5^2$</th>
<th>$5^3$</th>
<th>$5^4$</th>
<th>$5^5$</th>
<th>$5^6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>25</td>
<td>-3</td>
<td>-15</td>
<td>-11</td>
<td>9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$5^7$</th>
<th>$5^8$</th>
<th>$5^9$</th>
<th>$5^{10}$</th>
<th>$5^{11}$</th>
<th>$5^{12}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>-19</td>
<td>-31</td>
<td>-27</td>
<td>-7</td>
<td>29</td>
<td>17</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$5^{13}$</th>
<th>$5^{14}$</th>
<th>$5^{15}$</th>
<th>$5^{16}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>-23</td>
<td>13</td>
<td>1</td>
</tr>
</tbody>
</table>

So we obtain

\[ b(1) = 16, b(3) = 3, b(5) = 1, b(7) = 10, b(9) = 6, b(11) = 5, \]
\[ b(13) = 15, b(15) = 4, b(17) = 12, b(19) = 7, b(21) = 13, b(23) = 14, \]
\[ b(25) = 2, b(27) = 9, b(29) = 11, b(31) = 8, \quad \text{and } b(64 - n) = b(n). \]

10G We show that $2^{a-1}$ is an induced modulus for $\chi_{a,c}$ if and only if $c$ is even.

Then $\chi_{a,c}$ is primitive if and only if $c$ is odd, as at the top of page 221.

Note that $2^{a-1}$ is an induced modulus for $\chi_{a,c}$ precisely when $\chi_{a,c}(n) = 1$ for odd integers $n$ such that $n \equiv 1 \pmod{2^{a-1}}$. Thus $2^{a-1}$ is an induced modulus for $\chi_{a,c}$ precisely when $\chi_{a,c}(2^{a-1} + 1) = 1$.

Let $n = 2^{a+1} + 1$. Since $a \geq 3$, we have $n \equiv 1 \pmod{4}$. Then, by equations (24) and (25) on page 219, $\chi_{a,c}(n) = \omega^{b(n)c}$, where $\omega = \exp(2\pi i / 2^{a-2})$ and we choose $b(n)$ such that $n \equiv 5^{b(n)} \pmod{2^a}$ and $1 \leq b(n) \leq 2^{a-2}$.

Note that $n^2 \equiv 1 \pmod{2^a}$, and so $2b(n) = b(1) = 2^{a-2}$, by Theorem 10.11.

Thus $b(n) = 2^{a-3}$, and so

\[ \chi_{a,c}(n) = 1 \iff 2^{a-2} \mid 2^{a-3}c \iff 2 \mid c. \]

10H Let $m = 2^ap_1^{\alpha_1} \ldots p_r^{\alpha_r}$.

By Theorem 10.13 and 10.15, if $\alpha \geq 3$, then $c = 2^{a-2}$ or $2^{a-3}$ and $c$ is odd; so $\alpha = 3$. Thus $\alpha = 0, 2$ or 3.

Also, for each prime $p_i$, we have $h = 0$ or $h = \phi(p_i^{\alpha_i})/2$ and $p_i \nmid h$.

Thus each $\alpha_i = 1$. This proves the result.

Chapter 11

11A (a) $|\langle \sigma + it \rangle| = |\sum n^{-s}| \leq \sum |n^{-s}| = \sum n^{-\sigma} \leq \sum n^{-2} = \frac{1}{\pi^2}.$

(b) Since $|\mu(n)| \leq 1$ and $|\chi(n)| \leq 1$, we have

\[ |\sum f(n)n^{-s}| \leq \sum |f(n)|n^{-\sigma} \leq \sum n^{-\sigma} \leq \sum n^{-2} = \frac{1}{\pi^2}. \]

(c) Since $|\phi(n)/n| \leq 1$ and $|\phi(n)/n^3| \leq n^{-2}$, we have

\[ |\sum \phi(n)n^{-s-1}| \leq \sum n^{-\sigma} \leq \sum n^{-2} = \frac{1}{\pi^2} \]

and

\[ |\sum \phi(n)n^{-s-2}| \leq \sum n^{-\sigma-2} \leq \sum n^{-4} = \frac{1}{9\pi^4}. \]